UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TRABAJO DE GRADO PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

"AUDITORÍA DE SEGURIDAD INFORMÁTICA DIRIGIDA AL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN MIRA BASADO EN EL ESTÁNDAR COBITv5, SIGUIENDO LA METODOLOGÍA OSSTMMv3"

AUTOR: CRISTIAN LEONEL BRACHO ORTEGA

DIRECTOR DE TESIS: ING. FABIÁN CUZME, MSc.

IBARRA – ECUADOR

2 017

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA.

La UNIVERSIDAD TÉCNICA DEL NORTE dentro del proyecto Repositorio Digital institucional, determinó la necesidad de disponer los textos completos de forma digital con la finalidad de apoyar los procesos de investigación, docencia y extensión de la Universidad.

Por medio del presente documento dejo sentada mi voluntad de participar en este proyecto, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO		
Cédula de identidad	040174771-2	
Apellidos y Nombres	Bracho Ortega Cristian Leonel	
Dirección	Mira, calle Ricardo Rúales y 2 de Febrero	
Email	clbrachoo@utn.edu.ec	
Teléfono	Fijo: 062 280 647	Móvil: 0985517174

DATOS DE LA OBRA	
Título	**AUDITORÍA DE SEGURIDAD INFORMÁTICA DIRIGIDA AL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN MIRA BASADO EN EL ESTÁNDAR COBITv5, SIGUIENDO LA METODOLOGÍA OSSTMMv3**
Autor	Bracho Ortega Cristian Leonel
Fecha	Mayo, 2017
Programa	Pregrado
Titulo por el que opta	Ingeniería en Electrónica y Redes en Comunicación
Director	Ing. Fabián Cuzme, MSc.

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Cristian Leonel Bracho Ortega, con cédula de identidad Nro. 040174771-2, en calidad de autor y titular de los derechos patrimoniales de la obra o trabajo de grado descrito anteriormente, hago entrega del ejemplar respectivo en forma digital y autorizo a la Universidad Técnica del Norte, la publicación de la obra en el Repositorio Digital Institucional y el uso del archivo digital en la biblioteca de la universidad con fines académicos, para ampliar la disponibilidad del material y como apoyo a la educación, investigación y extensión, en concordancia con la Ley de Educación Superior Artículo 144.

3. CONSTANCIA

El autor manifiesta que la obra objeto de la presente autorización es original y se la desarrollo, sin violar derechos de autor de terceros, por lo tanto la obra es original y es titular de los derechos patrimoniales, por lo que se asume la responsabilidad del contenido de la misma y saldrá en defensa de la Universidad en caso de reclamación por parte de terceros.

En la cuidad de Ibarra,

El Autor:

Cristian Leonel Bracho Ortega

CI: 040174771-2

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIANCIAS APLICADAS

CESIÓN DE DERECHOS DE AUTOR DEL TRABAJO DE GRADO A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

Yo, Cristian Leonel Bracho Ortega, con cédula de identidad Nro. 040174771-2, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la ley de propiedad intelectual del Ecuador, articulo 4, 5 y 6, en calidad de autor del trabajo de grado denominado: **"AUDITORÍA DE SEGURIDAD INFORMÁTICA DIRIGIDA AL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN MIRA BASADO EN EL ESTÁNDAR COBITv5, SIGUIENDO LA METODOLOGÍA OSSTMMv3"**, que ha sido desarrollada para optar por el título de Ingeniería en Electrónica y Redes de Comunicación, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente. En mi condición de autor me reservo los derechos morales de la obra antes mencionada, aclarando que el trabajo aquí descrito es de mi autoría y que no ha sido previamente presentado para una calificación profesional.

En concordancia suscribo este documento en el momento que hago entrega del trabajo final en formato impreso y digital a la biblioteca de la Universidad Técnica del Norte

……..

Firma

Cristian Leonel Bracho Ortega

040174771-2

Ibarra, Mayo del 2017

UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

DECLARACIÓN

Yo, Cristian Leonel Bracho Ortega, con cédula de ciudadanía nro. 040174771-2, estudiante de la carrera de Ingeniería en Electrónica y Redes de Comunicación, libre y voluntariamente declaro bajo juramento que el trabajo aquí descrito es de mi autoría; y que este no ha sido previamente presentado para ningún grado o calificación profesional, para efectos académicos y legales será de mi responsabilidad.

A través de la presente declaración cedo los derechos de propiedad intelectual correspondientes a este trabajo, a la Universidad Técnica del Norte, según lo establecido por las leyes de propiedad intelectual, del reglamento y normativa vigente de la Universidad Técnica del Norte.

Cristian Leonel Bracho Ortega

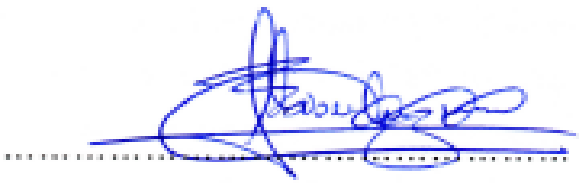
UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CERTIFICACIÓN

Certifico que el presente trabajo de titulación "**AUDITORÍA DE SEGURIDAD INFORMÁTICA DIRIGIDA AL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN MIRA BASADO EN EL ESTÁNDAR COBITv5, SIGUIENDO LA METODOLOGÍA OSSTMMv3"** ha sido realizada en su totalidad por el señor: Cristian Leonel Bracho Ortega portador de la cédula de identidad con número: 040174771-2 bajo mi supervisión.

Es todo en cuanto puedo certificar en honor a la verdad.



Ing. Fabián Cuzme, MSc

DIRECTOR DE TESIS

DEDICATORIA

A mis padres Rosa Esperanza Ortega Guerra y Luis Anibal Bracho Patiño, por haberme brindado la oportunidad de poder estudiar una carrera universitaria, a pesar de todos los contratiempos presentados durante todo el camino recorrido durante mis años de estudio y por su paciencia y entrega diaria con sus sabios consejos.

A mis hermanos y familiares cercanos que siempre supieron brindarme una palabra de aliento en los momentos difíciles, en especial a Dolores del Pilar Bracho Ortega que fue mi sustento económico en la mayor parte de mis años de estudio.

A mis amigos Galo Espinosa, Javier Cabascango, Eduardo Picuasi, Ronal Mena, Julio Tamayo y Carlos Muñoz, que a más de haber sido mis compañeros de clase siempre estuvimos apoyándonos en los momentos difíciles y en los momentos de alegría.

A Estefany Meneses que desde que me conoció ha sido una buena amiga, confidente y novia, siempre apoyándome y poco a poco convirtiéndose en una parte esencial de mi vida.

Cristian L. Bracho

AGRADECIMIENTO

Un agradecimiento especial a la Carrera de Ingeniería en Electrónica y Redes de Comunicación de la Facultad de Ciencias Aplicadas de la Universidad Técnica del Norte, por haberme abierto sus puertas para día a día enriquecer mi conocimiento académico y humano con sus sabias enseñanzas.

A mis padres, hermanos y familiares por haberme brindado su apoyo incondicional durante todo el período de mi vida estudiantil y por haberme formado siempre encaminado hacia el bien común.

Al Magister Fabián Cuzme, por haberme guiado durante todo el proceso de culminación de mi trabajo de grado, quien con su paciencia y sabios consejos supo brindarme su apoyo desinteresado para culminar mi proyecto de titulación con éxito.

Al Departamento de Sistemas del Gobierno Autónomo Descentralizado del Cantón Mira, en la persona del Sr. Damián Bastidas, quien supo abrirme las puertas de tan prestigiosa institución para realizar mi proyecto de titulación, siempre dispuesto a brindarme la información necesaria cuando yo lo requerí.

A todos los docentes de la Carrera de Ingeniería en Electrónica y Redes de Comunicación, quienes supieron compartir sus conocimientos conmigo dentro y fuera del aula, haciendo de mí un profesional integral en todos los aspectos; y al Lic. Hugo Enríquez por su ayuda prestada en la ejecución de este trabajo de grado.

Cristian L. Bracho

ÍNDICE DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ECUANCIONES

RESUMEN

El presente proyecto consiste en la ejecución de una auditoría de seguridad informática dirigida al Gobierno Autónomo Descentralizado del Cantón Mira, basado en el estándar COBIT versión 5 y siguiendo la metodología OSSTMM versión 3, con la finalidad de evaluar el estado de las medidas de seguridad que posee la red, y de esta manera encontrar los puntos más vulnerables y poder recomendar las medidas correctivas necesarias que permitan mejorar la eficiencia de la red. Para iniciar, se hace una breve descripción de la fundamentación teórica, para ello se hiso referencia de varios autores para describir aspectos fundamentales sobre la seguridad de la información; además se define la terminología del manual que se utilizará durante todo el proceso, tales como: RAV, seguridad operacional, canales, objetivos, vectores, controles, limitaciones, entre otros; sobre el estándar COBIT no se puede presentar mucha información, debido a que es licenciado y se necesita permisos corporativos de autor. Además se hace referencia de la legislación ecuatoriana en la que se regirá el proceso de la auditoría, esto con el fin de no tener problemas legales con la Institución. Posteriormente se hace una descripción de la situación actual de la infraestructura de la red de comunicaciones del GADM del Cantón Mira, en donde se describe varios aspectos de la entidad, tales como: la topología de red en la que se basa y los equipos con los que cuenta tanto para comunicaciones como para operaciones de cómputo. A continuación, se realizó el proceso de la auditoría, en el que se aplicó varias técnicas de ingeniería social para probar el canal humano y físico; para el canal de comunicaciones inalámbricas fue necesario aplicar una entrevista y el software detector de redes inalámbricas Vistumbler; el canal de telecomunicaciones fue definido como un objetivo no probado; y para el canal de redes de datos se aplicó una entrevista y el software de auditoría Kali-Linux. Para concluir se presenta la elaboración de la primera versión del Manual de Políticas de Seguridad de la Información para el GADM, el cual se desarrolla en trece temas diferentes, mismos que se encuentran referenciados al estándar COBIT para la Seguridad de la Información en su versión 5, con esto se trata de tener una base de regulación normativa para el GADM, ya que actualmente no posee una y esta debería considerarse como la base para regular todas las actividades que implican el manejo del recurso informático de cualquier entidad.

PALABRAS CLAVES: Seguridad informática, COBIT, OSSTMM, Auditoría, Controles operacionales, técnicas, canales.

ABSTRACT

The objective of this project is to make IT security audit process directed to the Decentralized Autonomous Government from Mira canton, based to COBIT standard version 5, following the OSSTMM methodology version 3, in order to evaluate the current state of the security network measures to find the most vulnerable points and to be able to recommend the necessary corrective measures, which allow to improve the efficiency of the network. To start, a brief description of the theoretical basis was made, based on some authors' information to describe fundamental aspects about data security. It also defines the terminology of the manual, which will be used throughout the process, such as: RAV, operational security, channels, targets, vectors, controls, limitations, and others; COBIT standard cannot submit a lot of information because it is licensed and it is necessary to have author permissions. In addition, reference is made to the Ecuadorian legislation because the audit process will be governed to avoid legal problems with the Institution. Subsequently, a description is given about the current situation of the GADM-Mira communications network infrastructure in Mira Canton, it describes different aspects of the entity, such as: the network topology on which it is based and the equipment of the institution for both communications and computing operations, the audit process was carried out, where several social engineering techniques were applied to test the human and physical channel; for wireless communications channel, it was necessary to apply an interview and Vistumbler wireless network detector software; the telecommunications channel was defined as an untested target and for the data network channel, it was applied an interview and Kali-Linux audit software, Finally, the first version of the GADM was presented, the Manual of Information Security Polices, which is developed in thirteen different themes, they were reference to COBIT standard for Information Security version 5, with this, it tries to have a normative regulation vase for the Institution, since at the moment, it does not have own one and this should be considered like the base to regulate all the activities then involve the handling of the computing resource for every Entities.

KEYWORDS: Informatics security, COBIT, OSSTMM, auditory, operational controls, techniques, channel

PRESENTACIÓN

El proyecto “AUDITORÍA DE SEGURIDAD INFORMÁTICA DIRIGIDA AL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN MIRA BASADO EN EL ESTÁNDAR COBITv5, SIGUIENDO LA METODOLOGÍA OSSTMMv3” se lo realiza con el propósito de tener un punto de partida para la medición de los sistemas de seguridad de la información implementados actualmente por el GADM-Mira, ya que es la primera vez que se realiza un proceso de auditoría de seguridad, para ello el manual de la metodología nos permite obtener valores separados de cinco canales diferentes: humano, físico, de comunicaciones inalámbricas, de telecomunicaciones y de redes de datos; esto con el fin de conocer con exactitud cuál de éstos canales requiere de una mayor atención. En vista de que la Institución antes mencionada no cuenta con una base legal que permita normar las actividades que realizan los empleados en torno al recurso informático, se plantea la creación de la primera versión del Manual de Políticas de Seguridad de la Información.

CAPÍTULO I

1. ANTECEDENTES

1.1 TEMA

Auditoría de seguridad informática dirigida al Gobierno Autónomo Descentralizado del Cantón Mira basado en el estándar COBITv5, siguiendo la metodología OSSTMMv3.

1.2 PROBLEMA

El GADM-Mira es una entidad de carácter público el cual se encuentra ubicado en la parroquia urbana de Mira, entre las calles León Rúales y González Suárez. En la anterior administración municipal se dio la pauta para que la Institución se incluyera al entorno de las tecnologías de la información y comunicación (TICs) y así se creó la red municipal para que el personal que allí labora, realice sus actividades una forma más ágil y se ejecuten las transacciones de manera más simple haciendo uso del Internet como una herramienta de trabajo, y en la actual administración se ha impulsado aún más la inclusión del personal en dichos temas; pero con este nuevo cambio, también surgieron nuevos retos que enfrentar. (GAD-Mira, 2014)

Según datos proporcionados por el encargado del Área de Sistemas de la Institución, nunca antes se ha sometido a su red de datos a un proceso de auditoría, en temas de seguridad informática, por lo que no se conoce a ciencia cierta cuáles son las falencias con respecto a los sistemas de seguridad de información con los que la entidad cuenta, y este hecho se lo puede tomar como una debilidad, ya que en la actualidad no solo se maneja información y cuentas propias de la institución, sino también de la ciudadanía en general, por tal razón, los sistemas con los que el establecimiento cuenta deben ser los suficientemente robustos como para enfrentar cualquier anomalía que se presente; de igual manera se había comentado que hace unos meses atrás, varios servidores sufrieron una sobrecarga de información casi hasta el punto de colapsar y este hecho puede ser un indicador de que algo fuera de lo normal ocurrió en la red, ya que el tráfico que se generó en dicha ocasión no fue el que debía haberse producido por las personas que en ese momento estaban haciendo uso de la

red; otro aspecto que hay que tomar en cuenta es que no se han dictado políticas de seguridad de la información para poder realizar un procedimiento ordenado en caso de sufrir un ataque de hacking, que pueda contemplar el acceso hacia el cuarto de telecomunicaciones, u otros; por lo que posiblemente no se ha creado un plan de contingencia que responda ante dichos hechos.

Muchas entidades ven a las auditorias como una amenaza para su integridad, pero son todo lo contrario a lo que las personas piensan ya que por medio de este proceso se puede conocer más a profundidad, no solo las fortalezas con las que la entidad cuenta, sino que también permite conocer sus debilidades, para poder poco a poco fortalecerlas y disponer de un ambiente seguro donde la información que se maneja sea en lo posible vulnerada, a fin de salvaguardar su buena imagen, en este caso la del GADM-Mira. Desde este punto de vista se ha creído conveniente poner a prueba los sistemas de seguridad de información con los que la red de la Institución cuenta y así conocer técnicamente y con datos reales el estado de los mismos.

La red municipal del GADM-Mira es parcialmente nueva, y por tanto aún no se la ha sometido a una auditoría de seguridad informática, a pesar que lo recomendable es realizar este procedimiento cada año; es por ello que haciendo uso de distintos tipos de herramientas y siguiendo el procedimiento que dicta el manual de metodologías que se tomará como referencia, se pondrá a prueba el estado de la red para detectar si existen fallas en su sistemas de defensa y así poder plantear una serie de recomendaciones y redactar un manual de políticas de seguridad de la información, luego de que se hayan obtenido y analizado los resultados arrojados, una vez finalizado el proceso de la auditoría.

1.3 OBJETIVOS

1.3.1 Objetivo General.

Diagnosticar el estado de la red municipal del Gobierno Autónomo Descentralizado Municipal (GADM) del cantón Mira, mediante una auditoría de seguridad informática basada en las técnicas del estándar COBIT versión 5 y siguiendo la metodología OSSTMM versión 3, a fin de encontrar las posibles debilidades que ésta pueda tener y así plantear una propuesta de mejoramiento que ayude a corregirlas.

1.3.2 Objetivos Específicos.

- Revisar la información teórica recopilada que permitirá la ejecución de la auditoría de seguridad informática en todas sus fases, manteniendo una base científica.
- Recopilar información sobre la ubicación de los recursos de TI (Tecnologías de la Información) de todo el sistema informático del GADM-Mira haciendo uso de su organigrama estructural y así formar la topología de red utilizada por la institución.
- Utilizar las herramientas escogidas previamente en la ejecución de las diferentes etapas de la auditoría de seguridad informática, basándose en la metodología planteada.
- Redactar un informe final con los resultados obtenidos luego de haber concluido con todo el proceso que conlleva la auditoría de seguridad informática en el que se incluyan las conclusiones y recomendaciones que se lograron durante todo el proceso.
- Realizar un manual de políticas de seguridad para el área de informática del GADM-Mira, en donde se enlisten los mecanismos a seguir para mantener seguro su recurso de TI.

1.4 ALCANCE

El desarrollo del proyecto empezó con la revisión del estándar que permitió encontrar una técnica a seguir para la ejecución de la auditoría de seguridad informática, para lo cual se escogió el estándar COBIT (Control Objectives for Information and related Technology) en su versión 5; seguidamente se revisó también la metodología, que permitió llevar un proceso ordenado de la auditoría de seguridad informática, para lo cual se ha escogido la metodología OSSTMM (Open Source Security Testing Methodology Manual) en su versión 3. Fue preciso investigar temas afines que tuvieron relevancia para el llevar a cabo un buen desarrollo del proceso de la auditoría.

Una vez que se logró entender la propuesta teórica que dicta los pasos a seguir para la consecución de la auditoría se seguridad informática, se inició con la primera fase del proyecto, la cual consistió en la recopilación de la información de todo lo que

engloba al sistema informático del GADM-Mira, entre ellos: departamentos, recursos de TI, software, talento humano, dependencias, etc.; y la ubicación exacta de cada uno de ellos para poder esquematizar la topología de red del GADM-Mira. Para culminar con esta fase, fue necesaria la colaboración del personal responsable del Área de Sistemas, ya que no solo se necesitaron datos del sistema informático, sino también datos de la Institución.

Luego de que se conoció la topología de la red del GADM-Mira, se procedió a buscar las herramientas y recursos que permitieron encontrar las partes más vulnerables a ataques de hacking dentro de la Institución; para ello se tomó en cuenta la utilización preferentemente de herramientas de software libre, hacking ético, a más de los procedimientos que dicte el estándar, dichas herramientas fueron analizadas dependiendo de las mejores características que presentaron, en base a los resultados que se pretendieron obtener. La metodología que se tomó como referencia dicta los procedimientos que deben llevarse a cabo para poner en marcha la auditoría de seguridad informática, una vez que hayan sido superadas las fases anteriores, la cual consiste en aplicar las herramientas que se escogieron y realizar una serie de ataques para buscar los puntos más vulnerables de la red municipal por los que se pueda violar los mecanismos de seguridad con los que ésta dispone, tomando en cuenta que no solo se realizaron ataques de software y de acceso, sino también haciendo uso de varias técnicas de ingeniería social, se intentó persuadir al talento humano, todo esto con la finalidad de buscar un punto de penetración hacia la red. Cabe señalar que los procedimientos realizados se los llevaron a cabo tratando de no interrumpir las funciones laborales del personal, por lo que se los debió realizar en un horario donde no se perturbe las actividades de los trabajadores que utilizan los equipos de TI como su herramienta de trabajo.

En la tercera fase se obtuvieron los resultados arrojados por la auditoría, mismos que se manejaron con mucha prudencia y de manera confidencial solo con el personal autorizado; basándose en dichos resultados, se redactó un informe final en donde se incluyeron los puntos más vulnerables encontrados, y en sí las debilidades que se presentaron en todo el entorno de la red, a más de las recomendaciones pertinentes para la corrección y mejoramiento de las mismas. El informe que se presentó se lo expuso a la persona encargada del área informática, además se realizó una propuesta

para corregir o mejorar las falencias encontradas; y para concluir se realizó una capacitación al personal de informática sobre las políticas de seguridad que se deben adoptar para mantener un buen funcionamiento de sus mecanismos de defensa contra intrusos.

1.5 JUSTIFICACIÓN

En la actual administración central se está impulsando el manejo de las Tecnologías de la Información (TI) como una herramienta de inclusión al mundo tecnológico, es por ello que las organizaciones, tanto públicas como privadas están optando por utilizar a la Internet como su mejor arma para su desarrollo; pero esto también implica varios aspectos que se deben tener en consideración y la seguridad es uno de los primordiales con los que se debe lidiar, ya que se debe salvaguardar todo el tráfico de información que por la red vaya a cursar debido a que puede ser violentado y utilizado de forma maliciosa o existen personas inescrupulosas que buscan causar daño solo con el fin de medir su nivel de penetración hacia una red de datos.

Al ser el GAD Municipal del cantón Mira una entidad de carácter público que utiliza parte de su recurso de TI para brindar servicios interconectados no solo para otras dependencias, sino también para la ciudadanía, debe proporcionar un ambiente donde los datos que en muchas ocasiones son tratados de manera confidencial con la Institución deban mantenerse de esa manera, y esto solo se lo puede lograr conociendo las fortalezas y debilidades que su sistema de defensa posea en caso de propiciarse un ataque de hacking, ya que esta es una de las nuevas modalidades que se están utilizando para delinquir.

Una auditoría de red externa puede mostrar a una entidad los riesgos de seguridad que debe enfrentar y la manera de tratar con dichas amenazas para asegurar no solo su recurso de TI, sino la información confidencial de las personas que harán uso de ellos; para ello es necesario comprender que una auditoría no es una amenaza que desmerece los diseños aplicados en el desarrollo de un sistema, ya que ese no es el objetivo de una auditoría sino todo lo contario, permite asesorar al personal encargado del departamento informático de la existencia de fallas y errores para que se los tome en

cuenta y puedan ser resueltos de tal manera que este procedimiento no afecte al buen funcionamiento de entorno de la red.

Para un futuro profesional de la carrera de ingeniería en electrónica y redes de la comunicación es un reto poder aplicar sus conocimientos adquiridos en el proceso de formación profesional para contribuir no solo con la misión de la universidad, de formar profesionales comprometidos con su entorno social, sino también de aportar en lo posible para que su comunidad pueda disponer de servicios que brinden la tranquilidad que se merecen y además aportar con un granito de arena para mejorar la red de datos de una de las dependencias más importantes del cantón.

CAPÍTULO II

2. FUNDAMENTACIÓN TEÓRICA

2.1 DESCRIPCIÓN GENERAL

En este capítulo se desarrolló la fundamentación teórica con la que se pretende sustentar todo el trabajo del presente proyecto; para ello se describieron los principales aspectos sobre la seguridad informática, el procedimiento para realizar una auditoría de seguridad informática según el manual de metodologías OSSTMM en su versión 3 y aspectos básicos sobre el apartado de Seguridad de la Información del estándar COBIT versión 5, ya que éste se encuentra bajo licencia de ISACA y no se debe divulgar mucha información de su contenido.

2.2 INTRODUCCIÓN

En las últimas décadas la seguridad de la información en una organización ha sufrido dos cambios fundamentales. Antes de la expansión del uso de equipamiento de procesamiento de datos, la seguridad de la información que una organización consideraba valiosa se proporcionaba, por un lado, por medios físicos, como el uso de armarios con cerraduras para almacenar documentos confidenciales y, por otro lado, por medios administrativos, como los procedimientos de protección de datos del personal que se usan durante el proceso de contratación. (Stallings, 2 004, pág. 2)

Con la introducción del computador, se hiso evidente la necesidad de disponer de herramientas automatizadas para la protección de archivos y otros tipos de información almacenada en el mismo. Esto ocurre especialmente en el caso de sistemas compartidos; y la necesidad se palpa aún más en sistemas a los que se puede acceder por medio de una red telefónica pública, una red de datos o Internet. (Stallings, 2 004)

El segundo cambio que afectó a la seguridad informática fue la introducción de sistemas distribuidos, y el uso de redes y herramientas de comunicación para transportar datos entre el usuario de un terminal y un ordenador, y entre dos o más ordenadores. Las medidas de seguridad de la red son necesarias para proteger los datos durante la transmisión. Por otra parte, servicios críticos para una sociedad moderna, como: servicios financieros, el control de la producción y suministro eléctrico

(centrales eléctricas, redes de distribución y transformación); medios de transporte (control de tráfico aéreo, y de vías terrestres y marítimas); sanidad (historial clínico informatizado, telemedicina), las redes de abastecimiento (agua, gas y saneamiento) o la propia Administración Pública están soportados casi en su totalidad por sistemas y redes informáticas, hasta el punto de que en muchos de ellos se han eliminado o reducido en forma drástica los papeles y los procesos manuales (Stallings, 2 004).

De hecho, el término seguridad de la red es engañoso, ya que prácticamente todas las organizaciones, las instituciones gubernamentales y académicas conectan sus equipos de procesamiento de datos formando un grupo de redes conectadas entre sí y hacen uso de servicios telemáticos. Este grupo se considera con frecuencia como una internet[1], y se emplea el término seguridad de la internet. (Stallings, 2 004, pág. 2)

2.3 RED INFORMÁTICA

El término "red informática" es usado hace muchos años atrás para identificar a toda una estructura que combina métodos físicos y técnicos, necesarios para interconectar toda clase de equipos informáticos, con el propósito de lograr un intercambio efectivo de información en un entorno específico, ya sea laboral, personal o global. Las redes informáticas deben ser lo suficientemente efectivas para poder compartir todo tipo de información y recursos que estén disponibles en los dispositivos terminales a los que el usuario accede, proveyendo de herramientas para centralizar o distribuir, según se requiera, las diferentes necesidades informáticas que se pueda tener. (Kats, 2013, pág. 2)

Para fines prácticos, una red informática, no es más que un conjunto de componentes de hardware, conectados físicamente mediante un medio de transmisión, y configurados de una manera homogénea y sincronizada, que permiten establecer comunicaciones entre sí. Sin embargo, una red informática es mucho más de lo que se puede apreciar a primera vista. Detrás de toda la estructura visible se encuentra una gran cantidad de protagonistas intangibles que son los que permiten establecer correctamente esta conexión de componentes con éxito. Este grupo de protagonistas

[1] [internet] con "i" minúscula, para referirnos a cualquier grupo de redes conectadas entre sí. Una intranet corporativa es un ejemplo de internet. Internet con "I" mayúscula puede ser una de las herramientas que usa una organización para construir su internet. (Stallings, 2 004)

está formado por protocolos, servicios y diseños estructurales establecidos previo a la implementación de la propia red. (Kats, 2013, pág. 2)

Dentro de la separación de contextos que conforman una red, el primero es un contexto de diseño. Toda red puede ser categorizada según sus procesos dentro de una estructura de niveles (o capas) que engloban actividades de características similares, es importante resaltar que dicha categorización es completamente abstracta, y es establecida en una postura netamente de diseño. (Kats, 2013, pág. 3)

2.3.1 Funcionamiento general de una red.

El funcionamiento de una red informática, por más simple que parezca, es un proceso complejo. Las comunicaciones que fluyen naturalmente entre los equipos conectados dependen de cientos (o miles) de factores clave, que deben ponerse a punto al máximo detalle para lograr una comunicación exitosa. (Kats, 2013, pág. 5)

Cuando el usuario ve una impresora compartida, la selecciona desde su procesador de textos, le da la orden de impresión, y retira la hoja segundos después. Este proceso involucró a más de trecientas comunicaciones entre diferentes agentes intermediando en la red. Cada vez que se envía un mensaje que diga “hola” a un amigo a través de un sistema de mensajería instantánea, el envío de esa cadena de cuatro caracteres significó un intercambio de unas doscientas veces esa cantidad de información, entre todos los componentes que forman parte del proceso. (Kats, 2013, pág. 5)

Un usuario sin notarlo, ni saberlo, su información es trasladada por diferentes partes geográficamente separadas, pero correctamente conectadas entre sí, y complejamente configuradas de una manera que permita un flujo eficiente y rápido de información. Son justamente dichas configuraciones las que hacen una buena red, ya que gracias a ellas se puede contar con comunicasiones exitosas alrededor del planeta. (Kats, 2013)

2.4 SEGURIDAD DE LA INFORMACIÓN

Es común hablar de seguridad informática y de seguridad de la información como si fueran la misma cosa y, a primera vista, pareciera ser, sobre todo si se tiene en cuenta que en la actualidad, gracias al constante desarrollo tecnológico, se tiende a digitalizar todo tipo de información y manejarla a través de un sistema informático.

Sin embargo, aunque tengan la necesidad de trabajar en armonía, cada uno de estos aspectos tiene objetivos y actividades diferentes. (Toth, 2014, pág. 26)

Por seguridad informática se entiende al conjunto de políticas, reglas, estándares, métodos y protocolos que se utilizan para la protección de la infraestructura de computadoras y toda la información contenida o administrada por ella. No solo se debe prestar atención a los ataques intencionales, sino también a posibles fallas de software o hardware que atenten contra la seguridad, tratando de minimizar los riesgos asociados al acceso y utilización de un determinado sistema de forma no autorizada o malintencionada para revelar, utilizar, modificar o destruir accidental o intencionalmente la información que en él se encuentre. Para ello, se deben evaluar y cuantificar los bienes a proteger, y en función de este análisis, implantar medidas preventivas y correctivas que eliminen o reduzcan los riegos asociados hasta niveles manejables. (Toth, 2014, pág. 27)

Por otra parte, seguridad de la información se refiere a todas aquellas medidas que procuren resguardar la información ante cualquier irregularidad. La principal diferencia entre seguridad informática y seguridad de la información es que la primera se encarga de la seguridad en un medio informático y la segunda se interesa en la información en general, pudiendo ésta estar almacenada tanto en un medio informático como en cualquier otro. Por ejemplo, un manual de procedimientos escrito en papel, el conocimiento que poseen las personas, escrituras en pizarras y papeles que se descartan, son fuentes importantes de información. (Toth, 2014, pág. 27)

Se debe tener en cuenta que la seguridad de un sistema informático dependerá de diversos factores, (Gómez, 2011, pág. 39) destaca los siguientes:

- La sensibilización de los directivos y responsables de la organización.
- Los conocimientos, capacidades e implicación de los responsables del sistema informático.
- La mentalización, formación y la asignación de responsabilidades de todos los usuarios del sistema.
- La limitación en la asignación de los permisos y privilegios de los usuarios.

- La correcta instalación, configuración, mantenimiento y actualizaciones de los equipos, añadiendo a ello el soporte de los fabricantes de hardware y software.
- Contemplar no sólo la seguridad frente a las amenazas del exterior, sino también las amenazas procedentes del interior de la organización.

2.4.1 Conceptos básicos en materia de seguridad informática.

En materia de seguridad de la información e informática, es habitual manejar una terminología específica, mismos que se detallan a continuación:

2.4.1.1 *Activos.*

Se definen como un recurso del sistema (informático o no), necesario para que la organización alcance sus objetivos propuestos; es decir, todo aquello que tenga valor y que deba ser protegido frente a un eventual percance, ya sea intencionado o no. Según esta definición, se considera como activos: los trabajadores, el software, los datos, los archivos, el hardware, las comunicaciones, etc. (Escrivá, Romero, Ramada, & Onrabia, 2013, pág. 8 y 9) dice que desde el punto de vista informático, los principales activos de una organización son los siguientes:

2.4.1.1.1 Información.

Todo aquel elemento que contenga datos almacenados en cualquier tipo de soporte. Como por ejemplo, documentos, libros, patentes, correspondencias, datos de los empleados, datos de los usuarios, etc.

2.4.1.1.2 Software.

Programas o aplicaciones que utiliza la organización para su buen funcionamiento o para automatizar los procesos. Entre estos se pueden encontrar las aplicaciones comerciales, los sistemas operativos, firmwares[2], etc.

[2] [Firmware] Es un tipo de software que controla un dispositivo, pero a diferencia del software de aplicación el firmware se localiza en alguna memoria no volátil dentro de los dispositivos comunicándose con el sistema operativo y el dispositivo. (Aranda Vera, 2014)

2.4.1.1.3 Físicos.

Toda infraestructura tecnológica utilizada para almacenar, procesar, gestionar o transmitir toda la información necesaria para el buen funcionamiento de la organización. También estaría incluida en esta categoría la estructura física de la organización, tal como la sala de servidores, los racks de comunicaciones, los cuartos de telecomunicaciones, etc.

2.4.1.1.4 Personal de la organización.

Es toda persona que utiliza la estructura tecnológica y de comunicación para el manejo y procesamiento de la información.

2.4.1.2 *RAV.*

Es una medición a escala de una superficie de ataque, la cantidad de interacciones no controladas con un objetivo, se calcula por el equilibrio cuantitativo entre la porosidad, limitaciones y controles. En esta escala, 100 ravs o 100% rav, es un equilibrio perfecto, también pocos controles y, por tanto, una mayor superficie de ataque. Más de 100 ravs muestra que más controles son necesarios lo que a su vez puede ser un problema, ya que los controles a menudo añaden interacciones dentro de un alcance, así como cuestiones de complejidad y mantenimiento. (Herzog, 2010)

2.4.1.3 *Limitaciones.*

(Escrivá, Romero, Ramada, & Onrabia, 2013, pág. 9), dice que: En el campo de la seguridad informática se considera como una limitación a cualquier debilidad de un activo que pueda repercutir sobre el correcto funcionamiento de un sistema informático. Estas debilidades conocidas también como "agujeros de seguridad", pueden estar asociadas a fallos en la implementación de las aplicaciones o en la configuración de los sistemas operativos, descuidos en la utilización de los sistemas, etc. Por ejemplo, no utilizar ningún tipo de protección frente a fallos eléctricos o carecer de mecanismos de protección frente a ataques informáticos, como antivirus o cortafuegos[3].

[3] [cortafuegos] es un método de protección de la red LAN o de un ordenador concreto con el que se pueden abrir o cerrar determinados puertos, aplicaciones, direcciones IP, etc. (Bellido Quintero, 2014)

Es muy importante corregir cualquier limitación detectada o descubierta, porque constituye un peligro potencial para la estabilidad y seguridad del sistema en general. Las limitaciones de algunas aplicaciones pueden permitir una escalada de privilegios, con lo que un atacante podría conseguir más privilegios de los previstos. Esto podría implicar que en algunos casos llegarán a tener los mismos privilegios que los administradores, pudiendo controlar el sistema en su totalidad. Para minimizarlas, los administradores de los sistemas informáticos deben actualizar periódicamente el sistema operativo y las aplicaciones y mantenerse actualizados en temas relacionados con la seguridad de la información.

2.4.1.4 *Amenazas.*

Se representan a través de una persona, entidad, una circunstancia o evento, un fenómeno o una idea maliciosa, las cuales pueden provocar daño en los sistemas de información, produciendo pérdidas materiales, financieras o de otro tipo. Aunque hay amenazas que afectan a los sistemas de forma involuntaria, como por ejemplo, una inundación, un fallo eléctrico o una organización criminal o terrorista. Así, una amenaza es todo aquello que intenta o pretende producir daño. Las amenazas se suelen dividir en pasivas y activas. (López López, 2014)

2.4.1.4.1 Amenazas pasivas.

Se las conoce también como “escuchadas”. Su objetivo es obtener información relativa a una comunicación. Por ejemplo, los equipos informáticos portátiles que utilizan programas especializados para monitorizar el tráfico de una red Wi-Fi. (Escrivá, Romero, Ramada, & Onrabia, 2013, pág. 9)

2.4.1.4.2 Amenazas activas.

Tratan de realizar algún cambio no autorizado en el estado del sistema, por lo que son más peligrosas que las pasivas; por ejemplo: inserción de mensajes ilegítimos, usurpación de identidad, etc. Otra posible clasificación, en función de su ámbito de acción, consiste en diferenciar entre amenazas sobre la seguridad física, lógica, de comunicaciones o de los usuarios; una clasificación de las amenazas más comunes se muestra en la Tabla 1: (Escrivá, Romero, Ramada, & Onrabia, 2013, pág. 9)

Tabla 1: Clasificación de las amenazas

Grupos de amenazas	Ejemplos
Desastres naturales	Fuego, daños por agua, desastres naturales
Desastres industriales	Fuego, daños por agua, desastres industriales, contaminación mecánica, contaminación electromagnética, etc.
Errores y fallos no intencionados	Errores de usuario, errores de configuración, etc.
Ataques deliberados	Manipulación de la configuración, suplantación de la identidad del usuario, difusión de software dañino, etc.

Fuente: Elaboración propia. Recuperado de (Escrivá, Romero, Ramada, & Onrabia, 2013, pág. 9)

2.4.1.5 *Ataques.*

Un ataque es una acción que trata de aprovechar una limitación de un sistema informático para provocar un impacto sobre él e incluso tomar su control. Se trata de acciones tanto intencionadas como fortuitas que pueden llegar a poner en riesgo un sistema. (Escrivá, Romero, Ramada, & Onrabia, 2013, pág. 10), dice que normalmente un ataque informático pasa por las siguientes fases:

2.4.1.5.1 Reconocimiento.

Consiste en obtener toda la información necesaria de la víctima, que puede ser una persona o una organización.

2.4.1.5.2 Exploración.

Se trata de conseguir información sobre el sistema a atacar, como por ejemplo, direcciones IP, nombres de host, datos de autenticación, etc. En el caso de la ingeniería social, que consiste en la obtención de la información confidencial y/o sensible de un usuario mediante métodos que son propios de la condición humana. El ataque más simpe sería el de engañar al usuario haciéndose pasar por el administrador del sistema de su organización para obtener alguna información de relevancia.

2.4.1.5.3 Obtención de acceso.

A partir de la información descubierta en la fase anterior, se intenta explotar alguna vulnerabilidad detectada en la víctima para llevar a cabo el ataque.

2.4.1.5.4 Mantener el acceso.

Después de acceder al sistema, se buscará la forma de implantar herramientas que permitan el acceso de nuevo al sistema en futuras ocasiones.

2.4.1.5.5 Borrar las huellas.

Finalmente, se intentarán borrar las huellas que se hayan podido dejar durante la intrusión para evitar ser detectado. En el mercado existen una gran variedad de herramientas de seguridad que permiten conseguir un nivel óptimo de seguridad, pero hay estrategias de ataque que hacen ineficaces a dichas herramientas, como las orientadas a explotar las debilidades del factor humano.

2.4.1.6 *Seguridad Operacional.*

La Seguridad Operacional es una función de una separación. O bien existe la separación entre un activo y cualquier amenaza o no lo hace. (Herzog, 2010), menciona que existen 3 maneras lógicas y dinámicas para crear esta separación:

1. Mover el activo para crear una barrera física o lógica entre éste y las amenazas.
2. Cambiar la amenaza a un estado inofensivo.
3. Destruir la amenaza.

Cuando se analiza el estado de la seguridad operacional se puede ver donde existe la posibilidad de interacción y donde no lo hay. Sabemos que todas, algunas, o incluso ninguna de estas interacciones pueden ser necesarias para las operaciones. Dado que el analista de seguridad puede no saber en este momento la justificación de negocio para todos estos puntos interactivos, nos referimos a esto como la Porosidad. La porosidad reduce la separación entre una amenaza y un acceso. Se clasifica como uno de los 3 elementos, visibilidad, acceso, o confianza; para describir su función en las operaciones permitiendo que se añadan los controles adecuados durante la fase de remediación, y así mejorar la protección. (Herzog, 2010)

2.4.1.7 *Controles.*

Cuando la amenaza está en todas partes, entonces los controles son los que proporcionarán seguridad en las operaciones. Los controles son un medio para influir

en el impacto de las amenazas y sus efectos. Si bien hay muchos nombres y diferentes tipos de controles operacionales, sólo hay 12 categorías principales que contienen todos los posibles controles. No obstante dos de las categorías, Identificación (la verificación de una identidad existente), y Autorización (el otorgamiento de permisos de la autoridad competente), no puede estar solo en un entorno operativo, por lo tanto en las operaciones, se combinan y se añaden al control de Autenticación. Esto deja a la Seguridad Operacional con diez posibles controles, que un analista tendrá que identificar y comprender. Por lo tanto, (Herzog, 2010) dispone la siguiente clasificación:

2.4.1.7.1 Controles Interactivos.

Los Controles Interactivos o de Clase A constituyen exactamente la mitad de todos los controles operativos. Estos controles influyen directamente en las interacciones visibilidad, acceso, o confianza. Las categorías de Clase A son: autenticación, indemnización, resistencia, subyugación y continuidad. (Herzog, 2010)

- *Autenticación*

Es la garantía de la identidad del usuario que origina una información; permite conocer con certeza quién envía o genera una información específica. La identidad del emisor puede ser validada, de modo que se puede demostrar que es quien dice ser. (Merino & Cañizares, 2013, pág. 12)

Un control de acceso permite garantizar el acceso a los recursos, únicamente a las personas autorizadas, gracias a una contraseña codificada, la utilización de más de un método, aumenta la posibilidad de que la autenticación sea más robusta; pero esta decisión debe estar relacionada al valor de la información a proteger dentro de la organización. (Jaramillo Remache, 2014, pág. 5)

- *Indemnización*

Es un control a través de un contrato entre el propietario de los activos y la persona a interactuar. Este contrato puede ser en forma de una advertencia visible como un precursor de una acción legal si no se siguen las reglas publicadas, detalles, protección legislativa pública, o con un proveedor de garantía de terceros en caso de daños, como una compañía de seguros. (Herzog, 2010)

- *Resistencia*

Es un control sobre todas las interacciones para mantener la protección de los bienes en el caso de algún fracaso o atentado. (Herzog, 2010)

- *Subyugación*

Es un control que asegura que las interacciones se producen sólo en función de los procesos definidos. El propietario de los activos define cómo se produce la interacción que elimina la libertad de elección, sino también la responsabilidad de la pérdida de la persona que interactúa. (Herzog, 2010)

- *Continuidad*

Es un control sobre todas las interacciones para mantener la interactividad con los bienes en el caso de algún fracaso o atentado. (Herzog, 2010)

2.4.1.7.2 Controles de Proceso.

La otra mitad de los controles operativos son los controles de Clase B que se utilizan para crear procesos defensivos. Estos controles no influyen directamente en las interacciones sino que protegen los activos una vez que la amenaza está presente; son también conocidos como controles de procesos e incluyen el No repudio, la Confidencialidad, la Privacidad, la Integridad y la Alarma. (Herzog, 2010)

- *No repudio*

Este principio es necesario tenerlo asegurado para garantizar la comunicación en un sistema informático, es decir, que las comunicaciones entre un emisor y un receptor queden garantizadas y que ni el emisor ni el receptor pueden negar que ha existido. (Escrivá, Romero, Ramada, & Onrabia, 2013), dice que existen dos clases:

  - *No repudio de origen*

Protege al destinatario del envío, ya que este recibe una prueba de que el emisor es quien dice ser.

- *No repudio de destino*

Protege al emisor del envío, ya que el destinatario no puede negar haber recibido el mensaje del emisor

- *Confidencialidad.*

Es la garantía de que la información no es conocida por personas, organizaciones o procesos que no disponen de autorización. Según la definición de la OIE, la confidencialidad se refiere a "garantizar que la información es accesible solo para aquellos que han sido autorizados". En un sistema donde se garantice la confidencialidad, si un tercero es capaz de interceptar una comunicación entre el remitente y el destinatario, no podrá visualizar ningún tipo de información clara. (Toth, 2014, pág. 28)

Los principales mecanismos de protección de la confidencialidad en los sistemas de información son los controles de acceso y criptografía; como ejemplo de amenazas a la confidencialidad se tiene el malware, los intrusos, la ingeniería social, las redes inseguras y los sistemas mal administrados. (Jaramillo Remache, 2014, pág. 3)

- *Privacidad*

Es un control que asegura la manera de cómo se accede a un activo, y se muestra o intercambia la información entre las partes, por lo que no puede ser conocida fuera de dichas partes. (Herzog, 2010)

- *Integridad*

Es la garantía de que la información no se ha transformado ni modificado de forma no autorizada durante su procesamiento, transporte o almacenamiento; y además permite detectar fácilmente las posibles modificaciones que pudieran haberse producido, por lo tanto, la modificación de dicha información o recursos se realiza únicamente por los entes autorizados y mediante métodos autorizados. (Merino & Cañizares, 2013, pág. 12)

La integridad en el contexto de la seguridad de la información no solo se refiere a la integridad de la información en sí, sino también del origen; es decir, la integridad de la fuente de información. Los mecanismos de protección de la integridad se pueden

agrupar en dos grandes grupos: los mecanismos preventivos, como los controles de acceso que impiden la modificación no autorizada de la información y los mecanismos detectives, que están destinados a detectar modificaciones no autorizadas cuando los mecanismos de prevención han fallado. (Jaramillo Remache, 2014, pág. 4)

- *Alarma*

"Es la notificación apropiada y precisa de las actividades que violan o intentan violar cualquiera de las dimensiones de la seguridad. En la mayoría de violaciones de seguridad, la alarma es el único proceso que genera reacción". Es un control para notificar que una interacción está ocurriendo o ha ocurrido. (Herzog, 2010)

2.4.1.8 *Riesgo.*

Es la probabilidad de que una amenaza se materialice sobre una limitación del sistema informático, causando un determinado impacto en la organización. El nivel de riesgo depende, por lo tanto, del análisis previo de las limitaciones y amenazas del sistema, y del posible impacto que éstas puedan causar en el funcionamiento de la organización. (Gómez, 2011, pág. 63)

Para poder establecer procedimientos de seguridad informática adecuados, será necesario realizar una clasificación de los datos y un análisis de riesgos, con el fin de establecer prioridades y realizar una administración más eficiente de los recursos de la organización. En el análisis de riesgos hay que tener en cuenta qué activos se deben proteger, su seguridad operacional, limitaciones, controles y amenazas, así como la probabilidad de que éstas se produzcan junto con el impacto de las mismas; también habrá que tener en cuenta durante cuánto tiempo y qué esfuerzo y dinero se está dispuesto a invertir. Los resultados del análisis de riesgos permiten recomendar qué medidas se deberán tomar para conocer, prevenir, impedir, reducir o controlar los riesgos previamente identificados y así poder reducir al mínimo su potencialidad o sus posibles daños. (Escrivá, Romero, Ramada, & Onrabia, 2013)

2.4.1.9 *Impacto.*

Una organización se ve afectada cuando se produce una situación que atenta contra su funcionalidad; estas consecuencias para la organización reciben el nombre de impacto. Dicho de otra forma, el impacto sería el daño producido o causado en caso

de que una amenaza se materialice. Un impacto leve no afecta prácticamente al funcionamiento de la organización y se produce en organizaciones que han identificado las amenazas y han establecido las pautas a seguir en el caso de que se materialicen. Por otro lado, un impacto grave afecta seriamente a la organización pudiendo ocasionar su quiebra y se produce en organizaciones que no han considerado las consecuencias que supone para ellas la materialización de alguna amenaza. (Escrivá, Romero, Ramada, & Onrabia, 2013)

Para valorar el impacto es necesario tener en cuenta tanto los daños tangibles, como la estimación de los daños intangibles (incluida la información). En este sentido, podría resultar de gran ayuda la realización de entrevistas en profundidad con los responsables de cada departamento, función o proceso de la organización, tratando de determinar cuál es el impacto real de la revelación, alteración o pérdida de la información para la organización, y no sólo del elemento TIC que lo soporta. Tal como se muestra en la Tabla 2, se puede emplear una escala cuantitativa o cualitativa para medir el impacto del daño en la organización: Bajo, Moderado y Alto. (Gómez, 2011, pág. 62)

Tabla 2: Escala propuesta para medir el impacto en la organización

Alto	- Pérdida o inhabilitación de recursos críticos - Interrupción de los procesos de negociación - Daños en la imagen y reputación de la organización - Robo o revelación de información estratégica o especialmente protegida
Moderado	- Pérdida o inhabilitación de recursos críticos pero que cuentan con elementos de respaldo. - Caída notable en el rendimiento de los procesos de negociación o en la actividad normal de la organización. - Robo o revelación de información confidencial, pero no considerada estratégica
Bajo	- Pérdida o inhabilitación de recursos secundarios - Disminución del rendimiento de los procesos de negociación - Robo o revelación de información interna no publicada.

Fuente: Elaboración Propia. Recuperado de: (Gómez, 2011)

2.4.1.10 *Desastres.*

Según ISO 270001, un desastre es cualquier evento accidental, natural o malintencionado que interrumpe las operaciones o servicios habituales de una organización. Por ejemplo, la caída de un servidor como consecuencia de una subida de tensión o un ataque. Tradicionalmente se planteaba únicamente la destrucción de

recursos físicos, como sillas, edificios, etc.; pero hoy día las organizaciones se enfrentan a una nueva forma de desastre que afecta a los recursos lógicos, que constituye uno de sus principales activos: la información. Un desastre de este tipo podría ocasionar grandes pérdidas e incluso el cese de la actividad económica de la organización. (Escrivá, Romero, Ramada, & Onrabia, 2013, pág. 13)

2.4.2 Objetivos de la seguridad informática.

El objetivo de la seguridad informática es proteger los recursos informáticos valiosos de la organización, tales como la información, el hardware o el software, a través de la adopción de medidas adecuadas; ayuda a la organización a cumplir con su visión, protegiendo sus recursos financieros, sistemas, reputación, situación legal, y otros bienes tanto tangibles como inmateriales. Desafortunadamente, en ocasiones se ve a la seguridad informática como algo que dificulta la consecución de los propios objetivos de la organización, imponiendo normas y procedimientos rígidos a los usuarios, a los sistemas y a los gestores; sin embargo se la debe ver como un medio de apoyo a la consecución de los objetivos de la organización. (Galdámez, 2013)

(Gómez, 2011, pág. 41), dice que para cumplir con los objetivos de la seguridad informática, una organización debe contemplar cuatro planos de actuación:

- Técnico: tanto a nivel físico como a nivel lógico.
- Legal: algunos países obligan por Ley a que en determinados sectores se implanten una serie de medidas de seguridad.
- Humano: sensibilización y formación de empleados y directivos, definición de funciones y obligaciones del persona.
- Organizativo: definición e implantación de políticas de seguridad, planes, normas, procedimientos y buenas prácticas de actuación.

2.5 MODELOS DE SEGURIDAD INFORMÁTICA

2.5.1 Seguridad por oscuridad.

Es uno de los primeros modelos de seguridad que se aplicó en el campo informático, se denomina por oscuridad debido a que está basado en el desconocimiento u ocultamiento de lo que se desea proteger, en este caso, los recursos informáticos; este modelo funciona mientras realmente permanezca secreto u oculto, es decir que en la

práctica puede funcionar por un tiempo limitado, porque a largo plazo se va a descubrir y su seguridad posiblemente va a ser violentada. (Jaramillo Remache, 2014, pág. 5)

2.5.2 Perímetro de defensa.

Proteger el perímetro de la red es quizá lo más razonable para mantener a salvo la información y los sistemas de una red de los ataques externos. De esta manera se separa la red interna de la red externa con el único fin de proteger todos los puntos de acceso a la red, lo que se considera correcto y es la principal razón por la que este modelo sigue vigente en la actualidad. (Jaramillo Remache, 2014, pág. 5)

Los principales problemas a los que se atiene este modelo son: que no brinda la seguridad necesaria frente a los ataques que se produzcan desde la red interna y que no presenta un adecuado nivel de protección en caso de que un ataque se materialice y rompa la barrera de seguridad perimetral. (Jaramillo Remache, 2014, pág. 5)

2.5.3 Defensa en profundidad.

Consiste en el diseño e implantación de varios niveles de seguridad dentro del sistema informático de la organización. De este modo, si una de las "barreras" es franqueada por los atacantes, conviene disponer de medidas de seguridad adicionales que dificulten y retrasen el acceso a información confidencial o el control de recursos críticos del sistema: seguridad perimetral, seguridad en los servidores, auditorías y monitorización de eventos de seguridad, etc. (Gómez, 2011, pág. 51)

Aplicando este modelo también se reduce de forma notable el número de potenciales atacantes, ya que los aficionados y script kiddies[4] sólo se atreven a atacar a los sistemas informáticos más vulnerables y por tanto, más fáciles de penetrar. Por este motivo, no conviene descuidar la seguridad interna, de modo que no dependa todo el sistema de la seguridad perimetral (Gómez, 2011, pág. 51)

Los componentes de defensa en profundidad incluyen al software antivirus, cortafuegos, programas anti-spyware[5], contraseñas jerárquicas, detección de intrusos

[4] [script kiddies] Atacantes de sistemas informáticos aficionados. (Álvarez Marañón & Pérez García, 2000)

[5] [anti-spyware] detecta y elimina las aplicaciones de spyware y también evita las instalaciones futuras. (Bellido Quintero, 2014)

y verificación biométrica. Además de las contramedidas electrónicas, la protección física de los recursos informáticos, junto con la capacitación del personal integral y continuo, mejora la seguridad de los datos de cualquier peligro, robo o destrucción. (Jaramillo Remache, 2014, págs. 5, 6)

2.6 ATAQUES COMUNES BASADOS EN EL MODELO OSI

Muchas de las redes de comunicaciones basan su funcionamiento en el modelo de referencia OSI para la interconexión de equipos informáticos, que define siete capas o niveles tal como se muestra en la Figura 1, de manera que cada nivel tiene una funcionalidad bien definida y se comunica mediante una interfaz que oculta los detalles de implementación al resto de los niveles, facilitando su uso por los niveles inmediatamente inferior o superior, que son los únicos que podrán acceder a él, en la Tabla 3 se puede apreciar de mejor manera los diferentes tipos de ataques más comunes que se pueden suscitar en los diferentes niveles del modelo de referencia OSI. (Escrivá, Romero, Ramada, & Onrabia, 2013, pág. 175)

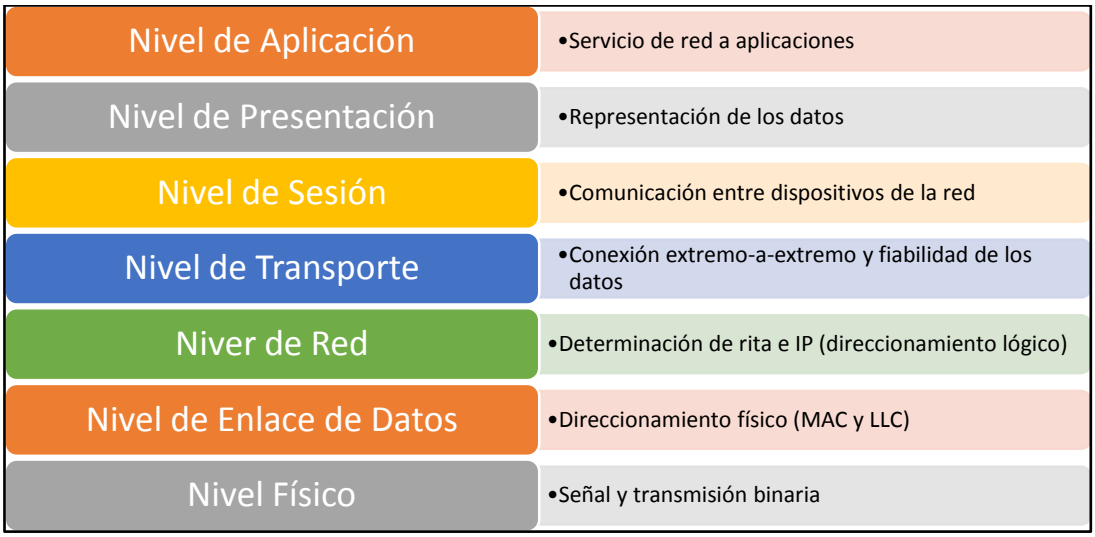


Figura 1: Pila del modelo OSI

Fuente: Elaboración propia. Recuperado de: (Escrivá, Romero, Ramada, & Onrabia, 2013).

Tabla 3: Ataques comunes basados en el modelo OSI

Nivel	Descripción	Ataque
Físico	Es responsable de la conexión del equipo informático a la red y se encarga de la transmisión de información a través de ella.	- Corte o desconexión de los cables de red. - Interferencias electromagnéticas ocasionadas por algún dispositivo. - Amenaza a las instalaciones
Enlace de Datos	Se encarga del direccionamiento físico, acceso al medio, la detección de errores, la distribución ordenada de tramas y del control de flujo.	- Escuchas de red, tanto intrusivas en medios cableados (pinchar un cable), como no intrusivas en medios inalámbricos (ataques WEP[6]) - Falsificación de direcciones MAC para evitar restricciones de acceso basadas en filtrado MAC. - Envenenamiento ARP[7].
Red	Proporciona conectividad entre equipos, permitiendo que la información llegue desde el origen al destino aunque se encuentren en redes diferentes. Esto se debe la información de cabecera que contienen todos los paquetes IP y a la utilización de elementos que permiten la interconexión de redes.	- Suplantación de mensajes - Denegación de servicio o DoS - Técnicas de sniffing - Falsificación de direcciones IP
Transporte	Este nivel proporciona un servicio de transporte desde la máquina origen a la de destino, independizándolo del hardware de red utilizado. Los protocolos más conocidos son TCP y UDP, que transmiten información sobre paquetes IP.	- Denegación de servicios sobre datagramas UDP, TCP o ICMP[8]. - Inundación SYN - Ataques contra el establecimiento de sesiones TCP - Ataques de reconocimiento - Desviación del tráfico
Sesión, Presentación y Aplicación	Estos niveles desconocen la forma en la que se comunican los equipos y la ruta establecida y se encargan de definir los protocolos de aplicación que utilizan las aplicaciones finales para intercambiar datos.	- Ataques a la confidencialidad - Suplantación del servicio de nombres de dominio - Agotamiento de direcciones IP - Inyección SQL - Escala de directorios - Cross Site Scripting (XSS) - Desbordamiento de búfer - Telnet

Fuente: Elaboración Propia. Recuperado de: (Escrivá, Romero, Ramada, & Onrabia, 2013)

[6] [WEP] Wired Equivalent Privacy. Estándar de seguridad para redes Wi-Fi. (Gutierrez, 2015)

[7] [ARP] Address Resolution Protocol, protocolo que permite determinar la dirección física de un equipo en la red, cuando sólo se conoce su dirección lógica (o dirección IP). (Kats, 2013)

[8] [ICMP] Internet Control Message Protocol, su función principal es establecer diagnósticos de comunicación entre dos equipos. (Kats, 2013)

2.7 AUDITORÍA DE SEGURIDAD INFORMÁTICA

2.7.1 Introducción

La seguridad informática es un proceso dinámico que no finaliza cuando se han implementado distintas medidas de seguridad informática en una organización. Es necesario evaluar si el sistema de seguridad informática que se ha adoptado está cumpliendo con su función y mejorarlo si fuera necesario. (Escrivá, Romero, Ramada, & Onrabia, 2013, pág. 188)

Por otra parte, los dueños de la información se ven obligados a capacitarse constantemente para poder estar un paso adelante y resguardar los datos ante cualquier incidente posible, ya que un sistema que un día era seguro, con el paso del tiempo, si no se va actualizando en materia de seguridad, puede presentar fallos. Con este fin se realizan auditorías de seguridad informática en las organizaciones. (Toth, 2014)

Realizar auditorías con cierta frecuencia asegura la integridad de los controles de seguridad aplicados a los sistemas de información. Acciones como el constante cambio en las configuraciones, la instalación de parches, actualización del software y la adquisición de nuevo hardware hacen necesario que los sistemas estén continuamente verificados mediante auditoría. (Costas Santos, 2010, pág. 295)

2.7.2 Concepto de auditoría de seguridad informática

Una auditoría de seguridad informática es el estudio que comprende el análisis y gestión de los sistemas informáticos, realizado por una persona o grupo de personas, denominados auditores, que pueden ser del propio personal o ajeno a la organización; para identificar y posteriormente corregir las diversas vulnerabilidades que se pudieran presentar en una revisión exhaustiva de las estaciones de trabajo, redes de comunicaciones o servidores. (Costas Santos, 2010)

Las auditorias de seguridad informática en el momento de su realización permiten conocer cuál es la situación exacta de sus activos de información en cuanto a protección, control y medidas de seguridad operacional y así mejorar la rentabilidad y la eficacia de todo el sistema en general, mediante la exposición de las debilidades y disfunciones que se van encontrando en el proceso, para luego levantar un informe

final donde se indica los planes de acción para eliminar dichas falencias a modo de recomendaciones. (Costas Santos, 2010)

2.7.2.1 *Fases de una auditoría de seguridad informática.*

Para elegir un tipo de prueba adecuado, lo mejor es entender primero cómo sus módulos están diseñados para trabajar. Dependiendo de la minuciosidad, negocio, asignación de tiempo y los requisitos de la auditoría, el analista puede programar los detalles de la misma realizada por fases, en la metodología OSSTMM versión 3 hay cuatro fases en su ejecución: Fase de Inducción, de Interacción, de Indagación y de Intervención. (Herzog, 2010)

2.7.2.1.1 Fase de Inducción.

Cada viaje comienza con una dirección. En la fase de inducción, el analista comienza la auditoría entendiendo los requisitos, el alcance y las limitaciones de la auditoría en dicho alcance. A menudo, el tipo de prueba se determina mejor después de esta fase. (Herzog, 2010)

La documentación para la auditoría de seguridad informática es el registro continuo de todas las tareas realizadas por el auditor. De este modo, con los documentos aportados por el auditor, se da soporte a aspectos importantes como las evidencias encontradas, las debilidades detectadas que requieren revisión y las conclusiones del auditor obtenidas a raíz de los resultados de la auditoría. Estos documentos se denominan también “papeles de trabajo” y deben ser complementados no solo en la redacción del informe de la auditoría, sino que deben elaborarse a lo largo de todas las fases de la auditoría. Para una correcta documentación del proceso de la auditoría, se recomienda la organización de los papeles de trabajo en dos tipos de archivos distintos: archivo permanente y archivo corriente. (Chicano Tejada, 2014, pág. 270)

2.7.2.1.2 Fase de Interacción.

Para que la auditoría de seguridad se desarrolle correctamente, será necesario elaborar un plan de auditoría. El objetivo de esta planificación es la recopilación de información de la organización y de sus sistemas informáticos para obtener una información global del área a auditar. La recopilación de información se deberá realizar a través de observaciones, entrevistas con los agentes que interactúan con el

sistema y con la solicitud de documentos e información a los responsables de la organización. Con esto, el auditor ya será capaz de definir concretamente el objetivo general del estudio, el alcance que la auditoría deberá tener y el programa desarrollado de las tareas de auditoría. (Chicano Tejada, 2014, pág. 282)

El plan de auditoría deberá señalar detalladamente el objetivo, el alcance y la dirección de la misma y deberá comprender también un plan de trabajo por si se produce algún cambio o modificación inesperada al plan general, estos se documentan debidamente en el plan de auditoría general. Si se tienen claros los objetivos, la metodología y el alcance de la auditoría del sistema a evaluar, ya se puede proceder a realizar una prueba de seguridad. Según (Chicano Tejada, 2014, pág. 283) los pasos a realizar en la elaboración del plan de auditoría son:

1. Identificación del origen de la auditoría.
2. Realización de una visita preliminar al área/organización que será auditada.
3. Establecimiento de los objetivos generales de la auditoría.
4. Determinación de los puntos y elementos a evaluar.
5. Elaboración de planes y presupuestos para la realización de las tareas de auditoría.
6. Identificación y selección de los métodos, herramientas, utilidades y procedimientos que van a ser necesarios a lo largo de la auditoría.
7. Asignación de los recursos materiales y técnicos necesarios para el desarrollo de las tareas.

2.7.2.1.3 Fase de Indagación.

Cuando ya se ha completado la fase de interacción de la auditoría de seguridad informática, el siguiente paso es indagar. La fase de indagación consiste en la realización de una serie de pruebas cuyos resultados permitan detectar debilidades y fortalezas del sistema de información auditado y justifiquen la detección de las evidencias. (Chicano Tejada, 2014, pág. 290)

- *Tipos de pruebas*

Para la obtención de las evidencias, se pueden utilizar varios tipos de pruebas, técnicas y procedimientos, (Chicano Tejada, 2014, pág. 290) recomienda los se describen a continuación:

- *Cuestionarios*

Para obtener información que justifique las evidencias detectadas, el auditor debe enviar una serie de cuestionarios a personas concretas y adecuadas, sin que estas sean de obligatorio cumplimiento.

- *Entrevistas*

Después de la primera toma de contacto, el auditor debe recabar información más detallada de tres formas: con la petición de documentación específica, con entrevistas abiertas sin guion preestablecido y con entrevistas predeterminadas y guionizadas.

- *Checklist*

Aparte de comprobar el funcionamiento del sistema probado, el auditor debe someter al auditado a un cuestionario llamado checklist, el que debe ser perfectamente comprensible para el auditado, de modo que las respuestas expresadas reflejen claramente la situación actual del sistema de información. Se recomienda que las checklists sean respondidas oralmente, no por escrito. Cabe destacar dos tipos de checklist, el de rango y el binario.

Las checklists de rango están formadas por una serie de preguntas a las que el auditor debe responder dentro de un rango preestablecido. Según la puntuación del rango obtenida, ya se hacen más específicas sobre los motivos de la puntuación. Sin embargo, la checklist binaria está formada por preguntas de respuesta única y excluyente: sí o no. Es necesario que las preguntas sean muy precisas para que los resultados obtenidos sean claros y exactos.

- *Comparación de programas*

La comparación de programas consiste en la correlación de una versión de una aplicación determinada en ejecución con otra versión de la misma aplicación modificada a propósito para detectar las diferencias.

- *Mapeo y rastreo de programas*

Con aplicaciones especializadas, se analizan los programas que se están ejecutando en ese momento, indicando información específica sobre el procesamiento de la información y las variables de memoria utilizadas.

- *Datos de prueba*

Con la utilización de los datos de prueba se preparan una serie de transacciones y operaciones con datos correctos e incorrectos para comprobar si los controles internos funcionan debidamente.

- *Software de auditoría*

En la actualidad, existen en el mercado programas y aplicaciones específicos para la realización de auditorías externas que ayudan al auditor a realizar la gran mayoría de pruebas descritas anteriormente.

2.7.2.1.4 Fase de Intervención.

Estas pruebas se centran en los recursos de los objetivos requeridos en la aplicación, mismos que se pueden intercambiar, cambiar, sobrecargar, o morir a causa de la penetración o interrupción. Esto es a menudo la fase final de una prueba de seguridad para asegurar que las interrupciones no afecten a las respuestas de las pruebas menos invasivas y porque la información para hacer estas pruebas no puede ser conocida hasta que otras fases se han llevado a cabo. (Herzog, 2010)

El informe de auditoría es el documento escrito que refleja los resultados obtenidos a través de las pruebas de la auditoría junto con sus conclusiones, observaciones, sugerencias y recomendaciones realizadas por el auditor. Es muy importante realizar correctamente este informe, ya que es el reflejo de todo el trabajo realizado por el auditor dentro de la organización. (Chicano Tejada, 2014, pág. 295)

- *Documentos específicos*

(Chicano Tejada, 2014), dice que se debe presentar particularmente tres documentos específicos: carta de envío, resumen ejecutivo e informe final de auditoría.

- *Carta de envío*

La carta de envío debe ser la presentación del auditor, es imprescindible que se muestre la profesionalidad del auditor y que tiene un extenso conocimiento, tanto en

la materia auditora como en la organización que se ha estado evaluando. (Chicano Tejada, 2014, pág. 296)

- *Resumen ejecutivo*

El resumen ejecutivo incluirá los aspectos generales de la auditoría. Más específicamente, (Chicano Tejada, 2014, pág. 296) recomienda que deberá contener:

1. Antecedentes.
2. Fundamento legal y normativa.
3. Objetivos y alcance de la auditoría.
4. Procedimientos relevantes utilizados y limitaciones encontradas
5. Resumen breve de los resultados de la auditoría.
6. Identificación de los hechos que deben originar responsabilidades.
7. Comentarios de la organización sobre la aceptación del informe de auditoría.

- *Informe de auditoría informática*

Esta parte del informe es la que debe contener la información importante sobre el desarrollo de las tareas de auditoría, los resultados obtenidos y las recomendaciones y sugerencias del auditor. (Herzog, 2010), recomienda que en este documento se deberá incluir, como mínimo:

1. Fecha y hora de la prueba.
2. Duración de la prueba.
3. Los nombre de los analistas responsables.
4. Tipo de prueba.
5. Alcance de la prueba
6. Índice (método de la enumeración del objetivo)
7. Canal probado
8. Prueba de vector
9. Métrica de la superficie de ataque
10. ¿Qué pruebas se han completado, desconocido o parcialmente terminado, y en qué medida?
11. Cualquier problema con respecto a la prueba y la validez de los resultados
12. Cualquier proceso que influya en las limitaciones de la seguridad
13. Cualquier incógnita o anomalía

2.7.3 Tipos de auditoría de seguridad informática

Las auditorías de seguridad informática se pueden clasificar en distintos tipos, atendiendo a criterios como el lugar desde el que se realiza la auditoría o cuáles son los objetivos en los que se centra la auditoría. De esta forma, se puede realizar la siguiente clasificación:

2.7.3.1 *Auditoría de seguridad interna.*

En este tipo de auditoría se realiza un análisis de riesgos, amenazas, vulnerabilidades e impactos desde dentro de la organización sin tener en cuenta los riesgos y amenazas desde Internet. En este tipo de auditoría se contrasta el nivel de seguridad y privacidad de las redes locales y corporativas de carácter interno. (Escrivá, Romero, Ramada, & Onrabia, 2013)

2.7.3.2 *Auditoría de seguridad perimetral y de DMZ.*

Se realiza desde Internet, fuera del perímetro de seguridad de la organización, con el objetivo de evaluar el grado de protección de la organización frente a ataques externos. Se evalúa tanto la protección de la red interna, como de la DMZ (zona desmilitarizada), que es donde se ubican los servidores de la organización que ofrecen servicios a Internet (DNS, web, correo, FTP, etc.) Se utilizan distintos tipos de ataques contra la red comprobando si esta es vulnerable, con previo aviso a la organización del momento en que se va a llevar a cabo la auditoría. (Escrivá, Romero, Ramada, & Onrabia, 2013, pág. 189)

2.7.3.3 *Test de intrusión.*

Consiste en un método de auditoría mediante el cual se intenta acceder a los sistemas para comprobar el nivel de resistencia a una intrusión no deseada. Se utiliza una base de datos de vulnerabilidades conocidas para automatizar el análisis y generar un informe con las vulnerabilidades encontradas. Es un complemento fundamental para la auditoría perimetral. (Escrivá, Romero, Ramada, & Onrabia, 2013, pág. 189)

2.7.3.4 *Auditoría de aplicaciones.*

Conocida también como análisis externo de la web, en este tipo de auditoría solo se testean y evalúan las aplicaciones de la organización, sin tener en cuenta los servidores, dispositivos de red o sistemas operativos. Se hacen pruebas como el desbordamiento de búfer, inyección SQL, verificación de la existencia y anulación de las posibilidades de Cross Site Scripting (XSS)[9], la escalada de directorios, etc. (Escrivá, Romero, Ramada, & Onrabia, 2013, pág. 189)

2.7.3.5 *Análisis forense.*

Es una auditoría que se realiza cuando los sistemas ya han sido atacados y comprometidos. En este caso, se separa la máquina atacada de la red y se analiza en detalle para ver qué es lo que ha ocurrido y poder evitar ataques similares en el futuro.

El análisis forense es una metodología de estudio ideal para el análisis posterior de incidentes mediante el cual se trata de reconstruir cómo se ha penetrado en el sistema, a la vez que se valoran los daños ocasionados. Si los daños han provocado la inoperatividad del sistema, este análisis se denomina análisis post mórtem. (Escrivá, Romero, Ramada, & Onrabia, 2013, pág. 189)

2.7.4 Herramientas y técnicas para auditorías de seguridad informática

A continuación, se comentan algunas de las herramientas y técnicas que utilizan los auditores de seguridad informática para realizar auditorías en una organización.

2.7.4.1 *Enumeración de redes.*

Su objetivo es identificar las redes IP asociadas a una organización y descubrir sus servidores. Esta información se puede obtener públicamente con herramientas como whois o el propio servicio DNS. La enumeración de redes sirve de base para el rastreo masivo de la red. (Escrivá, Romero, Ramada, & Onrabia, 2013, pág. 190)

[9] [Cross Site Scripting] Tipo de inyección de código malicioso, generalmente JavaScript, en las páginas web visitadas, cuyo objetivo es dejar libre a la máquina que lo origina y atacar al resto de usuarios que acceden a dichos servicio web. (Ramos Varón, Barbero Muñoz , Martínez Sanchez, García Moreno, & Gonzáles Nava, 2015)

2.7.4.2 *Rastreo de redes.*

Su objetivo es obtener información más detallada a partir de la conseguida en la enumeración. Sirve de base para el análisis de vulnerabilidades. Una de las herramientas más utilizadas para realizarlo es nmap, del que existen versiones para varios sistemas operativos como GNU/Linux o Windows. Sus técnicas son: barrido de direcciones IP con ICMP, barrido de puertos TCP y UDP, identificación del sistema operativo y aplicaciones. (Escrivá, Romero, Ramada, & Onrabia, 2013, pág. 190)

2.7.4.3 *Barrido de puertos.*

Un barrido de puertos trata de identificar qué puertos TCP y UDP están abiertos en un ordenador para poder aprovechar ciertos servicios que dependen de ellos para entrar en el sistema. Existe una gran variedad de herramientas de barrido de puertos accesibles en la red, una de las herramientas más conocidas para hacer barridos de puertos es NMAP. (Escrivá, Romero, Ramada, & Onrabia, 2013, pág. 190)

2.7.4.4 *Fingerprinting.*

Son técnicas que sirven para identificar el sistema operativo y las versiones de las aplicaciones que se están usando en los servidores. Además de las utilidades ya expuestas, NMAP también es una excelente herramienta para realizar esta técnica. Con un analizador de protocolos como Wireshark, también se puede identificar la versión de una aplicación como, por ejemplo, la versión de un servidor web cuando se le hace una petición web. (Escrivá, Romero, Ramada, & Onrabia, 2013, pág. 190)

2.7.4.5 *Análisis de vulnerabilidades.*

El objetivo de esta técnica es detectar debilidades en el sistema informático de la organización y corregirlas. Las debilidades se contrastan contra enormes bases de datos de vulnerabilidades donde se encuentran todas perfectamente definidas y catalogadas. Para el análisis de vulnerabilidades se pueden utilizar herramientas muy diversas, como por ejemplo, Nessus, entre otras. (Escrivá, Romero, Ramada, & Onrabia, 2013, pág. 190)

2.7.4.6 *Test de penetración.*

Los test de penetración, test de intrusión o pentest podría definirse como un conjunto de pruebas cuya finalidad es la de evaluar la efectividad de los protocolos de seguridad de los servicios informáticos y telemáticos de una organización. En el caso de encontrar vulnerabilidades, se intentará explotarlas. Entre los objetivos que se quieren conseguir, (Ramos Varón, Barbero Muñoz , Martínez Sanchez, García Moreno, & Gonzáles Nava, 2015) cita los siguientes:

- Evadir las medidas de seguridad existentes para conseguir extraer información sensible a la que no se debería tener acceso.
- Determinar si es posible provocar una denegación de servicio en redes y aplicaciones.
- Detectar vulnerabilidades no conocidas; por ejemplo, mediante técnicas de fuzzing[10].

Dependiendo del nivel de información de partida a la hora de realizar el test de penetración, (Ramos Varón, Barbero Muñoz , Martínez Sanchez, García Moreno, & Gonzáles Nava, 2015, pág. 16) establece la siguiente clasificación:

2.7.4.6.1 Caja Negra.

No se dispone inicialmente de información interna sobre el objetivo. Por tanto, se intenta emular un posible ataque realizado por alguien ajeno a la organización. En este caso, el atacante deberá recabar información sobre la víctima a partir de fuentes públicas de información. Entre los ataques que se realizarán, se encuentran aquellos relacionados con la inyección de código malicioso, búsqueda de configuraciones incorrectas de aplicaciones y servicios, utilización de exploits[11] y desbordamiento de memoria en aplicaciones, así como escaneo y ataques a las redes.

2.7.4.6.2 Caja Blanca.

El auditor dispondrá de total información sobre el sistema que se va a auditar. Esto incluye acceso a cuentas con distintos niveles de privilegios, códigos fuentes de aplicaciones y conocimiento de la arquitectura de red del objetivo. Aquí, los ataques

[10] [fuzzing] Envíos automáticos de datos al sitio web que se desea analizar. (Chicano Tejada, 2014)
[11] [exploits] Son programas que aprovechan una vulnerabilidad del sistema para atacarlo. (Fernández López, 2015)

que se van a realizar prestarán especial atención en revisar posibles vulnerabilidades en el código de las aplicaciones, en la configuración de los servicios, en el mantenimiento de contraseñas y protocolos de cifrado, etc.

2.7.4.6.3 Caja Gris.

Esta modalidad puede considerarse como una mezcla de las dos anteriores. Uno de los objetivos que se busca cubrir es cómo podría producirse una fuga de información realizada desde dentro de la organización, utilizando técnicas de caja negra pero disponiendo de conocimiento interno del objetivo.

2.7.5 Necesidad de aplicar una Metodología

Dada la importancia y el crecimiento de las auditorías de seguridad informática se ha hecho totalmente necesario una estandarización de la industria de tal modo que ayude a proveedores y clientes a entenderse, según (López Santoyo, 2015), esto se debe a la necesidad de:

- Estandarizar la terminología para los distintos niveles de auditorías de seguridad que se pueden realizar. Esto permite que el cliente pueda entender y conocer exactamente cuál es el servicio que contrata y lo que puede esperar de él.
- Una estructura de informe y del contenido de éste, de tal forma que si se realizan dos revisiones de seguridad por dos empresas, se puedan comparar de forma sencilla los resultados y evaluar si ha mejorado el estado global de la seguridad o no. Para esto ayuda mucho el uso de métricas.
- Que la auditoría sea válida en el cumplimiento de una regulación. Por ejemplo, las empresas que realizan transacciones bancarias, es decir, que manejen la información de las tarjetas de sus clientes deben cumplir el estándar PCI DSS (Payment Card Industry Data Security Standard), donde uno de los puntos que hay que cumplir para superar éste, es el de realizar un análisis de vulnerabilidades.

A la hora de realizar un análisis de seguridad hay tantas variables que afectan y tantas cosas que se deben tomar en cuenta, por lo que este trabajo se hace muy complicado de realizar sin tener una metodología. Hay muchas razones que hacen

necesaria la existencia y uso de metodologías. (López Santoyo, 2015), menciona las siguientes:

- Promueven un orden adecuado de las pruebas que se deben realizar.
- Cubren toda la variedad de pruebas que se deben realizar.
- Facilitan en gran medida las tareas del analista.
- Los resultados se trasladan al cliente de una forma más organizada y sistematizada, y por tanto organizada.
- Ayuda a realizar el proceso de la auditoria de una forma ética y legal.

2.8 COBIT 5 PARA LA SEGURIDAD DE LA INFORMACIÓN

2.8.1 Introducción

Fundada en 1969, ISACA es una organización independiente y sin fines de lucro que desarrolla estándares internaciones de control y auditoría de seguridad de sistemas de información (SSII) y avala habilidades y conocimientos en TI mediante sus mundialmente reconocidos certificados. ISACA tiene todos los derechos reservados de todos los productos de COBIT por lo que constantemente actualiza el marco de referencia COBIT, el cual ayuda a los profesionales de TI y líderes de las organizaciones a llevar a cabo sus responsabilidades en la gestión y gobierno de TI, particularmente en las áreas de aseguramiento, seguridad, riesgo y control y proporcionar valor al negocio. (ISACA, 2012, pág. 2)

2.8.2 Motivos para utilizar COBIT

COBIT 5 para Seguridad de la Información pretende ser una norma de trabajo "paraguas" para conectarse con otras normas, buenas prácticas y estándares de seguridad de la información, describe la universalidad de la seguridad de la información a lo largo de toda la organización y provee normas genéricas de catalizadores; pero otras publicaciones también pueden ser de ayuda ya que desarrollan aspectos más concretos, por ejemplo, prácticas para la seguridad de la información o guías de configuración. Las normas, buenas prácticas y estándares relevantes para seguridad de la información necesitan ser adaptados para encajar en requerimientos específicos en el entorno de la organización. El auditor puede entonces decidir, sobre la base de las necesidades específicas de la organización, qué norma o combinación de

normas es mejor utilizar, teniendo también en consideración la situación heredada, la disponibilidad de las normas y otros factores. (ISACA, 2012, pág. 59)

Los motivos más importantes para el desarrollo de COBIT 5 para Seguridad de la Información incluyen: (ISACA, 2012, pág. 13)

- La necesidad de describir la seguridad de la información en el contexto de una organización incluyendo:
    a) Las responsabilidades funcionales de principio a fin de seguridad de la información para el negocio y TI.
    b) Todos los aspectos que llevan a un gobierno y gestión efectivos de la seguridad de la información, tales como estructuras organizativas, políticas y culturas.
    c) La relación y enlace de la seguridad de la información con los objetivos de la organización.
- Una necesidad creciente de la organización de:
    a) Mantener el riesgo de información a un nivel aceptable y protegerla contra divulgaciones no autorizadas, modificaciones involuntarias o no autorizadas y posibles intrusiones.
    b) Asegurar que los servicios y sistemas se encuentran disponibles continuamente para los grupos de interés internos y externos, con el objetivo de satisfacer a los usuarios en relación al compromiso y los servicios proporcionados por TI.
    c) Cumplir con el número creciente de leyes y regulaciones relevantes, así como con requisitos contractuales y políticas internas para la seguridad y protección de la información y sistemas y proporcionar transparencia sobe el nivel de cumplimiento.
    d) Alcanzar todo lo anterior a la vez que se contiene el coste de servicios de TI y la protección de la tecnología.
- La necesidad de conectarse y, cuando sea relevante, alinearse con otras normas y estándares importantes en el mercado. El mapeo no exhaustivo ayudará a los grupos de interés a entender la relación entre los diferentes normas, buenas prácticas y estándares, además de cómo pueden ser usados de forma conjunta y complementarse bajo el paraguas de COBIT 5 para Seguridad de la Información.

Además de estos motivos principales para el desarrollo de COBIT 5 para Seguridad de la Información está el hecho de que la seguridad es esencial en las operaciones diarias de las organizaciones. Las brechas en la seguridad de la información pueden llevar a un impacto sustancial en la organización, por ejemplo debido a daños financieros u operativos. Adicionalmente, la organización puede estar expuesta a impactos externos como riesgos de reputación o legales, que pueden poner en peligro las relaciones con clientes y empleados, e incluso la supervivencia de la organización. (ISACA, 2012, pág. 15)

2.8.3 Contenido

(ISACA, 2012), describe cada sección y su interrelación con otras de esta manera:

- Sección I: profundiza en el tema de seguridad de la información y describe brevemente cómo la arquitectura de COBIT 5 puede ser adaptada a necesidades específicas de seguridad de la información; además proporciona una base conceptual que es utilizada en el resto de la publicación.
- Sección II: profundiza en el uso de los catalizadores de COBIT 5 para implementar seguridad de la información. En esta sección se introduce el concepto de catalizadores específicos para seguridad, los cuales se explican utilizando ejemplos prácticos.
- Sección III: Profundiza en cómo adaptar COBIT 5 para seguridad de la información a un entorno organizacional. Esta sección contiene guías de cómo se pueden implementar las iniciativas de seguridad de la información y proporciona un mapeo con otros estándares y normas dentro del área de seguridad de la información y COBIT 5 para Seguridad de la Información.

Los apéndices contienen guías detalladas basadas en los catalizadores introducidos en la sección II: (ISACA, 2012, pág. 17)

- Apéndice A: Guía detallada acerca de los principios, políticas y normas catalizadores
- Apéndice B: Guía detallada acerca de los procesos catalizadores
- Apéndice C: Guía detallada acerca de las estructuras organizativas catalizadoras

- Apéndice D: Guía detallada acerca la cultura, ética y comportamientos catalizadores
- Apéndice E: Guía detallada acerca de la información catalizadora
- Apéndice F: Guía detallada acerca de los servicios, infraestructura, y aplicaciones catalizadoras
- Apéndice G: Guía detallada acerca de las personas, habilidades y competencias catalizadoras.
- Apéndice H: Mapeos detallados de COBIT 5 para Seguridad de la Información con otros estándares de seguridad de la información.

2.8.4 Ventajas de COBIT para la Seguridad de la Información

En la tabla 4 se muestra una comparación de las principales ventajas de COBIT 5 para la Seguridad de la Información, frente a ITIL (Information Technology and Infrastructure Library)

Tabla 4: Comparación entre COBIT el ITIL

	COBIT	**ITIL**
Última versión	Versión (año 2012)	Versión 3 (año 2011)
País de creación	Estados Unidos	Reino Unido
Organización que la sustenta	ISACA Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información)	Agencia Central de Telecomunicaciones y Computación del Gobierno Británico (Central Computer and Telecommunications Agency CCTA)
Trayectoria	Desde el año 1969	Nació en la década de 1980
Descripción	Es un marco de referencia integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas.	Es un marco de trabajo de las buenas prácticas destinadas a facilitar la entrega de servicios de tecnologías de la información (TI).
Público al que va dirigido	Directores y gerentes de seguridad de la información, otros profesionales y grupos de interés dentro de la	Únicamente al personal directivo, gerencial y operativo de los departamentos de TI que estén directa o indirectamente involucrados con la prestación y soporte de servicios de TI.

Continúa ⟶

	organización, incluyendo terceras partes.	
Enfoque	Táctico, es más completo y sistemático	Operacional, se centra en la gestión del servicio
Cuál elegir	En la práctica, por lo general un consultor se dirige a COBIT en primer lugar, para evaluar, formular, definir, justificar y auditar	En segundo lugar, viene ITIL, cuando se necesitan más detalles, o cuando necesito la autoridad del o de los directivos para justificar lo que sugiero
Relación costo-beneficio	Mejor gestión de los costos relacionados con la función de seguridad de la información	Evalúa los costos asociados a la prestación de servicios

Fuente: Elaboración Propia

2.9 OSSTMM VERSIÓN 3

2.9.1 Introducción

OSSTMM es un manual de metodologías para pruebas y análisis de seguridad realizado siguiendo la metodología OML (Open Methodology License), siendo el manual en sí publicado bajo licencia Creative Commons 3.0; permitiendo el libre uso y distribución del mismo. Como proyecto de Software Libre, permite a cualquier analista de seguridad contribuir a la mejora del manual lo cual, además, garantiza pruebas de seguridad más eficaces, eficientes y procesables. (Opentesting, 2010)

La metodología OSSTMM se centra en los detalles técnicos de los elementos que necesitan ser comprobados, qué hacer antes, durante y después de las pruebas de seguridad, así como evaluar los resultados obtenidos. Las pruebas que recoge el manual incluyen todos los canales de operación: humanos, físicos, medios inalámbricos, telecomunicaciones, redes de datos y cualquier otra descripción derivada de una métrica real. Busca establecer un método científico para el análisis de la seguridad, evitando basarse en la experiencia y subjetividades del analista, tratando de realizar una medición de la seguridad en un ambiente operativo, teniendo en cuenta los controles, en las interacciones y limitaciones que éstos puedan presentar. (Toth, 2014, pág. 40)

2.9.2 Historia de OSSTMM

El OSSTMM por sus siglas en inglés “Open Source Security Testing Methodology Manual” o “Manual de Metodología Abierta para Pruebas de Seguridad” tal como fue nombrada oficialmente en su versión en español, es uno de los estándares profesionales más completos y comúnmente utilizados a la hora de revisar la Seguridad de los Sistemas de Información. (Racciati, 2013)

Desde su creación a finales de 2000 por Pete Herzog, Director Ejecutivo de ISECOM (Instituto para la Seguridad y Metodologías Abiertas), el OSSTMM creció rápidamente para abarcar todos los canales de seguridad con la experiencia aplicada de miles de colaboradores. Para 2005, el OSSTMM ya no se considera sólo un marco de mejores prácticas sino que se había convertido en una metodología para asegurar la seguridad en el plano operacional debido a que las auditorías de seguridad se convirtieron en una práctica permanente, la necesidad de una metodología sólida se hizo crítica. (Herzog, 2010)

En 2006, el OSSTMM cambió la definición de las pruebas basadas en soluciones tales como pruebas de firewall y pruebas del router, a un estándar para los que necesitan una prueba de seguridad fiable y no sólo un informe de cumplimiento de un reglamento o legislación específica. Actualmente se está considerando OSSTMM como un nuevo estándar ISO. (Herzog, 2010)

Este manual también contempla el cumplimiento de normas y mejores prácticas como las establecidas en el NIST, ISO 27001 – 27002 e ITIL entre otras, lo que la hace uno de los manuales más completos en cuanto a la aplicación de pruebas a la seguridad de la información en las instituciones. (Racciati, 2013)

2.9.3 Propósito del manual

El principal propósito del manual es proporcionar una metodología científica para la caracterización precisa de la seguridad operacional (OpSec) a través del examen y la correlación de los resultados de pruebas de una manera consistente y confiable; es adaptable a casi cualquier tipo de auditoría, incluyendo pruebas de penetración, hacking ético, evaluaciones de seguridad, evaluaciones de vulnerabilidad, y así sucesivamente. Está escrito como un documento de investigación de seguridad y está

diseñado para la verificación de la seguridad objetiva y presentación de indicadores a nivel profesional. (Herzog, 2010)

Un segundo propósito es proporcionar directrices que, cuando se siguen correctamente, permitirán al analista realizar una auditoría certificada por OSSTMM. (Herzog, 2010), toma estas directrices para asegurar lo siguiente:

1. El ensayo se llevó a cabo a fondo.
2. La prueba incluyó a todos los canales necesarios.
3. La postura para la prueba de cumplimiento con la ley.
4. Los resultados son medibles de forma cuantificable.
5. Los resultados son consistentes y repetibles.
6. Los resultados contienen sólo los hechos como se deriva de las propias pruebas.

2.9.4 Contenido

(Herzog, 2010), describe los capítulos de la siguiente manera:

- Capítulo 1: ¿Qué necesitas saber?

En este apartado se hace una explicación de los términos que el manual utiliza en sus páginas posteriores, esto se debe a que el manual utiliza su propia nomenclatura para identificar términos que comúnmente se maneja en materia de seguridad informática, como por ejemplo: RAV, vector, porosidad, limitaciones, controles, seguridad operacional, entre otros; cabe aclarar que la mayoría de dichos términos, es decir los más importantes, ya se los detalló en el capítulo anterior.

- Capítulo 2: ¿Qué necesitas hacer?

A lo largo de este capítulo se dictan las pautas para realizar una buena prueba de seguridad informática y cómo manejar los distintos tipos de errores que se puedan presentar durante el proceso. Para ello (Herzog, 2010) sugiere el siguiente procedimiento de 7 pasos a seguir:

1. Definir lo que desea proteger, es decir los activos. Los mecanismos de protección de dichos activos son los **Controles**, mismos que se probaran para identificar las **Limitaciones**.

2. Identificar el área alrededor de los activos, que incluye los mecanismos de protección y los procesos o servicios construidos en torno a los activos. Esta se conoce como la **zona de enfrentamiento**.
3. Definir todo fuera de la zona de enfrentamiento que sea necesario para mantener a los activos operativos. Pudiendo incluir cosas que no son capaz de influir directamente como la electricidad, alimentos, agua, aire, suelo estable, información, legislación, reglamentos y las cosas con las que alguien puede ser capaz de trabajar tales como sequedad, calidez, frescura, claridad, los contratistas, los colegas, la marca, asociaciones, y así sucesivamente. También contar lo que mantiene a la infraestructura operativa como, protocolos y recursos continuos. Este es el **alcance** de la prueba.
4. Definir cómo el alcance interactúa dentro de sí y con el exterior. Lógicamente se debe fraccionar los activos dentro del alcance a través de la dirección de las interacciones, como del interior al exterior, exterior al interior, del interior para el interior, etc. Estos son los **vectores**. Cada vector debería idealmente ser una prueba separada para mantener una duración corta de cada prueba fraccionada antes de que puedan ocurrir muchos cambios en el medio ambiente.
5. Identificar qué equipos serán necesarios para cada prueba. Dentro de cada vector, las interacciones pueden ocurrir en varios niveles. Estos niveles pueden clasificarse de muchas maneras, sin embargo aquí se han clasificado según su función como cinco **canales**. Los canales son Humano, Físico, Comunicaciones inalámbricas, Telecomunicaciones y Redes de Datos. Cada canal debe ser probado por separado para cada vector.
6. Determinar qué información se desea descubrir de la prueba. El **tipo de prueba** debe ser definido de forma individual para cada prueba, sin embargo, hay seis tipos comunes identificados aquí como Blindaje o Hacking Ético, Doble Blindaje (auditoría de Caja Negra o Pruebas de Penetración), Caja Gris, Doble Caja Gris, Test Tándem o Secuencial e Inverso.
7. Asegurar que la prueba de seguridad que se ha definido cumpla con **las normas judiciales,** esto con el fin de certificar que el proceso para una prueba de seguridad adecuada no cree malentendidos, confusiones, o falsas expectativas.

- Capítulo 3: Análisis de seguridad

Aquí se trata de que el auditor tome las pautas que la metodología recomienda para poder llevar a cabo un buen análisis de seguridad, se profundiza sobre el modelo OpSec y como realizar un informe de la auditoria de manera transparente, tomando como principal herramienta no un análisis de riesgos o de seguridad, sino un análisis de confianza.

- Capítulo 4: Métricas operativas de seguridad

Este capítulo es de gran importancia ya que es aquí donde se aprende a manejar las métricas de seguridad (RAV), que es la medida que la metodología utiliza para dar valores a los distintos tipos de métricas utilizados para calcular la **seguridad actual** del canal probado ya sea utilizando la hoja calculadora de Excel, o las distintas fórmulas para realizarlo de forma manual.

- Capítulo 5: Análisis de confianza

En este capítulo se pretende que el auditor en vez de realizar un análisis de riesgos, realice un análisis de confianza valiéndose de diez propiedades (tamaño, simetría, visibilidad, subyugación, consistencia, integridad, compensación, valor, componentes y porosidad). También dicta unas pequeñas reglas para aplicar correctamente las propiedades antes mencionadas en una prueba de seguridad.

- Capítulo 6: Flujo de trabajo

Aquí se dictan las pautas para llevar a cabo un proceso ordenado durante el tiempo que tome en finalizar la auditoría como tal, para ello se dictan varias pautas a seguir dependiendo del canal que se vaya a probar y los módulos para cada fase de la auditoría (inducción, interacción, indagación, intervención).

- Capítulo 7: Pruebas de seguridad humana

Como su nombre lo indica, en este capítulo se detallan las pruebas que deben ser aplicadas al personal, dentro la institución a auditar. Este canal se encuentra en auge en la actualidad ya que aquí se aplican las técnicas de la conocida ingeniería social; cabe tomar muy en cuenta que también se debe hacer una exhaustiva revisión de la legislación que se aplica para cada canal, incluido éste.

- Capítulo 8: Pruebas de seguridad sobre entornos físicos

En este capítulo se detallan las pruebas que se deben llevar a cabo para auditar todo lo tangible dentro de la institución, es decir, el espacio físico donde se llevan a cabo las interacciones informáticas; incluyendo las estaciones de trabajo, puertas de acceso y todo lo que se encuentre inmiscuido dentro del espacio físico de la institución.

- Capítulo 9: Pruebas de seguridad Wireless

En este capítulo se detallan las pruebas que se deben llevar a cabo para auditar las emanaciones dentro del espectro electromagnético (EM), que la organización utilice en su infraestructura de red, o dicho en otras palabras, escanear las comunicaciones inalámbricas que la organización maneje, tratando de evitar las ondas de radiación que son perjudiciales para la salud, a menos que se cuente con un equipo especializado para hacerlo.

- Capítulo 10: Pruebas de seguridad de telecomunicaciones

Para probar este canal, el auditor necesitará de habilidades y conocimientos en el área de electrónica y así poder manipular los equipos que se encuentran dentro de la red telefónica tanto analógica como digital, esto con el fin de recolectar datos verdaderos que nacen de la comunicación verbal entre las personas que interactúan en la emisión y recepción de un mensaje.

- Capítulo 11: Pruebas de seguridad para redes de datos

En este canal se trata de realizar una prueba de penetración al sistema informático de la organización, especialmente a los equipos que proveen de conexión a la red, para ello puede ser necesario la utilización de varias herramientas de software como sniffers, capturador de paquetes, descifradores de contraseñas, entre otros.

- Capítulo 12: Compliance o cumplimiento normativo

En este capítulo, el OSSTMM reconoce tres tipos de cumplimientos: el legislativo, el contractual y el basado en estándares; esto con el fin de normar el proceso de auditoría de seguridad informática y conocer las regulaciones que existen tanto en la organización como en la región donde se la desarrolla.

- Capítulo 13: Creación de reportes con STAR

STAR (Security Test Auditing Report) son las siglas en inglés para el Informe de Auditoría de Pruebas de Seguridad. La metodología proporciona una plantilla con los datos que se deben considerar al presentar a la organización un informe que contenga todos los aspectos que se contemplaron en la ejecución de la auditoría.

- Capítulo 14: Qué obtienes

Aquí se detallan los beneficios de utilizar OSSTMM para realizar una auditoría de seguridad y las recomendaciones a seguir en caso de aplicar la metodología en otro proceso de auditoría futuro.

- Capítulo 15: Metodología de licencias abierta

Para finalizar con el proceso de la auditoría de seguridad se detallan 12 ítems en los que se especifica en qué consiste la aplicación de una metodología de seguridad de código o fuente abierta.

2.9.5 Ventajas de OSSTMM

A continuación, en la tabla 5 se muestra una comparación entre varias metodologías:

Tabla 5: Diferencias entre varias metodologías

	OSSTMM	**PTES**	**NIST 800-115**	**OWASP**
Ámbito operacional	Sí	No	No	Sí
Ámbito físico	Sí	No	No	No
Ámbito social	Sí	No	Sí	No
Guía técnica	No	Sí	No	Sí
Métricas	Sí	No	No	No
Informes	Sí	Sí	Sí	No
Gestión de proyecto	No	Sí	No	No

Fuente: Elaboración propia

El análisis comparativo de las metodologías OSSTMM, PTES, NIST 800-115 y OWASP; se lo realiza en base a varios factores. El primero trata sobre los ámbitos de

aplicación de las metodologías, de donde se puede rescatar que sólo dos cumplen en separar la seguridad de la información en un ámbito operacional, es decir buscar las limitaciones que poseen sus controles, solo OSSTMM abarca el ámbito físico y en dos de ellas se pueden aplicar técnicas de ingeniería social.

El siguiente factor a tomar en cuenta es si la metodología cuenta con una guía técnica de aplicación de las pruebas, de donde se puede rescatar que PTES y OWASP cuentan con una guía detallada de pruebas; pero OSSTMM aunque no cuenta con una guía, dicta ejemplos de las pruebas que se deberían efectuar a lo largo de su contenido.

Una ventaja significativa con la que debe contar una metodología es de disponer de algún tipo de métrica que permita hacer un análisis cuantitativo del estado de la seguridad informática de la organización donde se efectué el proceso de la auditoría; y sólo OSSTMM cuenta con dichas métricas operacionales.

Una vez que se haya concluido con el proceso de la auditoría, se debe contar con un informe donde se plasmen los resultados obtenidos de la misma; y solo OWASP no cuenta con esta herramienta. Y para finalizar, se debe tomar en cuenta un aspecto que no es de mucha trascendencia para el auditor sobre la parte previa y posterior al proyecto ya que esta tarea debe ser realizada por un Manager o Comercial de la empresa u organización.

2.10 LEGISLACIÓN ECUATORIANA QUE REGULA EL PROCESO DE AUDITORÍA PARA EL GADM-MIRA

En vista de que OSSTMM versión 3, hace hincapié sobre la obligatoriedad de llevar a cabo de un proceso de auditoría que cumpla con las normas judiciales y de que el GADM-Mira no cuenta con una regulación normativa interna que garantice que un proceso de auditoría de seguridad informática no sea un instrumento que pueda crear malos entendidos, confusiones o falsas expectativas, se creyó conveniente nombrar algunas de las Leyes Ecuatorianas que amparan, tanto al proceso de la auditoría como al auditor que llevará a cabo dicho proceso. Entre ellas tenemos:

2.10.1 Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos

Esta Ley fue expedida en el año 2002 en el registro oficial número 67 y según (Congreso Nacinoal del Ecuador , 2002) regula los mensajes de datos, la firma

electrónica, los servicios de certificación, la contratación electrónica y telemática, la prestación de servicios electrónicos, a través de redes de información, incluido el comercio electrónico y la protección a los usuarios de estos sistemas. En el Capítulo V de se trata sobre las infracciones informáticas y lo que más se destaca de ella es lo siguiente:

Art. 57.- Infracciones informáticas.- Se considerarán infracciones informáticas, las de carácter administrativo y las que se tipifican, mediante reformas al Código Penal, en la presente ley.

Más adelante se detallarán las reformas al Código Integral Penal vigente, en donde se incluyen los artículos sin numerar que se disponen en la Ley de comercio electrónico, firmas electrónicas y mensajes de datos.

2.10.2 Ley Orgánica de Transparencia y Acceso a la Información Pública

(Congreso Nacional del Ecuador, 2004), describe esta Ley como:

"Esta Ley garantiza y norma el ejercicio del derecho fundamental de las personas a la información conforme a las garantías consagradas en la Constitución Política de la República, Pacto Internacional de Derechos Civiles y Políticos, Convención Interamericana sobre Derechos Humanos y demás instrumentos internacionales vigentes, de los cuales nuestro país es signatario". Los aspectos más importantes que hay que tomar en cuenta de esta Ley son los siguientes:

- Toda la información que emane o que esté en poder de las instituciones, organismos y entidades, personas jurídicas de derecho público o privado que, para el tema materia de la información tengan participación del Estado o sean concesionarios de éste, en cualquiera de sus modalidades, conforme lo dispone la Ley Orgánica de la Contraloría General del Estado; las organizaciones de trabajadores y servidores de las instituciones del Estado, instituciones de educación superior que perciban rentas del Estado, las denominadas organizaciones no gubernamentales (ONGs), están sometidas al principio de publicidad; por lo tanto, toda información que posean es pública, salvo las excepciones establecidas en esta Ley.
- Los funcionarios de las entidades de la Administración Pública y demás entes señalados en el artículo 1 de la presente Ley, que incurrieren en actos

u omisiones de denegación ilegítima de acceso a la información pública, entendiéndose ésta como información que ha sido negada total o parcialmente ya sea por información incompleta, alterada o falsa que proporcionaron o debieron haber proporcionado, serán sancionados, según la gravedad de la falta, y sin perjuicio de las acciones civiles y penales a que hubiere lugar, de la siguiente manera:

a) Multa equivalente a la remuneración de un mes de sueldo o salario que se halle percibiendo a la fecha de la sanción;
b) Suspensión de sus funciones por el tiempo de treinta días calendario, sin derecho a sueldo o remuneración por ese mismo lapso; y,
c) Destitución del cargo en caso de que, a pesar de la multa o suspensión impuesta, se persistiere en la negativa a la entrega de la información.

2.10.3 Ley de Propiedad Intelectual

(Congreso Nacional del Ecuador, 2006), explica lo siguiente sobre esta Ley:

"Esta ley se crea con el fin de que el Estado reconozca, regule y garantice la propiedad intelectual adquirida de conformidad con la ley, las decisiones de la Comisión de la Comunidad Andina y los convenios internacionales vigentes en el Ecuador".

En esta Ley se ampara la creación de un programa de ordenador (software), la cual se define en la propia Ley como: Toda secuencia de instrucciones o indicaciones destinadas a ser utilizadas, directa o indirectamente, en un dispositivo de lectura automatizada, ordenador, o aparato electrónico o similar con capacidad de procesar información, para la realización de una función o tarea, u obtención de un resultado determinado, cualquiera que fuere su forma de expresión o fijación. El programa de ordenador comprende también la documentación preparatoria, planes y diseños, la documentación técnica, y los manuales de uso.

En la Sección V que trata sobre las Disposiciones Especiales sobre ciertas obras, en el Parágrafo primero se encuentran los artículos que amparan a los programas de ordenador, en la que constan los siguientes:

Art. 28.- Los programas de ordenador se consideran obras literarias y se protegen como tales. Dicha protección se otorga independientemente de que hayan sido incorporados en un ordenador y cualquiera sea la forma en que estén expresados, ya sea en forma legible por el hombre (código fuente) o en forma legible por máquina (código objeto), ya sean programas operativos y programas aplicativos, incluyendo diagramas de flujo, planos, manuales de uso, y en general, aquellos elementos que conformen la estructura, secuencia y organización del programa.

Art. 29.- Es titular de un programa de ordenador, el productor, esto es la persona natural o jurídica que toma la iniciativa y responsabilidad de la realización de la obra. Se considerará titular, salvo prueba en contrario, a la persona cuyo nombre conste en la obra o sus copias de la forma usual.

Dicho titular está además legitimado para ejercer en nombre propio los derechos morales sobre la obra, incluyendo la facultad para decidir sobre su divulgación.

El productor tendrá el derecho exclusivo de realizar, autorizar o prohibir la realización de modificaciones o versiones sucesivas del programa, y de programas derivados del mismo.

Las disposiciones del presente artículo podrán ser modificadas mediante acuerdo entre los autores y el productor.

Art. 30.- La adquisición de un ejemplar de un programa de ordenador que haya circulado lícitamente, autoriza a su propietario a realizar exclusivamente:

a) Una copia de la versión del programa legible por máquina (código objeto) con fines de seguridad o resguardo;
b) Fijar el programa en la memoria interna del aparato, ya sea que dicha fijación desaparezca o no al apagarlo, con el único fin y en la medida necesaria para utilizar el programa; y,
c) Salvo prohibición expresa, adaptar el programa para su exclusivo uso personal, siempre que se limite al uso normal previsto en la licencia. El adquirente no podrá transferir a ningún título el soporte que contenga el programa así adaptado, ni podrá utilizarlo de ninguna otra forma sin autorización expresa, según las reglas generales.

Se requerirá de autorización del titular de los derechos para cualquier otra utilización, inclusive la reproducción para fines de uso personal o el aprovechamiento del programa por varias personas, a través de redes u otros sistemas análogos, conocidos o por conocerse.

2.10.4 Ley Orgánica de Participación Ciudadana

(Asamblea Nacional de la República del Ecuador, 2010), manifiesta lo siguiente:

"La presente Ley tiene por objeto propiciar, fomentar y garantizar el ejercicio de los derechos de participación de las ciudadanas y los ciudadanos, colectivos, comunas, pueblos y nacionalidades indígenas, pueblos afroecuatoriano y montubio, y demás formas de organización lícitas, de manera protagónica, en la toma de decisiones que corresponda, la organización colectiva autónoma y la vigencia de las formas de gestión pública con el concurso de la ciudadanía; instituir instancias, mecanismos, instrumentos y procedimientos de deliberación pública entre el Estado, en sus diferentes niveles de gobierno, y la sociedad para el seguimiento de las políticas públicas y la prestación de servicios públicos; fortalecer el poder ciudadano y sus formas de expresión; y, sentar las bases para el funcionamiento de la democracia participativa, así como, de las iniciativas de rendición de cuentas y control social".

De esta Ley se destacan los siguientes artículos:

Art. 96.- Libre acceso a la información pública.- El Estado garantiza el derecho que tienen las ciudadanas y ciudadanos de acceso libremente a la información pública, de conformidad con la Constitución y la ley. Este derecho constituye un instrumento fundamental para ejercer la participación ciudadana, la rendición de cuentas y el control social.

Art. 100.- Promoción del derecho de acceso a la información.- Todas las entidades que conforman el sector público o la entidades privadas que manejen fondos del Estado, realicen funciones públicas o manejen asuntos de interés público están obligadas a promover y facilitar el ejercicio del derecho de acceso a la información pública.

Art. 101.- Democracia electrónica.- Todos los gobiernos autónomos descentralizados expedirán políticas específicas e implementarán mecanismos concretos para la utilización de los medios electrónicos e informáticos en los procesos

de información, consulta, constitución de grupos, foros de discusión y diálogos interactivos. Para el efecto, cada uno de los gobiernos y dependencias dispondrá y actualizará permanentemente su respectivo portal web con información relativa a leyes, ordenanzas, planes, presupuestos, resoluciones, procesos de contratación, licitación y compras entre otros. Las autoridades públicas de todas las funciones del Estado mantendrán un espacio dedicado en el portal institucional para poder informar, dialogar e interactuar con la comunidad.

2.10.5 Ley Orgánica de Telecomunicaciones

(Asamblea Nacional de la República del Ecuador, 2015), dice que:

"La Ley Orgánica de Telecomunicaciones tiene por objeto desarrollar, el régimen general de telecomunicaciones y del espectro radioeléctrico como sectores estratégicos del Estado que comprende las potestades de administración, regulación, control y gestión en todo el territorio nacional, bajo los principios y derechos constitucionalmente establecidos".

La presente Ley se aplicará a todas las actividades de establecimiento, instalación y explotaciones de redes, uso y explotación del espectro radioeléctrico, servicios de telecomunicaciones y a todas aquellas personas naturales o jurídicas que realicen tales actividades a fin de garantizar el cumplimiento de los derechos y deberes de los prestadores de servicios y usuarios. No corresponde al objeto y ámbito de esta Ley, la regulación de contenidos.

En esta Ley se pueden destacar los siguientes artículos:

Art. 29.- Regulación Técnica.- Consistente en establecer y supervisar las normas para garantizar la compatibilidad, la calidad del servicio y solucionar las cuestiones relacionadas con la seguridad y el medio ambiente.

Art. 76.- Medidas técnicas de seguridad e invulnerabilidad.- Las y los prestadores de servicios ya sea que usen red propia o la de un tercero, deberán adoptar las medidas técnicas y de gestión adecuadas para preservar la seguridad de sus servicios y la invulnerabilidad de la red y garantizar el secreto de la comunicaciones y de la información transmitida por sus redes. Dichas medidas garantizarán un nivel de seguridad adecuado al riesgo existente.

En caso de que exista un riesgo particular de violación de la seguridad de la red, el prestador de servicios de telecomunicaciones deberá informar a sus abonados, clientes o usuarios sobre dicho riesgo y, si las medidas para eliminar o atenuar ese riesgo no están bajo su control, sobre las posibles soluciones.

Art. 85.- Obligaciones adicionales.- La Agencia de Regulación y Control de las Telecomunicación establecerá y reglamentará los mecanismos para supervisar el cumplimiento de las obligaciones tanto de secreto de las comunicaciones como de seguridad de datos personales y, en su caso, dictará las instrucciones correspondientes, que serán vinculantes para las y los prestadores de servicios, con el fin de que adopten determinadas medidas relativas a la integridad y seguridad de las redes y servicios. Entre ellas podrá imponer:

1. La obligación de facilitar la información necesaria para evaluar la seguridad y la integridad de sus servicios y redes, incluidos los documentos sobre las políticas de seguridad.
2. La obligación de someterse a costo del prestador, a una auditoría de seguridad realizada por un organismo público, autoridad competente, y de ser el caso, por una empresa privada o persona natural independiente.

2.10.6 Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional

(Asamblea Nacional de la República del Ecuador, 2009), explica lo siguiente:

Esta ley tiene por objeto regular la jurisdicción constitucional, con el fin de garantizar jurisdiccionalmente los derechos reconocidos en la Constitución y en los instrumentos internacionales de derechos humanos y de la naturaleza; y garantizar la eficacia y la supremacía constitucional. Aquí el tema más importante a tratar es el pedido de **Hábeas Data**, considerándose los siguientes artículos:

Art. 49.- Objeto.- La acción de hábeas data tiene por objeto garantizar judicialmente a toda persona el acceso a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, estén en poder de entidades públicas o de personas naturales o jurídicas privadas, en soporte material o electrónico. Asimismo, toda persona tiene derecho a conocer el uso que se haga de dicha información, su finalidad, el origen y destino, y el tiempo de vigencia del archivo o banco de datos.

El titular de los datos podrá solicitar al responsable del archivo o banco de datos, el acceso sin costo a la información antes referida, así como la actualización de los datos, su rectificación, eliminación o anulación. No podrá solicitarse la eliminación de datos personales que por disposición de la ley deban mantenerse en archivos públicos.

Las personas responsables de los bancos o archivos de datos personales únicamente podrán difundir la información archivada con autorización del titular o de la ley.

Las presentes disposiciones son aplicables a los casos de rectificación a que están obligados los medios de comunicación, de conformidad con la Constitución.

El concepto de reparación integral incluirá todas las obligaciones materiales e inmateriales que el juez determine para hacer efectiva dicha reparación.

Art. 50.- Ámbito de protección.- Se podrá interponer la acción de hábeas data en los siguientes casos:

a) Cuando se niega el acceso a los documentos, datos genéticos, bancos o archivos de datos personales e informes que consten en entidades públicas o estén en poder de personas naturales o jurídicas privadas.
b) Cuando se niega la solicitud de actualización, rectificación, eliminación o anulación de datos que fueren erróneos o afecten sus derechos.
c) Cuando se da un uso de la información personal que viole un derecho constitucional, sin autorización expresa, salvo cuando exista orden de jueza o juez competente.

2.10.7 Código Orgánico Integral Penal (COIP)

(Asamblea Nacional de la República del Ecuador, 2014), indica lo siguiente:

"Este Código tiene como finalidad normar el poder punitivo del Estado, tipificar las infracciones penales, establecer el procedimiento para el juzgamiento de las personas con estricta observancia del debido proceso, promover la rehabilitación social de las personas sentenciadas y la reparación integral de las víctimas".

En la sección sexta de este Código se pueden citar los siguientes artículos:

Art. 178.- Violación a la intimidad.- La persona que, sin contar con el consentimiento o la autorización legal, acceda, intercepte, examine, retenga, grabe,

reproduzca, difunda o publique datos personales, mensajes de datos, voz, audio y video, objetos postales, información contenida en soportes informáticos, comunicaciones privadas o reservadas de otra persona por cualquier medio, será sancionada con pena privativa de libertad de uno a tres años.

No son aplicables estas normas para la persona que divulgue grabaciones de audio y video en las que interviene personalmente, ni cuando se trata de información pública de acuerdo con lo provisto en la ley.

Art. 179.- Revelación de secreto.- La persona que teniendo conocimiento por razón de su estado u oficio, empleo, profesión o arte, de un secreto cuya divulgación pueda causar daño a otra persona y lo revele, será sancionada con pena privativa de libertad de seis meses a un año.

Art. 190.- Apropiación fraudulenta por medios electrónicos.- La persona que utilice fraudulentamente un sistema informático o redes electrónicas y de telecomunicaciones para facilitar la apropiación de un bien ajeno o que procure la transferencia no consentida de bienes, valores o derechos en perjuicio de esta o de una tercera, en beneficio suyo o de otra persona alterando, manipulando o modificando el funcionamiento de redes electrónicas, programas, sistemas informáticos, telemáticos y equipos terminales de telecomunicaciones, será sancionada con pena privativa de la libertad de uno a tres años.

La misma sanción se impondrá si la infracción se comete con inutilización de sistemas de alarma o guarda, descubrimiento o descifrado de claves secretas o encriptadas, utilización de tarjetas magnéticas o perforadas, utilización de controles o instrumentos de apertura distancia, o violación de seguridad electrónicas, informáticas u otras semejantes.

Art. 191.- Reprogramación o modificación de información de equipos terminales móviles.- La persona que reprograme o modifique la información de los equipos terminales móviles, será sancionada con pena privativa de libertad de uno a tres años.

Art. 229.- Revelación ilegal de bases de datos.- La persona que, en provecho propio o de un tercero, revele información restringida, contenida en ficheros, archivos, bases de datos o medios semejantes, a través o dirigidas a un sistema electrónico,

informático, telemático o de telecomunicaciones; materializando voluntaria e intencionalmente la violación del secreto, la intimidad, y la privacidad de las personas, será sancionada con pena privativa de libertad de uno a tres años.

Art. 230.- Interceptación ilegal de datos.- Será sancionada con pena privativa de libertad de tres a cinco años:

1. La persona que sin orden judicial previa, en provecho propio o de un tercero, intercepte, escuche, desvíe, grabe u observe, en cualquier forma un dato informático en su origen, destino o en el interior de un sistema informático, una señal o una transmisión de datos o señales con la finalidad de obtener información restringida o disponible.
2. La persona que diseñe, desarrolle, venda, ejecute, programe, o envíe mensajes, certificados de seguridad o páginas electrónicas, enlaces o ventanas emergentes o modifique el sistema de resolución de nombres de dominio de un servicio financiero o pago electrónico u otro sitio personal o de confianza, de tal manera que induzca a una persona a una persona a ingresar a una dirección o sitio de internet diferente a la que quiere acceder.
3. La persona que a través de cualquier medio copie, clone o comercialice información contenida en las bandas magnéticas, chips u otro dispositivo electrónico que esté soportada en las tarjetas de crédito, débito, pago o similares.
4. La persona que produzca, fabrique, distribuya, posea o facilite materiales, dispositivos electrónicos o sistemas informáticos destinados a la comisión del delito del delito descrito en el inciso anterior.

Art. 232.- Ataque a la integridad de sistemas informáticos.- La persona que destruya, dañe, borre, deteriore, altere, suspenda, trabe, cause mal funcionamiento, comportamiento no deseado o suprima datos informáticos, mensajes de correo electrónico, de sistemas de tratamiento de información, telemático o de telecomunicaciones a todo o partes de sus componentes lógicos que lo rigen, será sancionada con pena privativa de libertad de tres a cinco años.

Con igual pena será sancionada la persona que:

1. Diseñe, desarrolle, programe, adquiera, envíe, introduzca, ejecute, venda o distribuya, de cualquier manera, dispositivos o programas informáticos maliciosos o programas destinados a causar los efectos señalados en el primer inciso de este artículo.
2. Destruya o altere sin la autorización de su titular, la infraestructura tecnológica necesaria para la transmisión, recepción o procesamiento de información en general.

Si la infracción se comete sobre bienes informáticos destinados a la prestación de un servicio público o vinculado con la seguridad ciudadana, la pena será de cinco a siete años de privación de libertad.

Art. 234.- Acceso no consentido a un sistema informático, telemático o de telecomunicaciones.- La persona que sin autorización acceda en todo o en parte a un sistema informático o sistema telemático o de telecomunicaciones o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho, para explotar ilegítimamente el acceso logrado, modificar un portal web, divisar o redireccionar el tráfico de datos o voz u ofrecer servicios que estos sistemas proveen a terceros, sin pagarlos a los proveedores de servicios legítimos, será sancionada con la pena privativa de la libertad de tres a cinco años.

2.10.8 Acuerdos Internacionales

Según el Acuerdo Ministerial 1762 sobre el Plan Nacional de Gobierno Electrónico, éste se debe vincular con las estrategias e indicadores de la Organización de las Naciones Unidas (ONU); y los principios de la Carta Iberoamericana de Gobierno Electrónico (CLAD).

La Organización de las Naciones Unidas a más de imponer una legislación lo que hace es especificar o unificar los criterios con respecto a las definiciones relacionadas con los delitos informáticos, entre los países integrantes. En este sentido los tipos de delitos informáticos según la ONU son (Almeida Romo, 2011, pág. 103):

- **Fraudes cometidos mediante manipulación de computadoras.**
    a) Manipulación de los datos de entrada.
    b) La manipulación de programas.
    c) Manipulación de los datos de salida.

d) Fraude efectuado por manipulación informática.

- **Falsificaciones informáticas**
  a) Como objeto.
  b) Como instrumentos
- **Daños o modificaciones de programas o datos computarizados**
  a) Sabotaje informático
  b) Acceso no autorizado a servicios y sistemas informáticos.
  c) Piratas informáticos o hackers.

A más de los dos instrumentos descritos anteriormente, actualmente varios países alrededor del mundo se están destacando tanto por sus leyes como su infraestructura para tratar los delitos informáticos, entre ellos constan los siguientes: España, Estados Unidos, Bolivia, Argentina, Chile, Brasil, Colombia, Francia, Holanda, Gran Bretaña y Venezuela (Almeida Romo, 2011, pág. 98).

A nivel de Latinoamérica algunos países como Chile, Argentina, Venezuela y Perú, cuentan con regulación, a nivel legislativo que tipifica los delitos informáticos, mientras que en otros países se ha procedido a la reforma de los Códigos de Procedimiento Penal para la aplicación de las sanciones, ante las infracciones informáticas cometidas (Almeida Romo, 2011, pág. 98).

CAPÍTULO III

3. ANÁLISIS DE LA SITUACIÓN ACTUAL

3.1 DESCRIPCIÓN GENERAL

En este capítulo se describieron los principales datos sobre el Gobierno Autónomo Descentralizado Municipal del Cantón Mira y la infraestructura de red de datos que éste manejó en el año 2016, basándose en la información proporcionada por la persona responsable del Área de Sistemas de la Institución, quien es el encargado de administrar toda la infraestructura de la red de datos de la Institución, sumándole visitas técnicas a las instalaciones físicas donde se encuentran los diferentes dispositivos de comunicaciones.

3.2 DESCRIPCIÓN GENERAL DEL GADM-MIRA

El 18 de Agosto de 1980 se crea el Cantón Mira mediante Decreto Legislativo No. 47 y publicado en el Registro Oficial No. 261 del 27 de Agosto de 1980, quedando la administración política en manos del Gobierno Autónomo Descentralizado, regido por el alcalde y el grupo edilicio conformado por tres concejales urbanos correspondiente a la parroquia urbana Mira y cuatro concejales rurales en representación de las tres parroquias rurales. La administración a nivel de las parroquias se realiza mediante los Gobiernos Autónomos Descentralizados Parroquiales de: Juan Montalvo, La Concepción y Jacinto Jijón y Caamaño y la representación del gobierno nacional se realiza a través del Jefe Político del Cantón. (Padilla Ulloa & otros, 2013)

El Cantón Mira se encuentra asentado en un mirador natural conocido como "Balcón de los Andes", cuenta con variedad de microclimas, ya que su suelo inclinado va desde los 1000 hasta los 3500 metros sobre el nivel del mar, dando lugar a temperaturas altas, medias y bajas. La población actual del supera los 13.000 habitantes distribuidos a lo largo y ancho del cantón cuya extensión es de 587.8 Km^2, ocupando el segundo lugar en extensión dentro de la provincia del Carchi. (Padilla Ulloa & otros, 2013)

El GADM-Mira como institución al servicio de todo un cantón tiene su misión, visión, valores, objetivos y estrategias que aportan directamente al desarrollo y visón

cantonal, mismos que detallan a continuación; y para cimentar todos estos aspectos se basa en el Organigrama estructural por procesos que se aprecia en la Figura 2.

3.2.1 Misión

La Misión del Gobierno Autónomo Descentralizado Municipal del Cantón Mira como institución pública autónoma está encaminada a satisfacer y mejorar las necesidades básicas de la comunidad a través de mecanismos de participación ciudadana, en la búsqueda del desarrollo social cantonal. (GAD-Mira, 2014)

3.2.2 Rol de la Municipalidad en el Desarrollo Cantonal

El rol del Gobierno Autónomo Descentralizado Municipal del Cantón Mira está cambiando, ya no es simplemente una entidad gubernamental proveedora de servicios públicos, sino que hoy en día debe afrontar nuevas temáticas y satisfacer las crecientes expectativas de la población que atiende. El GADM-Mira está asumiendo el reto y eso implica tener una institución abierta al cambio y conjugar su accionar con las demandas de la colectividad mireña. (GAD-Mira, 2014)

3.2.3 VISIÓN

3.2.3.1 *Visión de desarrollo cantonal.*

La diversidad de intervenciones que se realizan para lograr el desarrollo integral de una población ubicada dentro de un territorio o jurisdicción, demandan cada día de la implementación de acciones e iniciativas más elaboradas, estructuradas y con un mayor grado de planificación. Es esencialmente importante conocer hacia dónde quiere ir el cantón y toda la población, cuál es su visión de desarrollo, y con esta base, unir esfuerzos y recursos humanos, técnicos y económicos para enrumbarlos en la construcción del camino hacia esa anhelada visión. (GAD-Mira, 2014)

3.2.3.2 *Visión institucional del GADM-Mira.*

La Visión del desarrollo cantonal para el 2020, consiste en que el cantón Mira será un modelo de desarrollo armónico e integral en lo social, agrícola, pecuario, turístico, artesanal, cultural y deportivo. Líder en gestión participativa, con servicios de calidad,

potenciando permanentemente el desarrollo humano con dignidad y equilibrio económico, dentro de un ambiente sano y sustentable. (GAD-Mira, 2014)

3.2.4 Organigrama de la Institución

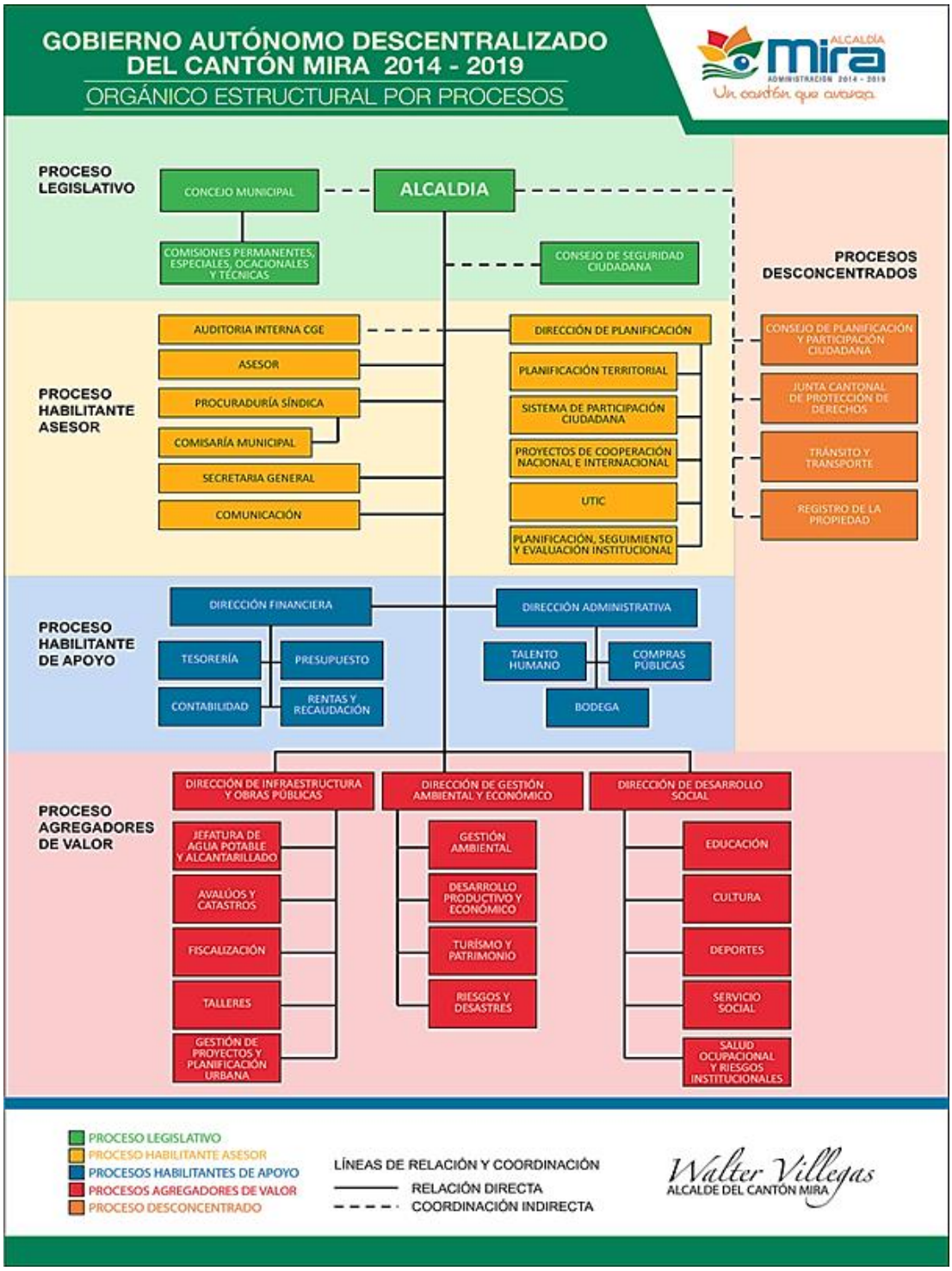


Figura 2: Organigrama Institucional por procesos del GADM-Mira

Fuente: Ley Orgánica de Transparencia y Acceso a la Información Pública. Recuperado de: http://www.mira.gob.ec/images/literales/ORGANICO.png

3.2.5 Ubicación física del GADM-Mira

El GADM-Mira se encuentra situado en la única parroquia urbana del cantón; que también posee el nombre de Mira y es la cabecera cantonal, sus instalaciones se encuentran en la esquina de la Avenida León Rúales Nro. C8-010 y la calle Gonzáles Suárez, tal como se muestra en la Figura 3 (tomada de Google maps); cabe recalcar que la actual infraestructura fue reconstruida en el año de 1994, debido a un incendio, y desde esa fecha no se han realizado modificaciones notables en su diseño. (GAD-Mira, 2014)

Figura 3: Ubicación: del GADM-Mira

Fuente: Elaboración propia. Recuperado de: Google maps.

3.2.6 Instalaciones del GADM-Mira

El edificio del GADM-Mira consta de tres plantas en su infraestructura central, tal como se muestran en las figuras 4 y 5, así como de una construcción externa anexa de dos plantas la cual pertenecía al registro civil; pero que en la actualidad es ocupada por varios funcionarios de la Institución. En toda la infraestructura se distribuyen las diferentes instancias departamentales en donde los funcionarios realizan sus labores y actividades; la oficina de Sistemas se encuentra ubicado en el tercer piso y es de aquí donde se distribuyen los recursos informáticos a toda la Institución.

Figura 4: Vista de la parte interna del GADM-Mira

Fuente: Elaboración propia. Recuperado de: GADM-Mira, 2016.

Figura 5: Vista de la parte externa del GADM-Mira

Fuente: Elaboración propia. Recuperado de: GADM-Mira, 2016.

En la Figura 6 se muestra la planta externa anexa al edificio del GADM-Mira, en donde se distribuyen varias oficinas departamentales que han sido readecuadas y en la actualidad son ocupadas por varios funcionarios en su gran mayoría de servicios comunales, ambientales y sociales.

Figura 6: Vista frontal y posterior de la planta externa del GADM-Mira

Fuente: Elaboración propia. Recuperado de: GADM-Mira, 2016.

3.2.7 Distribución departamental

En la Tabla 6, se detalla la distribución departamental por plantas de las diferentes jurisdicciones del GADM Mira.

Tabla 6: Distribución por departamentos del GADM del cantón Mira

PLANTA	DEPARTAMENTO	UNIDAD A LA QUE PERTENECE
BAJA	Recursos Humanos	**Dirección Administrativa**
	Recaudación de Impuestos	**Administración Financiera**
	Rentas	
	Recaudación Agua Potable	
	Tesorería	
	Bodega	**Otros Servicios Comunales**
	Avalúos y Catastros	**Dirección de Planificación**
SEGUNDA	Obras Públicas	**Dirección de Obras Públicas**
	Salón Máximo	**Administración General**
	Sala de Sesiones	
TERCERA	Departamento Jurídico	**Dirección Administrativa**
	Dirección Financiera	**Administración Financiera**
	Secretaría General	**Administración General**
	Alcaldía	
	Sistemas	**Dirección de Planificación**
EXTERNA	Agua Potable	**Dirección de Obras Públicas**
	Comisaría Municipal	**Dirección Administrativa**
	Comisaría Nacional	**Otros Servicios Comunales**
	Jefatura Política	
	Correos	
	Mecanización	
	Bodegas	**Dirección Administrativa**
	Planificación	**Dirección de Planificación**
	Cultura	**Desarrollo Social**
	Ambiente y Productividad	**Gestión Ambiental**

Fuente: Elaboración propia. Recuperado de: GADM-Mira, 2016.

3.3 ESTRUCTURA ACTUAL DE LA RED DE DATOS

La red LAN del GADM-Mira está funcionando aproximadamente desde el año 2007 y tomando en cuenta que el actual edificio del GADM-Mira fue reconstruido, su nueva planta central fue edificada pensando en los nuevos avances tecnológicos y en el uso de una red LAN de datos, para ello se construyó dos ductos de 0,75m de ancho, por 1m de largo, para la distribución del cableado estructurado hacia las diferentes plantas del edificio.

El cuarto de telecomunicaciones de la Institución se encuentra actualmente ubicado en el tercer piso y desde aquí se debe distribuir los diferentes recursos de red hacia las plantas inferiores; pero a pesar de contar con los ductos antes mencionados, para las nuevas instancias departamentales que se van incorporando es necesario adecuar nuevas rutas externas de cableado, dependiendo de las condiciones de ubicación que se presenten.

La red LAN del GADM-Mira es de tipo Ethernet y posee una distribución topológica jerárquica tipo árbol, al momento de su implementación se pensó en una red escalable en el tiempo ya que en aquel entonces solamente se contaba con 30 puntos de red, según datos proporcionados por la persona encarga del Área de Sistemas, de los cuales 21 se utilizaban para las primeras computadoras que tenían acceso a la Internet y el resto se dejaron libres.

3.3.1 Cableado Horizontal y Vertical

En el transcurso de la realización del presente trabajo de grado, se pudo constatar que tanto el cableado horizontal como vertical está compuesto por cable UTP categoría 5E y no se cumplen las especificaciones establecidas por las normas: ANSI/EIA/TIA 569-C (que trata sobre los espacios y canalizaciones para telecomunicaciones), ya que los espacios para el cableado se van adecuando conforme se van modificando las diferentes áreas de trabajo dentro del edificio y por tanto, las nuevas rutas se las distribuye, en el mejor de los casos, por canaletas, o en su defecto se lo deja a la intemperie. La norma ANSI/TIA/EIA-568-C (que trata sobre el cableado de telecomunicaciones para edificios comerciales), ya que en muchos casos se infringe con el radio de curvatura permitido para el cable, y la norma ANSI/TIA/EIA-607 que

trata sobre las tierras y aterramientos para los sistemas de telecomunicaciones de los edificios comerciales.

En cuanto al cableado vertical, a pesar de que existen los ductos antes mencionados para su distribución, se debería tomar en cuenta el ambiente que existe dentro de ellos, ya que éste contribuye a que el cable de cobre se corroa con el paso del tiempo, en tal virtud, se debería utilizar un cable especial que cuente con una protección adecuada tanto para el ambiente que existe dentro de los ductos, como para posibles roedores que pudieran guarecer en el interior de los mismos.

Para el caso de la planta externa, el cableado vertical también infringe con las normas antes mencionadas, ya que su tendido no se lo dispone de una forma adecuada y se encuentra colgado a la intemperie. A los problemas antes mencionados se suma el hecho de no contar con la debida certificación del sistema de cableado estructurado, y de no proveer un etiquetado de los equipos y dispositivos terminales, ya que este mecanismo provee de una pronta identificación, en caso de presentarse algún problema de conectividad con un equipo específico.

En la Figura 7, se puede apreciar un collage de fotos con los diferentes métodos inadecuados de tendido del cableado horizontal utilizados para distribuirlo en varias instancias de la Institución.

Figura 7: Recorrido del cableado horizontal

Fuente: Elaboración propia. Recuperado de: GADM-Mira, 2016.

En la Figura 8, se puede apreciar la distribución del cableado vertical por los ductos de distribución hacia las plantas inferiores del GADM-Mira, aunque los ductos tienen una cubierta que los protege en caso de lluvia, se puede notar que muchos de los cables de datos no están debidamente protegidos para el ambiente que existe en el interior de los ductos, también se puede observar que el ducto de la derecha no se utiliza en gran medida para los cables UTP.

Figura 8: Ductos para distribución del cableado vertical
Fuente: Elaboración propia. Recuperado de: GADM-Mira, 2016.

3.3.2 Cuarto de Telecomunicaciones

El cuarto de telecomunicaciones por cuestiones de diseño se encuentra ubicado en la tercera planta del edificio del GADM-Mira, en él predominan tres racks: dos piso, uno abierto de 64 UR y otro cerrado de 48 UR, y uno de pared (cerrado) de 24 UR; en ellos se ubican principalmente el equipo de ruteo y los equipos de conmutación para todas las estaciones de trabajo de la Institución, junto al éste se encuentra ubicada la oficina del Área de Sistemas, esto debido a que la persona encargada del área debe estar al tanto de todo lo que pasa con los equipos, en caso de suscitarse algún tipo de problema y así poder dar una solución inmediata.

En la Figura 9, se puede apreciar los tres racks que existen en el cuarto de telecomunicaciones del GADM-Mira. El rack de la derecha es utilizado para ubicar los equipos de distribución y tal como se observa, no existe un etiquetado de los dispositivos que se encuentran actualmente activos, ni orden con los patch cords de interconexión entre dispositivos que se encuentran dentro del mismo. El rack del medio es utilizado para alojar a un servidor de pruebas para bases de datos y en el rack de la izquierda se encuentra ubicado el equipo que da salida a la Internet.

Figura 9: Racks del cuarto de telecomunicaciones

Fuente: Elaboración propia. Recuperado de: GADM-Mira, 2016.

El cuarto de telecomunicaciones del GADM-Mira es de tipo TIER 1, ya que poco a poco se lo ha ido adaptando a las exigencias evolutivas de su red de datos y al incremento de los usuarios de la red municipal, no posee mecanismos de redundancia para los equipos de comunicación; pero si posee UPS que proveen de alimentación eléctrica a los equipos de Core, en caso de presentarse un corte de energía eléctrica; existe un solo equipo de aire acondicionado para todo el cuarto, el cual permite mantener una temperatura de 16ºC, para suministrar un ambiente óptimo de funcionamiento para los equipos de comunicaciones.

Dos de los servicios prestados por el Área de Sistemas se encuentran implementados en servidores in chassis: el servidor de bases de datos y el servidor de Internet; los servicios de web, hosting y firewall son entregados a través de un contrato con empresas privadas.

En caso de que se requiera realizar tareas de mantenimiento preventivo de los equipos de comunicaciones, que por cuestiones de operatividad se lo debe realizar mínimo 2 veces al año siguiendo el manual de procedimientos de la Institución, el personal del Área de Sistemas realiza este proceso en horarios fuera de la jornada laboral o en fines de semana ya que toda la red de la Institución queda totalmente inoperativa.

En cuanto a los mecanismos de seguridad para el acceso al cuarto de telecomunicaciones se podría decir que es prácticamente fácil de vulnerar, ya que no existe algún método automatizado que evite el ingreso de personas no autorizadas al

mismo, basta tener la autorización (verbal o escrita) del responsable del Área de Sistemas para poder acceder, ya que primero se debe cruzar por su oficina personal. El único método de seguridad con el que cuenta el cuarto de telecomunicaciones es con un sistema de video-vigilancia que permite observar quien ingresa sin autorización.

En la Figura 10, se puede observar a breves rasgos tanto el cuarto de telecomunicaciones, y la oficina de la persona encargada del Área de Sistemas del GADM-Mira.

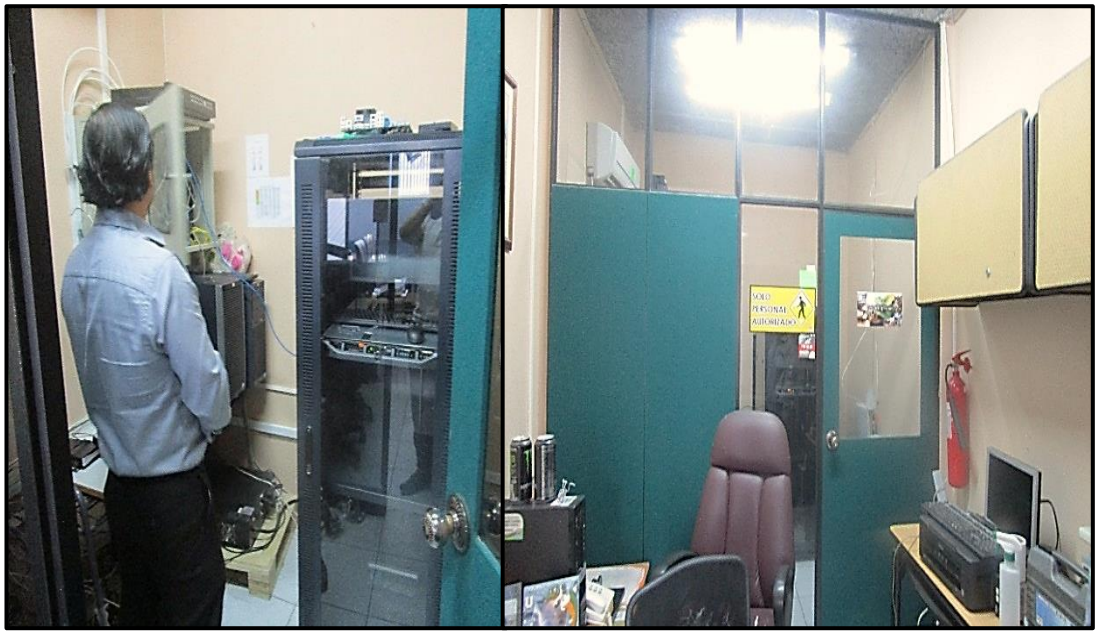


Figura 10: Cuarto de telecomunicaciones y oficina del encargado del área de Sistemas
Fuente: Elaboración propia. Recuperado de: GADM-Mira, 2016.

3.3.3 Áreas de trabajo

El GADM-Mira se encuentra dividido en diferentes áreas departamentales, mismas que están constituidas por oficinas o en su defecto en áreas modulares compartidas en cada una de las plantas del edificio y se las adecuan acorde a una planificación basada en las necesidades de la administración general de turno, por lo tanto los puntos de red se deben adecuar según la ubicación del terminal que haga uso del servicio de Internet o de la intranet, así que esto es uno de los principales justificativos del por qué no existe un etiquetado de los equipos. En la Figura 11 se puede apreciar un ejemplo de una estación de trabajo completa.

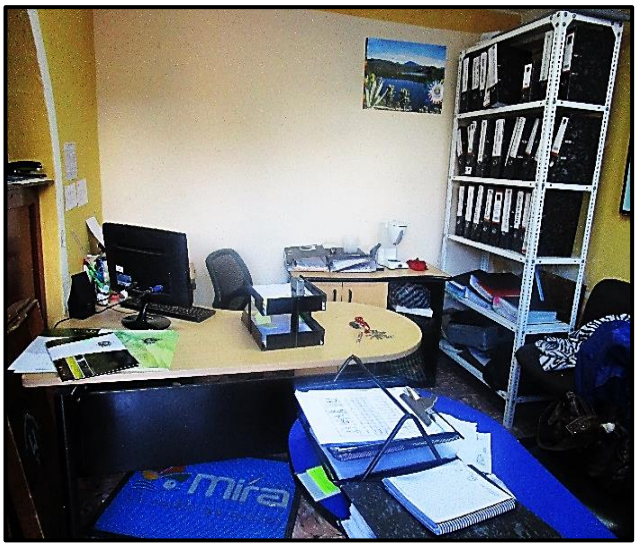


Figura 11: Ejemplo de un área de trabajo

Fuente: Elaboración propia. Recuperado de: GADM-Mira, 2016.

3.3.4 RED ACTIVA ACTUAL

3.3.4.1 *Topología física de la red.*

La red LAN del GADM-Mira es de tipo Ethernet, manejando actualmente una topología de distribución jerárquica tipo árbol, tal y como se puede apreciar en la Figura 12, su sistema de cableado estructurado está diseñado para soportar velocidades de transmisión que van desde los 512 Kbps en enlaces compartidos, hasta los 8 Mbps en enlaces dedicados. Gran parte de sus equipos son no administrables o se encuentran funcionando en su modo más básico o por defecto, la red no posee segmentación por lo que sus equipos poseen un solo dominio de broadcast.

El recorrido para llegar a una estación de trabajo es el siguiente: partiendo desde el cuarto de telecomunicaciones desde el switch de core, se pasa al switch de distribución, dependiendo de dónde se encuentre la estación de trabajo, se llega hasta el switch de acceso, habrá que recorrer por medio de cable hasta un terminal donde se encuentran los cajetines con sus respectivos conectores o jacks y finalmente por medio de un patch cord se llega al dispositivo terminal; para la fecha se cuenta con un inventario total de 75 equipos informáticos en las estaciones de trabajo operativas, a las que se suman: 2 impresoras IP, 2 servidores, 2 servicios privados de web y hosting; y 2 DVR sin IP pública.

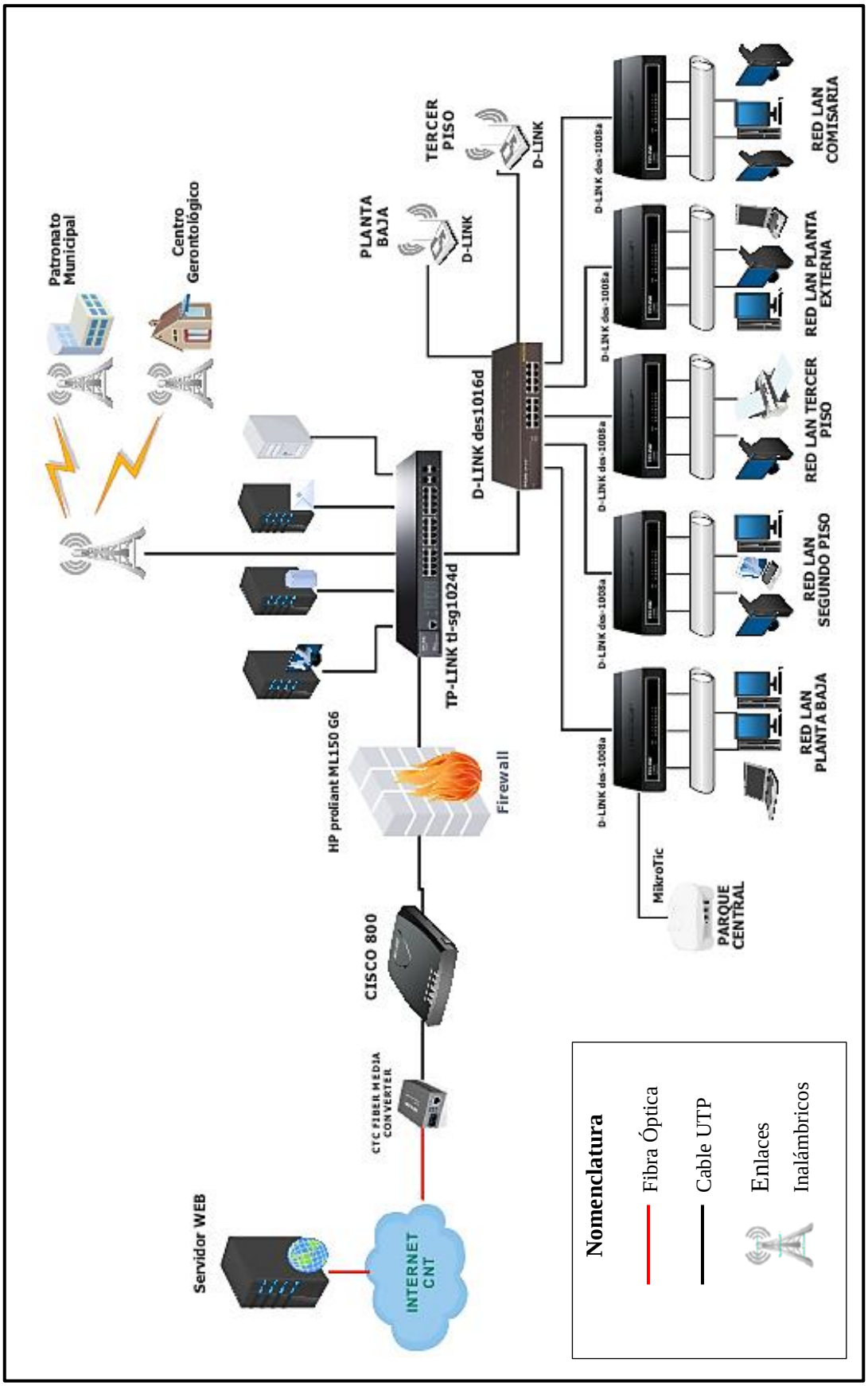


Figura 12: Ejemplo de un área de trabajo

Fuente: Elaboración propia. Recuperado de: GADM-Mira, 2016.

3.3.5 DETALLE DE LOS RECURSOS INFORMÁTICOS

3.3.5.1 *Equipos de enrutamiento.*

El GADM-Mira no cuenta con un equipo propio de enrutamiento, ya que posee un solo router (CISCO 800) proporcionado por la empresa proveedora de servicios de Internet, que más allá de brindar un protocolo de enrutamiento dinámico, sirve como salida hacia la Internet (NAT) a los usuarios de la red LAN de la Institución, ya que se encuentra funcionando en su forma más simple, que es en su modo por defecto.

3.3.5.1.1 Enlace WAN.

El GADM-Mira posee un contrato por concepto de servicios de Internet con la empresa CNT E.P. (Corporación Nacional de Telecomunicaciones-Empresa Pública) con una capacidad total de 13 Mbps simétricos por medio de una conexión de Fibra Óptica monomodo sin back-up, como se puede considerar en la Figura 13. Para poder cambiar de medio de transmisión (óptico a electromagnético), se hace uso de un conversor fibra óptica a Ethernet tipo LC, luego se llega hasta el router (CISCO 800); para controlar el tráfico de red tanto de entrada como de salida desde y hacia la Internet se hace uso del servicio de Firewall.

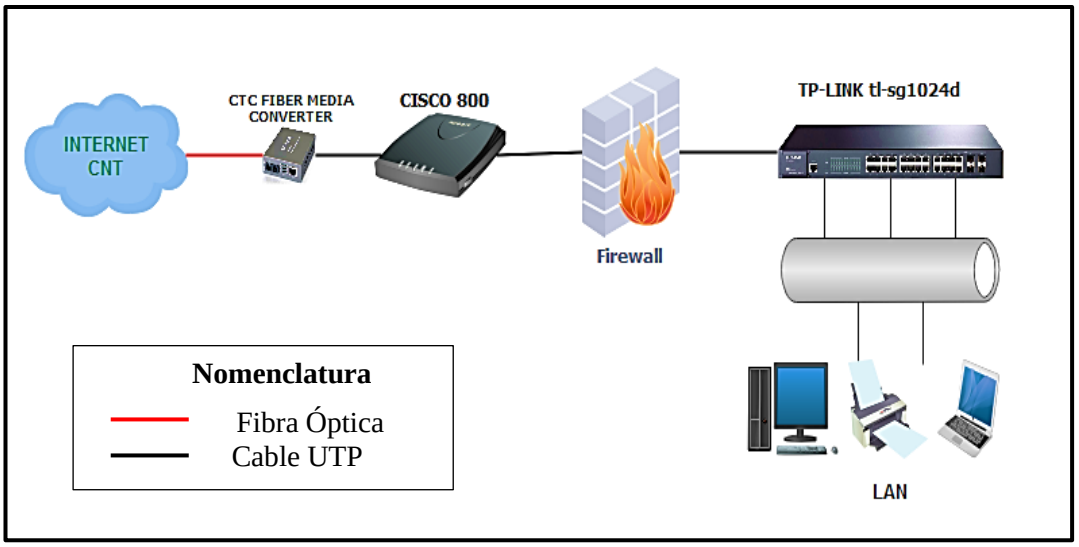


Figura 13: Conexión hacia la Internet del GADM Mira

Fuente: Elaboración propia. Recuperado de: GADM-Mira, 2016.

3.3.5.1.2 Direccionamiento.

El direccionamiento asignado para los equipos de comunicación, los ordenadores y/o dispositivos terminales del GADM-Mira es de clase C, es decir, los tres primeros bytes de la dirección IP representan a la porción de red y el cuarto byte representa el número de hosts permitidos, siendo para este tipo de direcciones de 254 direcciones IP disponibles para hosts, esto se debe a que con un porcentaje de escalabilidad de la red, la Institución no requiere más de 100 direcciones IP para sus usuarios, porque la red municipal es relativamente pequeña. El direccionamiento principal de la red municipal se detalla en la Tabla 7.

Tabla 7: Direccionamiento de la red municipal

NOMBRE	DIRECCIÓN	MÁSCARA
Red Interna	192.20.X.X	255.255.255.0
Red Externa	192.168.X.X	255.255.255.248

Fuente: Elaboración propia. Recuperado de: GADM-Mira, 2016.

3.3.5.2 *Equipos de conmutación.*

Los equipos de conmutación del GADM-Mira son no-administrables y se encuentran conectados en un orden jerárquico, basándose en el modelo de conexión en cascada, mismo que empieza en el switch de core, pasa al switch de distribución y finalmente a los switches de acceso, cuyas características se muestran en la Tabla 8 y sus hojas de especificaciones en los Anexos 1, 2 y 3 respectivamente. En caso de necesitar más puertos para las estaciones de trabajo se deja un puerto libre en un switch de acceso y en este puerto se conecta otro switch de acceso, formando una cascada; y así se extiende la red hasta que se logre satisfacer el número de dispositivos terminales requeridos en cada planta del edificio. Cabe señalar que la conexión en cascada de los equipos de conmutación no es muy recomendable, ya que en caso de fallar un equipo que se encuentre en lo más alto del orden jerárquico tomado como referencia, prácticamente toda la porción de red que de él dependa quedará totalmente inoperativa.

Tabla 8: Características de los equipos de conmutación del GADM-Mira

Jerarquía	Marca	Modelo	Nro. de Puertos	Estándares soportados
Core	TP-LINK	tl-sg1024d	24	IEEE 802.3 IEEE 802.3u IEEE 802.3x IEEE 802.3ab
Distribución	D-LINK	des-1016d	16	IEEE 802.3 IEEE 802.3u
Acceso	D-LINK	des-1008a	8	IEEE 802.3az IEEE 802.3x

Fuente: Elaboración propia. Recuperado de: GADM-Mira, 2016.

3.3.5.3 *Servidores.*

Básicamente el GADM-Mira hace uso de 5 servicios elementales como son el de bases de datos, Internet, Firewall proxy, web y hosting para cuentas de correo electrónico; de los cuales solo dos (bases de datos e Internet) se encuentran instalados físicamente en el cuarto de telecomunicaciones de la Institución, sus especificaciones se pueden apreciar en la Tabla 9; para su implementación se hace uso del sistema operativo WinServer 2008 SP1. Los otros tres servicios son contratados a empresas privadas: el de Firewall proxy es un complemento al servicio de antivirus prestado por la empresa ESET Smart Security, los servicios de web y hosting para cuentas de correo electrónico son prestados por la empresa NIC.EC.

Tabla 9: Especificaciones de los servidores del GADM del cantón Mira

SERVIDOR	MARCA/ MODELO	PROCESADOR	RAM	DISCO DURO	IMAGEN
BASES DE DATOS	HP ProLiant ml350 g5	Intel Xeon 1,87GH	4GB	140GB	
INTERNET	HP ProLiant ml150 g6	Intel Xeon 2GH	2GB	160GB	

Fuente: Elaboración propia. Recuperado de: GADM-Mira, 2016.

3.3.5.4 *Distribución de las estaciones de trabajo por plantas.*

En la Tabla 10 se detalla la distribución por plantas de los 75 ordenadores que actualmente son propiedad del GADM-Mira, a esta lista se añaden también varias estaciones de trabajo que no se encuentran físicamente en el interior de la planta central de la Institución, pero que forman parte su inventario de equipos informáticos, ya que se encuentran operando como parte de su recurso de TICs, entre ellas se encuentran las del Proyecto FIE, Biblioteca MIPRO, Centro Gerontológico, entre otras.

Tabla 10: Distribución por plantas de los usuarios

PLANTA	OFICINA	ORDENADORES	TIPO
BAJA	Tesorería	2	PC de escritorio
	Contabilidad	4	PC de escritorio
	Agua Potable	1	PC de escritorio
	Avalúos y Catastros	3	PC de escritorio
	Recaudación	1	PC de escritorio
	Talento Humano	1	PC de escritorio
	Dirección Administrativa	1	PC de escritorio
TOTAL		**13**	
SEGUNDA	Compras Públicas	2	PC de escritorio
	Obras Públicas	4	PC de escritorio
	Concejales	1	PC de escritorio
TOTAL		**7**	
TERCERA	Secretaría	1	PC de escritorio
	Pro-Secretaría	1	PC de escritorio
	Dirección Jurídica	2	PC de escritorio
	Alcaldía	1	PC de escritorio
		1	PC Portátil
	Dirección Financiera	1	PC de escritorio
		1	PC Portátil
	Sistemas	4	PC de escritorio
		2	Servidor Tower
	Adquisiciones	1	PC de escritorio
	Desarrollo Económico	1	PC de escritorio
TOTAL		**16**	

Continúa ⟶

	Deportes	1	PC de escritorio
	Comunicación	2	PC de escritorio
	Fiscalización	1	PC de escritorio
	Bodega	2	PC de escritorio
	Dirección de Desarrollo Social	2	PC de escritorio
		1	PC Portátil
	Cultura	2	PC de escritorio
EXTERNA	Deportes	1	PC Portátil
	Turismo	1	PC de escritorio
	Dirección de Planificación	3	PC de escritorio
		3	PC Portátil
	Medio Ambiente	2	PC de escritorio
	Comisaría	2	PC de escritorio
	Gestión de Riesgos	1	PC Portátil
	Tránsito y Transporte	1	PC de escritorio
TOTAL		**25**	
	Biblioteca	1	PC de escritorio
	CC Niñez y Adolescencia	3	PC de escritorio
	Gerontológico	1	PC de escritorio
OTROS		1	PC Portátil
	Garajes	1	PC de escritorio
	Biblioteca MIPRO	4	PC de escritorio
	Proyecto FIE	3	PC de escritorio
TOTAL		**14**	
TOTAL DE DISPOSITIVOS TERMINALES			**75**

Fuente: Elaboración propia. Recuperado de: GADM-Mira, 2016.

3.3.5.5 *Central de voz.*

El GADM-Mira hace uso de una central telefónica analógica la cual no afecta al tráfico de datos de la red, ya que como se explicó anteriormente no existe un equipo de enrutamiento que discrimine el tráfico de voz con el de datos, así que esta central provee su servicio separado de la red de datos. La central telefónica es de marca y

modelo Panasonic kx-tem824 (ver Anexo 4) la cual provee de una capacidad máxima de 16 líneas externas y una capacidad final de 24 extensiones; esta central telefónica es utilizada por los empleados para comunicar datos urgentes entre oficinas departamentales que se encuentran físicamente separadas.

3.3.5.6 *Enlaces inalámbricos.*

Básicamente existen dos enlaces principales, uno de radiofrecuencia, con su respectivo back-up el cual se encuentran dirigido desde la terraza del edificio del GADM-Mira, hacia una pequeña torre de 5m de altura que se articula en la terraza del edificio del ex Patronato Municipal, esto debido a que gracias a la elevación que tiene dicha infraestructura, se pueden repartir de mejor manera varios radioenlaces a diferentes instituciones y dependencias que forman parte de la jurisdicción administrativa del GADM, ya que se facilita la línea de vista con dichas entidades, a las cuales la Institución les facilita su conexión al servicio de Internet. Para la interconexión de los radioenlaces se utilizan equipos de la marca Ubiquiti, tanto para transmisión como para recepción de las señales de radio, se pueden apreciar de mejor manera en la Figura 14.

El otro enlace que brinda el GADM-Mira de forma gratuita a la ciudadanía, es la conexión a la señal inalámbrica del servicio de Internet al parque central de la ciudad, o más conocida como la zona Wi-Fi, utilizando para ello un router MickoTic de gama baja.

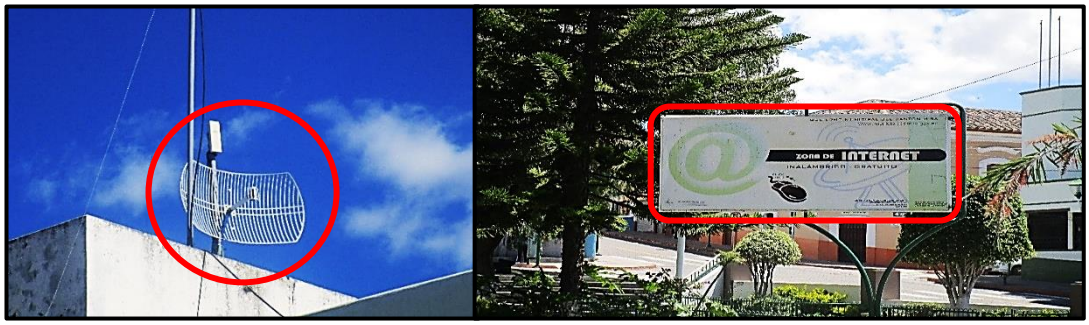


Figura 14: Radioenlaces desde el GADM-Mira

Fuente: Elaboración propia. Recuperado de: GADM-Mira, 2016.

3.3.5.6.1 Enlace ex Patronato Municipal

Este radioenlace, mostrado en la Figura 15, es uno de los más importantes que posee el GADM-Mira ya que gracias a él, la Institución crea enlaces no solo de red, sino

también de fraternidad con las entidades a las que comparte esta interconexión; para ello se utiliza una antena Ubiquiti airGrid AG-HP-5G27 de 23dBi (ver hoja de especificaciones en el Anexo 5) tanto para transmisión como para recepción a una distancia lineal de 180 metros, se lo implementó hace aproximadamente 5 años y gracias a las grandes prestaciones que este brindó desde un inicio, se ha logrado desde aquí implementar algunos radioenlaces a varias instituciones y varios repetidores, las más importantes se enlistan a continuación:

- Unidad Educativa Carlos Martínez Acosta
- Infocentro y CIBV de la comunidad de Mascarilla
- Unidad Educativa León Rúales
- Puesto de Salud El Hato
- Piscina Municipal del Cantón Mira
- Policía Nacional (UPC Mira)
- Escuadrón de Carreteras del Cantón Mira
- Distrito de Educación de la cuidad de Mira
- Cuerpo de Bomberos del cantón Mira
- Garajes del GADM de Mira
- Centro de Salud de San Antonio de Mira

Figura 15: Radioenlaces desde el GADM-Mira hacia la torre del ExPatronato Municipal
Fuente: Elaboración propia. Recuperado de: GADM-Mira, 2016.

- *Enlace de back-up*

Para este radioenlace, se utiliza un equipo Ubiquiti locoM5 NanoStation de 13 dBi (ver hoja de datos en Anexo 6), fue implementado aproximadamente hace 3 años para

brindar una conexión de respaldo al radioenlace principal, anteriormente descrito, en caso de presentarse alguna falla, ya que varias instituciones dependen de éste y no sería bien visto que se interrumpa el servicio de Internet que brinda la Institución por medio de estos radioenlaces.

3.3.5.7 *Estaciones de Trabajo.*

Dependiendo de la movilidad que el usuario necesite, en cada oficina se cuenta por lo menos con 2 o 3 computadoras de escritorio ya que el número de computadoras portátiles es limitado (9 en total), designadas para uso de los siguientes cargos: alcaldía, deportes, planificación, gestión de riesgos, dirección financiera, dirección de planificación y dirección de desarrollo social. Los 75 ordenadores que forman parte del recurso informático la Institución poseen conexión a Internet y están dispuestas para uso del jefe departamental y para su respectivo asistente o secretaria; el sistema operativo que predomina es el de Microsoft Windows con sus respectivas versiones y distribuciones, mismas que van desde Windows XP, hasta Windows 8.1; de la totalidad de los ordenadores operativos, solo 4 cuentan con una distribución de Linux y uno con el Sistema Operativo MAC.

La mayoría del personal utiliza en gran medida las herramientas de Microsoft Office, pero dependiendo de las funciones departamentales, existen programas o sistemas que son propios del usuario como por ejemplo el sistema integral de catastros, sistema financiero, sistema de agua potable, programas y herramientas de diseño, entre otros. En las Tablas 11, 12, 13 y 14 se hará una clasificación de todas las estaciones de trabajo por la versión del sistema operativo que utiliza y se mostrará las diferentes características que estos poseen:

Tabla 11: Estaciones de trabajo con Sistema Operativo Windows XP y Vista

Windows XP				
Nro.	**Marca**	**Procesador**	**Memoria RAM**	**Capacidad de Almacenamiento**
2	HP ProBook	Intel Core 2 Duo	2,9 GB	500 GB
1	Hp Pavilion Slimline	Intel Core 2 Duo	2 GB	300 GB
1	No especificada	Intel Core 2 Duo	2 GB	300 GB
1	Dell	Intel Pentium - 3.40 GHz	1 GB	150 GB

Continúa ⟶

Windows XP Profesional				
Nro.	**Marca**	**Procesador**	**Memoria RAM**	**Capacidad de Almacenamiento**
5	Hp Pro3000	Intel Core 2 Duo	4 GB	300 GB
1	Hp COMPAQ Pro 6300MT	Intel Core i3 de 3,40 GHz	2 GB	500 GB
Windows XP Profesional SP3				
Nro.	**Marca**	**Procesador**	**Memoria RAM**	**Capacidad de Almacenamiento**
1	Hp Pro3000	Core 2 Duo	4 GB	300 GB
1	Dell	Intel Core 2 Duo - 2,4 GHz	1 GB	150 GB
1	Dell	Pentium Dual Core – 3 GHz	2 GB	100 GB
2	Hp COMPAQ 6000 Pro MT	Intel Core 2 Quad - 2,83 GHz	4 GB	300 GB
1	No especificada	Pentium Dual Core – 3 GHz	2 GB	300 GB
1	No especificada	Intel Core 2 - 1,80 GHz	1 GB	260 GB
1	No especificada	Intel Pentium 4 - 3.00 GHz	496 MB	120 GB
1	No especificada	Intel Pentium 4 - 3,20 GHz	2 GB	100 GB
Windows XP SP3				
Nro.	**Marca**	**Procesador**	**Memoria RAM**	**Capacidad de Almacenamiento**
1	No especificada	Intel Pentium 4 - 2,80 GHz	256 MB	100 GB
1	Hp Elite 7100 MT	Intel Core 2 Quad - 2,4 GHz	1,97 GB	260 GB
Windows XP Profesional SP2				
Nro.	**Marca**	**Procesador**	**Memoria RAM**	**Capacidad de Almacenamiento**
1	No especificada	Intel Pentium 4 - 2,80 GHz	512 MB	100 GB
1	No especificada	Intel Pentium - 3.00 GHz	512 MB	100 GB
1	No especificada	Pentium Dual Core - 2.99 GHz	2 GB	260 GB
1	No especificada	Intel Pentium 4 - 2.80 GHz	256 MB	40 GB
Windows Vista Sp3				
Nro.	**Marca**	**Procesador**	**Memoria RAM**	**Capacidad de Almacenamiento**
1	No especificada	Intel Core 2 - 3.00 GHz	2 GB	260 GB

Fuente: Elaboración propia. Recuperado de: Inventario de Equipos Informáticos y Equipos de Computación del GADM-Mira.

Tabla 12: Estaciones de trabajo con Sistema Operativo Windows 7

Windows 7				
Nro.	**Marca**	**Procesador**	**Memoria RAM**	**Capacidad de Almacenamiento**
1	Benq GL 955	Intel Core 2 Quad - 2.66 GHz	4 GB	80 GB
1	No especificada	Intel Core 2 Quad	2 GB	300 GB
1	No especificada	Intel Core 2 Duo - 2,43 GHz	4 GB	500 GB
2	Xtratech	Intel Core I3	2 GB	500 GB
1	No especificada	Intel R Celeron	4 GB	500 GB
1	Hp Pavilion DV5 1137 LA	AMD Turion Dual Core - 2,1 GHz	4 GB	320 GB
9	HP ProDesk 400G1 MT	Core i5	4GB	500 GB
6	Hp ProDesk G1SFF	Core i3 - 3.40 GHz	4GB	500 GB
Windows 7 Ultimate				
Nro.	**Marca**	**Procesador**	**Memoria RAM**	**Capacidad de Almacenamiento**
1	Hp COMPAQ 6000 Pro MT	Intel Core 2 - 2,83 GHz	4 GB	500 GB
2	Hp Elite 7100 MT	Intel Core i3 - 3.07 GHz	4 GB	500 GB
2	Hp COMPAQ 6005 Pro	AMD Anthlon II - 3.00GHz	2 GB	250 GB
2	No especificada	Intel Pentium R	2 GB	500 GB
2	Hp COMPAQ Pro	Intel Core i7 - 3.40 GHz	4 GB	500 GB
Windows 7 Profesional				
Nro.	**Marca**	**Procesador**	**Memoria RAM**	**Capacidad de Almacenamiento**
1	Toshiba Satellite	AMD - 2,20 GHz	2 GB	200 GB
1	No especificada	Intel Core 2 Duo - 2,43 GHz	4 GB	500 GB
1	Hp COMPAQ Pro 6300MT	Intel Core i3 - 3,40 GHz	2 GB	300 GB
2	Hp Probook 4440s	Intel Core i3 - 2,50 GHz	4 GB	500 GB

Fuente: Elaboración propia. Recuperado de: Inventario de Equipos Informáticos y Equipos de Computación del GADM-Mira.

Tabla 13: Estaciones de trabajo con Sistema Operativo Windows 8 y 8.1

Windows 8 Pro				
Nro.	**Marca**	**Procesador**	**Memoria RAM**	**Capacidad de Almacenamiento**
2	Hp ProBook 440G1	Core i3 - 2.4 GHz	4 GB	700 GB
Windows 8.1 Pro				
Nro.	**Marca**	**Procesador**	**Memoria RAM**	**Capacidad de Almacenamiento**
1	Hp 640	Core i7 - 2.90 GHz	4 GB	500 GB

Fuente: Elaboración propia. Recuperado de: Inventario de Equipos Informáticos y Equipos de Computación del GADM-Mira.

Tabla 14: Estaciones de trabajo con otros Sistemas Operativos

Windows Server 2008 SP1				
Nro.	**Marca**	**Procesador**	**Memoria RAM**	**Capacidad de Almacenamiento**
1	HP PROLIANT ML350	Intel (R) Xeon (R) G5 - 1,87 GHz	4 GB	140 GB
Ubuntu				
Nro.	**Marca**	**Procesador**	**Memoria RAM**	**Capacidad de Almacenamiento**
4	Xtratech	Intel Core i3	2 GB	500 GB
Centos OS 2.16				
Nro.	**Marca**	**Procesador**	**Memoria RAM**	**Capacidad de Almacenamiento**
1	DELL	Intel Core 2 Duo	4 GB	320 GB
Mac. Osx, 10.6.8				
Nro.	**Marca**	**Procesador**	**Memoria RAM**	**Capacidad de Almacenamiento**
1	Macintosh	Intel Core 2 Duo	-------	------
NO ESPECIFICADOS				
1	No especificada	Intel Core 2 - 1,86 GHz	1 GB	150 GB
1	HP Proliant ML150 G6	Intel XEON	-----	-------

Fuente: Elaboración propia. Recuperado de: Inventario de Equipos Informáticos y Equipos de Computación del GADM-Mira

3.3.5.8 *Dispositivos de soporte*

El Área de Sistemas del GAD-Mira, en el año 2008 hiso una sugerencia para la adquisición de varios UPS (Uninterruptible Power Supply), los cuales en ese entonces podían proveer de energía eléctrica por un lapso de dos horas continuas, en la actualidad, debido a que su vida útil se ha ido desmejorando, solamente proveen una hora de energía eléctrica; este equipo de soporte se lo utiliza con el fin de que los servidores, equipos de comunicación y sistemas no se apaguen bruscamente en caso de presentarse un corte de energía eléctrica.

3.3.5.9 *Normativa en el GADM del Cantón Mira*

Actualmente no existe una normativa interna con la que el encargado del área de Sistemas pueda regular internamente las infracciones cometidas por el personal o por personas ajenas que cometan alguna falta, ya sea de forma intencionada o involuntaria hacia el recurso informático de la Institución; así que en caso de suscitarse algún tipo de contratiempo, el procedimiento que se debería seguir es comunicarlo a la Fiscalía General del Estado, y el GADM deberá acogerse a las disposiciones que ellos propongan para solucionar el problema.

Dado el caso de que en el proceso investigativo se llegará a detectar algún tipo de delito informático dirigido desde instancias internacionales hacia el GADM-Mira, éste deberá acogerse a la Normativa que ampara la Secretaría Nacional de la Administración Pública en base a los acuerdos que se dictaminan en el Plan Nacional de Gobierno Electrónico ya que el Ecuador se vincula directamente con las leyes, planes, lineamientos y normativas nacionales e internacionales, siendo estos: La Constitución de la República del Ecuador, Plan Nacional del Buen Vivir, estrategias e indicadores de la Organización de las Naciones Unidas (ONU), principios de la Carta Iberoamericana de Gobierno Electrónico (CLAD) y las definiciones de gobierno abierto, gobierno cercano, gobierno eficaz y eficiente, complementados en dicho Plan. (SECRETARÍA NACIONAL DE LA ADMINISTRACIÓN PÚBLICA, 2016)

Según indicó el encargado del Área de Sistemas del GADM-Mira, existe un proyecto en borrador en el que se detallan los instructivos de usuario de herramientas y aplicaciones utilizadas por los empleados de la Institución; pero en caso de ser necesario se firma un acuerdo de responsabilidad por parte del responsable del Área

de Sistemas, Sr. Damián Bastidas en representación del GADM-Mira, y su contraparte, con el fin de salvaguardar la integridad de los activos de la Institución. Para efectos del presente caso de estudio, se convino en subscribir un acuerdo de confidencialidad y no divulgación de información (ver Anexo 7), con el fin de salvaguardar información considerada valiosa, que se haya suministrado durante todo el proceso de la auditoría.

3.3.6 Administración del sistema de red

3.3.6.1 *Gestión del software.*

La gestión del software se realiza manualmente en el equipo terminal que presente problemas, o en caso de que un nuevo funcionario vaya hacer uso del mismo, para lo cual se debe seguir el siguiente procedimiento: el responsable del Área de Sistemas notifica al departamento de Recursos Humanos para que se le asigne un perfil de usuario, en caso de que vaya a hacer uso de algún tipo de sistema o aplicación especial, se la instala en ese momento, y para finalizar, el nuevo empleado debe firmar un acuerdo de responsabilidad de uso del ordenador

3.3.6.2 *Gestión del hardware*

Al momento de hacer la entrega de un activo informático a un funcionario, el responsable del Área de Sistemas registra en su inventario personal, en una hoja de Excel, las especificaciones técnicas, en caso de ser un computador, y la marca y modelo, en caso de una impresora. En caso de presentarse un fallo técnico ya sea en las computadoras, impresoras, o problemas de red; el técnico se dirige al lugar donde se presenta el inconveniente y verifica si se trata de un problema de software o de hardware, en caso de ser una falla manejable se trata de arreglarlo de inmediato, pero si es un problema mayor, se traslada el equipo a la oficina de Sistemas para darle una solución, una vez que se haya solucionado el problema, se pone nuevamente al equipo en funcionamiento.

En caso de que el equipo ya haya cumplido con su tiempo de vida útil y se lo deba dar de baja, se lo lleva a la bodega en donde el encargado del área de sistemas hace una revisión final y con ello se realiza un informe con la respectiva recomendación de que el equipo necesita ser dado de baja, ya una vez que se cumple con todo el trámite

administrativo, se borra toda la información que este contenga y se lo lleva a una recicladora para evitar afectaciones al medio ambiente.

3.3.6.3 *Gestión del antivirus.*

Hace un año la administración del servicio de antivirus y sus respectivas actualizaciones para cada uno de los ordenadores del GADM-Mira se realizaba mediante un servidor (RAID 0), actualmente, la instalación de todo el paquete de antivirus se realiza de forma manual en cada ordenador. La empresa que provee de este servicio es ESET, a través de un contrato vigente por el lapso de tiempo de un año, así que la Institución posee una Licencia original otorgada por dicha empresa privada, por lo que solo se debe ingresar la contraseña en la interfaz gráfica del antivirus y el servicio queda en total funcionamiento por un año entero.

3.3.6.4 *Gestión de la central telefónica.*

En cuanto a la gestión de la central telefónica cabe señalar que no se ha explotado todas las utilidades que está brinda, ya que solo se ha realizado varias restricciones de las extensiones, y se restringe los tiempos excesivos de llamadas telefónicas o de larga distancia, eso se debe a que la garantía de la central ha finalizado, y en caso de presentarse algún fallo se debe realizar un gasto extra por mal manejo.

3.3.6.5 *Software de monitoreo.*

El encargado del Área de Sistemas del GADM-Mira hace uso de una aplicación que permite hacer un reconocimiento de todos los enlaces inalámbricos operativos en tiempo real, esto con el fin de verificar mediante un ping todos los enlaces que están activos, y en caso de que algún enlace falle tratar de darle una solución lo más breve posible.

3.3.7 Responsabilidades del Área de Sistemas del GADM-Mira

3.3.7.1 *Misión.*

Mantener estándares para el análisis, diseño, programación, implementación y pruebas de sistemas de información de acuerdo a las metodologías establecidas,

realizando actividades de actualización y/o mantenimiento de sistemas de información.

3.3.7.2 *Reglamento orgánico funcional.*

Según el Reglamento Orgánico Funcional por procesos para resultados sustitutivos del Gobierno Autónomo Descentralizado del Cantón Mira el responsable de los sistemas informáticos debe cumplir con las siguientes competencias:

a) Implementar y ejecutar las políticas y procedimientos en el área de desarrollo y programación que permitan organizar la tecnología de la información y comunicación en la Institución;
b) Implementar y ejecutar el plan informático estratégico de tecnología en el área de programación que permitan regular el crecimiento informático;
c) Establecer mecanismos que protejan y salvaguarden contra pérdidas y fugas la información que se procesa en los sistemas informáticos;
d) Ejecutar el plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado a su área;
e) Asistir y coordinar el sitio web Institucional;
f) Coordinar en los proyectos informáticos, los estándares para el análisis, diseño, programación e implantación de los sistemas de información;
g) Mantener actualizados y en correcto funcionamiento los sistemas informáticos en base a los requerimientos de la Institución;
h) Mantener respaldos periódicos y actualizados de los sistemas
i) Efectuar el mantenimiento de los sistemas de información, cumpliendo con las normas y estándares establecidos, niveles de seguridad, calidad y performance requeridos;
j) Actualizar la documentación técnica de los aplicativos informáticos.

3.3.7.3 *Instaladores.*

La mayor parte de instaladores que utilizan los diferentes departamentos se encuentran en CD’s originales y se los almacena en un estante en la oficina de sistemas, los paquetes que más se instalan son los sistemas operativos, los utilitarios de office, drivers, y otros tipos de softwares como sistemas y aplicaciones propias de cada

departamento; en caso de no existir las versiones originales de los programas instalados se utilizan parches que no son originales los cuales se descargan de Internet.

3.3.7.4 *Licencias.*

Las únicas computadoras que cuentan con licencias originales de Windows son las laptops y varias computadoras que manejan los jefes departamentales; los servidores son desarrollados bajo software libre; pero en caso de ser licenciados, cuentan con una licencia original dependiendo de la versión de Windows que se haya utilizado. Las licencias no tienen un tratamiento especial ya que se realiza un procedimiento mecánico en caso de instalar algún programa que sea licenciado.

3.3.7.5 *Documentación.*

Como información tangible en documentos físicos el GADM-Mira posee la siguiente documentación, a la cual es posible acceder únicamente con el consentimiento del encargado del Área de Sistemas:

- Registro de direcciones IP
- Inventarios de los recursos informáticos
- Manual de uso del Internet
- Acuerdos de confidencialidad del uso de sistemas
- Diagramas topológicos de la red LAN cableada
- Diagramas topológicos de la red LAN inalámbrica
- Planos del cableado estructurado del edificio del GADM-Mira

CAPITULO IV

4. APLICACIÓN DE LA METODOLOGÍA

4.1 DESCRIPCIÓN GENERAL

Haciendo referencia a la sección tres del estándar COBIT 5 para la Seguridad de la Información, la cual trata sobre la adaptación del estándar al entorno de la organización, recomienda que es necesario la utilización de herramientas de autoevaluación, medición y diagnóstico; por consiguiente será necesario el uso y total comprensión del manual de metodologías escogido, para el caso el OSSTMM en su versión 3, como una herramienta evaluativa de la situación actual de la red de datos del GADM-Mira. Si bien la metodología recomienda que se haga una revisión exhaustiva de la legislación que regula la región, para cada canal auditado, varias fuentes legislativas importantes, ya se han considerado en el Capítulo II.

También se utilizó los criterios del estándar COBIT para la creación de la primera versión del manual de políticas de seguridad de la información del GADM-Mira, ya que esta entidad carece de este importante recurso legal; esto con la finalidad de cubrir los puntos más vulnerables encontrados, luego de finalizar el proceso de la auditoría.

4.2 TIPO DE PRUEBA

El Manual de Metodologías de Seguridad OSSTMM versión 3, expone seis tipos de pruebas: Hacking Ético, Caja Negra, Caja Gris, Caja Blanca, Tándem e Inversión; de las cuales se optó por escoger la de caja gris para desarrollar las pruebas de cada uno de los canales, a fin de que la persona responsable del Área de Sistemas del GADM-Mira tenga la posibilidad de poner a punto sus mecanismos de defensa con antelación; y el auditor pueda obtener datos más reales de las pruebas realizadas.

Según (Herzog, 2010), la prueba de Caja Gris consiste en tener un conocimiento limitado de las defensas del objetivo y de los activos que éste posee; por esta razón es necesario que la persona encargada del Área de Sistemas del GADM-Mira, brinde al analista cierta información antes de iniciar con las pruebas para los diferentes canales a evaluar: humano, físico, de comunicaciones inalámbricas, de telecomunicaciones y de redes de datos.

Para poder dar inicio al proceso de la auditoría, se contó con el debido permiso del encargado del Área de Sistemas del GADM-Mira, con el fin de poder intervenir tanto en el personal de la entidad, como en sus equipos; y en caso de ser necesario, para extraer la información requerida fuera de la Institución. Este permiso se lo obtuvo a través de la emisión de un oficio (ver Anexo 8), en el que también se propone un cronograma de actividades con el cual se pretende organizar las pruebas de cada canal en lapsos de tiempo establecidos, y para que la Institución se prepare de antemano para las mismas.

4.3 MÉTRICAS OPERACIONALES APLICADAS

El RAV (ver página 12) es una medición a escala de la superficie de ataque, la cantidad de interacciones no controladas con un objetivo, que se calcula por el equilibrio cuantitativo entre las operaciones, limitaciones y controles. Contar con los ravs es entender cómo gran parte de la superficie de ataque está expuesta. En esta escala, 100 rav, es un equilibrio perfecto; menos de 100 rav significa que existen pocos controles y, por tanto, una superficie de ataque mayor. Más de 100 rav muestra que existen más controles de los necesarios, lo que a su vez puede ser un problema, ya que los controles a menudo añaden interacciones dentro de un ámbito, así como cuestiones de complejidad y mantenimiento, (Herzog, 2010). La manera de cómo se relacionan las tres medidas operacionales (porosidad, controles y limitaciones); se la evidencia en la Tabla 15.

Tabla 15: Relación de la Porosidad, Controles y Limitaciones

Categoría		**Seguridad Operacional**	**Limitaciones**
Operaciones		Visibilidad	Exposición
		Acceso	
		Confianza	Vulnerabilidad
Controles	Clase A	Autenticación	Debilidad
		Indemnización	
		Resistencia	
		Subyugación	
		Continuidad	
	Clase B	No-Repudio	Preocupación
		Confidencialidad	
		Privacidad	
		Integridad	
		Alarma	
			Anomalía

Fuente: Elaboración propia. Recuperado de: (Herzog, 2010)

De la tabla anterior se toman los criterios para formular las siguientes ecuaciones:

4.3.1 Porosidad

La Seguridad Operacional, también conocida como la porosidad del alcance, es el primer valor a calcular de los tres factores que permiten obtener la medición de la Seguridad Actual de los canales auditados: humano, físico, de comunicaciones inalámbricas, telecomunicaciones y redes de datos. Se mide como la suma de la Visibilidad $(\boldsymbol{P_V})$, el Acceso $(\boldsymbol{P_A})$ y la Confianza $(\boldsymbol{P_T})$ del alcance. (Herzog, 2010)

Para ello fue necesario aplicar la siguiente ecuación:

$$\boldsymbol{OpSec_{sum} = P_V + P_A + P_T} \qquad \textbf{(1)}$$

Ecuación 1: Seguridad Operacional
Fuente: Elaboración Propia. Recuperado de: (Herzog, 2010)

4.3.2 Controles

El siguiente paso para calcular el RAV es definir los controles, que no son nada más que los mecanismos de seguridad puestos en marcha para proteger la seguridad operacional. Para obtener el valor de LC_{sum} o Suma de los Controles, se debe sumar los 10 tipos de los controles, explicados en el capítulo II (páginas 15 a la 19); mismos que encuentran divididos en dos grupos de 5 cada uno, así: Controles de clase A: Autenticación (TC_{Au}), Identificación (TC_{Id}), Resistencia (TC_{Re}), Subyugación (TC_{Su}) y Continuidad (TC_{Ct}); y los Controles de clase B: No-Repudio (TC_{NR}), Confidencialidad (TC_{Cf}), Privacidad (TC_{Pr}), Integridad (TC_{It}) y Alarma (TC_{Al}) (Herzog, 2010).

Por lo tanto la Suma de los Controles está dada por la siguiente ecuación:

$$\boldsymbol{TC_{sum} = TC_{Au} + TC_{Id} + TC_{Re} + TC_{Su} + TC_{Ct} + TC_{NR} + TC_{Cf} + TC_{Pr} + TC_{It} + TC_{Al}} \qquad \textbf{(2)}$$

Ecuación 2: Suma de los Controles
Fuente: Elaboración Propia. Recuperado de: (Herzog, 2010)

4.3.2.1 *Controles Ausentes.*

Los Controles Ausentes MC_{sum}, se calculan para equilibrar el valor de pérdida de $OpSec_{sum}$ y se calculan con el fin de evaluar el valor de las restricciones de seguridad; por lo tanto deben calcularse de forma individual para cada una de las diez categorías

de los controles. Por ejemplo para determinar los Controles Ausentes de la Autenticación MC_{Au}, hay que restar $OpSec_{sum} - TC_{Au}$; pero siempre se debe tomar en cuenta que los Controles Ausentes nunca pueden ser menor que cero, por lo tanto se debe cumplir con la siguiente condición: (Herzog, 2010)

$$\text{Si } OpSec_{sum} - TC \leq 0$$

$$\text{Entonces } MC_{Au} = 0$$

$$\text{Sino } MC_{Au} = OpSec_{sum} - LC_{Au}$$

El resultado de los Controles Ausentes total (MC_{sum}), se debe calcular sumando individualmente cada uno de los 10 Controles, tal como se ve a continuación:

$$\boldsymbol{MC_{sum} = MC_{Au} + MC_{Id} + MC_{Re} + MC_{Su} + MC_{Ct} + MC_{NR} + MC_{Cf} + MC_{Pr} + MC_{It} + MC_{Al}} \quad \textbf{(3)}$$

Ecuación 3: Suma de los Controles Ausentes
Fuente: Elaboración Propia. Recuperado de: (Herzog, 2010)

4.3.3 Limitaciones

Finalmente se debe calcular el valor numérico de las Limitaciones, mismas que se ponderan de manera individual, verificándolas siempre que sea posible. Haciendo referencia a la tabla 15, se puede evidenciar que los valores de las Exposiciones (L_E), y Vulnerabilidades (Lv), son dependientes de la Porosidad u $OpSec_{sum}$, de esta manera: Visibilidad y Acceso para la Exposición, y Confianza para la Vulnerabilidad. La ponderación de las Debilidades (L_w) y Preocupaciones (L_C) están basadas en una relación con los Controles aplicados al objetivo; y para el caso de las Anomalías (L_A), la existencia de otras limitaciones también juega un papel importante en su ponderación. (Herzog, 2010).

4.3.3.1 *Exposición.*

Para encontrar el valor de la Exposición es necesario contabilizar cada acción injustificable, falla o error que proporcione una visibilidad directa o indirecta de los objetivos o los activos dentro del alcance en el canal elegido. (Herzog, 2010)

4.3.3.2 *Vulnerabilidad.*

Para ponderar las Vulnerabilidades es necesario contabilizar por separado cada falla o error que desafía las protecciones mediante el cual una persona o proceso puede ganar el acceso, denegar el acceso a los demás, u ocultarse o activarse dentro del alcance. (Herzog, 2010)

4.3.3.3 *Debilidad.*

El valor de la Debilidad se calcula contabilizando cada defecto o error en los controles interactivos o de Clase A: Autenticación (FC_{Au}), Indemnización (FC_{Id}), Resistencia (FC_{Re}), Subyugación (FC_{Su}) y Continuidad (FC_{Ct}). (Herzog, 2010)

Por lo tanto:

$$\boldsymbol{L_w = FC_{Au} + FC_{Id} + FC_{Re} + FC_{Su} + FC_{Ct}} \qquad \textbf{(4)}$$

Ecuación 4: Ecuación de la Debilidad
Fuente: Elaboración Propia. Recuperado de: (Herzog, 2010)

4.3.3.4 *Preocupación.*

Para encontrar el valor de este segmento en necesario contabilizar cada defecto o error en los controles de proceso o de Clase B: No-repudio (FC_{NR}), Confidencialidad (FC_{Cf}), Privacidad (FC_{Pr}), Integridad (FC_{It})y Alarma (FC_{Al}). (Herzog, 2010)

Por lo tanto:

$$\boldsymbol{L_C = FC_{NR} + FC_{Cf} + FC_{Pr} + FC_{It} + FC_{Al}} \qquad \textbf{(5)}$$

Ecuación 5: Ecuación de la Preocupación
Fuente: Elaboración Propia. Recuperado de: (Herzog, 2010)

4.3.3.5 *Anomalía.*

Para encontrar el valor de este segmento en necesario contabilizar cada elemento identificable o desconocido que no puede tenerse en cuenta en las operaciones normales, generalmente cuando el origen o el destino del elemento no pueden ser entendidos. Una anomalía puede ser una señal temprana de un problema de seguridad, una auditoría de seguridad adecuada requiere que se tome nota de cualquier anomalía.

4.3.4 Calculadora RAV

Los valores numéricos que se obtendrán de las tres medidas para el cálculo del RAV (Porosidad, Controles y Limitaciones); y sus respectivos subíndices se obtendrán de las pruebas que recomienda la metodología. Una manera sencilla y simple para hacer un RAV es utilizar las hojas de cálculo creadas específicamente para calcular la superficie de ataque y diversas métricas requeridas, a partir de los datos obtenidos de la prueba. Esta hoja se encuentra disponible en el sitio web de ISECOM (http://www.isecom.org/research/ravs.html), en formato de una hoja de Excel; en dicha hoja, el auditor sólo tiene que introducir los valores en los cuadros vacíos o en blanco y el resto de los cálculos se manejarán de forma automática (Herzog, 2010).

Una vez que se hayan introducido los valores indicados para cada ítem de la **Porosidad (OPSEC):** Visibilidad, Acceso y Confianza; **Controles**: Autenticación, Indemnización, Resistencia, Subyugación, Continuidad, No-Repudio, Confidencialidad, Privacidad, Integridad y Alarma; y **Limitaciones:** Vulnerabilidad, Debilidad, Preocupación, Exposición y Anomalía; automáticamente se mostraran en la Tabla los demás valores de medición.

Cuando ya se obtengan los resultados finales en la Hoja calculadora del RAV, se puede realizar una interpretación de los resultados obtenidos del canal auditado haciendo uso de dos expresiones, la primera es **Seguridad Δ,** que no es nada más que el equilibrio que existe entre los valores numéricos de la **porosidad**, los **controles** y las **limitaciones**, por lo tanto, dependiendo del signo que éste posea: positivo (+) o negativo (-), se pueden considerar los siguientes aspectos: un delta positivo muestra lo mucho que se gasta en controles o incluso si el exceso de gasto es demasiado en un tipo de control; un delta negativo muestra una falta de controles o que se controlan a sí mismos con limitaciones que no pueden proteger adecuadamente al objetivo. (Herzog, 2010). Este valor puede ser verificado en base al siguiente criterio tomado de la hoja de cálculo del RAV:

$$\textbf{Seguridad}\ \Delta = \textbf{Controles Verdaderos} - \textbf{OPSEC} - \textbf{Limitaciones} \qquad \textbf{(6)}$$

Ecuación 6: Ecuación para el cálculo del Seguridad Δ
Fuente: Elaboración Propia. Recuperado de: Calculadora RAV de OSSTMM3

La segunda expresión es la **Seguridad Actual,** que no es nada más que un término para mostrar una imagen de una superficie de ataque en un entorno operativo. Es una representación logarítmica de los controles, limitaciones y porosidad en un momento determinado en el tiempo. Es logarítmica, ya que representa la realidad del tamaño cuando una aplicación tendrá una superficie de ataque más grande, aunque matemáticamente los controles equilibran la porosidad. Otro beneficio de la representación matemática de una superficie de ataque por medio de la seguridad actual es que a más de mostrar donde las medidas de protección son deficientes, también se puede demostrar lo contrario. Dado que es posible tener más controles de los que uno necesita, esto se puede representar matemáticamente como más de 100 ravs. La representación matemática es útil para mostrar las pérdidas económicas, ya que puede ser utilizado para demostrar que el dinero se gastó en tipos incorrectos de controles o controles redundantes. (Herzog, 2010)

4.3.5 Presentación de informes con The STAR

Una vez que se haya corroborado que todos los datos obtenidos con la hoja de cálculo del RAV son los correctos, se procede a hacer uso de The STAR por sus siglas en inglés (Security Test Auditing Report). La finalidad del Informe de Auditoria de Pruebas de Seguridad es servir como un resumen ejecutivo de cálculo preciso indicando la Superficie de Ataque de los objetivos analizados, dentro de un alcance particular. ISECOM en su sitio web (http://www.isecom.org/mirror/STAR.3.pdf), proporciona una plantilla que debe ser llenada manualmente con los valores obtenidos de las pruebas realizadas en el canal auditado y debe contar con la firma de verificación del auditor. (Herzog, 2010)

En lo posterior, para diferenciar cada criterio que se tomará en cuenta en la suma del valor numérico total de cada inciso, para cada uno de los canales probados, se lo marcará con un asterisco, así: **(*)**; por lo que en caso de ser necesaria una explicación más clara del valor obtenido, se debe verificar el análisis realizado en las tablas, imágenes o explicaciones descritas.

4.4 PRUEBAS DE SEGURIDAD HUMANA

Si bien este canal trata de medir el nivel de defensa del personal de una institución hacia sus activos y hacia los activos de la institución en sí, ya que el guardián de los activos puede asegurar que el personal cuida muy bien de ellos, pero es necesario medir esta afirmación con datos reales; para ello será necesario aplicar varias técnicas de ingeniería social; pues el verdadero objetivo del cumplimiento de las pruebas de seguridad en este canal, es la concienciación del personal de seguridad y la medición del desfase con la norma de seguridad requerida que se indica en la política de la organización, regulaciones de la industria, o la legislación regional. (Herzog, 2010)

4.4.1 Encuesta

Para realizar la encuesta en el GADM-Mira se tomó como referencia el directorio completo de los empleados de planta central de la institución, vigente en el año 2016 (ver Anexo 9), en él se contabilizaron un total 79 empleados. Basándose en el orgánico estructural por procesos aprobado a la fecha, en la sección de proceso habilitante de apoyo, se contabilizaron diez áreas departamentales, el cual está compuesto por: dirección financiera, tesorería, presupuesto, contabilidad, rentas y recaudación, dirección administrativa, talento humano, compras públicas, bodega, a ésta también se incluye el Área de Sistemas. Para poder acceder al directorio de los empleados se lo puede hacer de dos maneras: descargándolo de la página web oficial del municipio (www.mira.gob.ec), o a través de una solicitud de acceso a la información pública (ver Anexo 10)

Para obtener resultados que reflejen el objetivo de la encuesta, se aplicó el principio de muestreo por criterio, el cual según (Estupiñán Gaitán, 2007) dice que: “es aquel en que las partidas que se han de revisar de un universo, se seleccionan con un fundamento en el criterio del auditor”, este criterio se aplicó con la finalidad de extraer una muestra representativa del universo, que en este caso serían los 79 empleados de planta central de la Institución, y que además interactúen con el Área de Sistemas de la Institución.

En consecuencia se diseñaron 10 encuestas, mismas que se repartieron de la siguiente manera:

- 1 al encargado de la oficina de recaudación

- 3 a los empleados del área de contabilidad
- 1 tesorería
- 2 a los encargados de las bodegas
- 1 al funcionario de compras públicas
- 1 al jefe administrativo
- 1 al responsable del departamento de sistemas

Cabe recalcar que las encuestas fueron diseñadas de tal manera que ninguna de las personas encuestadas se sienta comprometida con los resultados obtenidos; por lo tanto se optó porque sean anónimas, con el fin de obtener criterios de evaluación más reales; el diseño y tabulación de las mismas se encuentra en el Anexo 11.

4.4.2 POROSIDAD

4.4.2.1 *Visibilidad (P_V).*

Enumerar el personal dentro del alcance para el acceso, tanto a los autorizados y a los no autorizados a los procesos dentro del objetivo, sin importar el tiempo o el tipo de acceso, y el método para la obtención de esos datos (Herzog, 2010). En la Tabla 16, se muestra el análisis aplicado para obtener el valor numérico de este apartado, el cual hace referencia a las recomendaciones de la metodología.

Tabla 16: Resultados de la Visibilidad para el canal humano

Visibilidad		
Técnica	Observación y Persuasión	
Objetivo	Cuarto de telecomunicaciones	
Departamentos y Áreas	**Sistemas (*)** **Comunicación (*)** **Dirección de Planificación (*)** **Área Financiera (*)** **Personal de seguridad (*)**	Dirección de Sistemas Rentas y Recaudación Contabilidad Tesorería Bodega Compras Públicas Dirección Administrativa Secretaría General
Enumeración de Personal	Autorizado	No Autorizado

Fuente: Elaboración propia.

El valor numérico de la **Visibilidad** en el canal Humano es de: $\boldsymbol{P_V}$ **= 5**; este valor se obtiene contabilizando los valores marcados de la tabla anterior, luego de realizar la enumeración del personal autorizado para los procesos dentro del objetivo (cuarto de comunicaciones), cabe señalar que se aplicó la técnica de la observación y persuasión en un lapso de cinco días diferentes para obtener valores más reales.

4.4.2.2 *Acceso (P_A).*

El acceso se calcula en base al número de lugares diferentes donde puede ocurrir una interacción. Si bien el acceso del personal fuera de su estación de trabajo es un verdadero escenario, utilizado a menudo para robar la propiedad de la información, esto se puede limitar utilizando interacciones solamente en el alcance para proteger los derechos del personal en su vida privada (Herzog, 2010).

En la Tabla 17, se puede apreciar el análisis aplicado para encontrar el valor numérico de este apartado, señalando que no se aplicó los escenarios fuera de las estaciones de trabajo de cada empleado, con el fin de no interferir en la vida privada de los mismos.

Tabla 17: Resultados del Acceso para el canal humano

Acceso		
Técnica	Encuestas	
Proceso de Acceso	Cuarto de telecomunicaciones	**Computadoras personales (*)** **Dispositivos móviles (*)** **Contraseñas de acceso (*)** **Herramientas informáticas (*)**
Autoridad	Guardia	Jefe de Sistemas
Autenticación	Requiere Autorización	No requiere Autorización

Fuente: Elaboración propia.

El valor numérico para el **Acceso** en el canal humano es igual a: $\boldsymbol{P_A}$ **= 4**; este valor se lo obtiene sumando los cuatro valores marcados en la tabla anterior, mismos que corresponden a los diferentes tipos escenarios en donde pueden ocurrir una interacción sin que se necesite una autorización del empleado guardián de la información generada en su estación de trabajo (computadoras personales, dispositivos móviles, contraseñas y herramientas informáticas).

4.4.2.3 *Confianza (P_T).*

Probar la confianza entre el personal dentro del alcance, donde la confianza se refiere al acceso a la información o a los activos físicos de otros objetivos dentro del alcance (Herzog, 2010). En la Tabla 18 se puede apreciar el análisis dispuesto para calcular el valor numérico de este apartado.

Tabla 18: Resultados de la Confianza para el canal humano

	Confianza
Técnica	Llamada telefónica falsa
Personal	Funcionarios de Sistemas Guardias
Información Obtenida	**Uso de credenciales (*)** **Acceso a las oficinas (*)** **Acceso a los activos físicos (*)**

Fuente: Elaboración propia.

Contabilizando los valores marcados con un asterisco en la tabla anterior, se obtiene un valor numérico para la **Confianza,** en el canal humano igual a: $\boldsymbol{P_T = 3}$**.** Esto se debe a que se consideró tres puntos primordiales para medir el acceso en este ítem, dirigido hacia los funcionarios de área de sistemas y al personal de seguridad del GADM-Mira, de donde se verificó que necesitan el **uso de credenciales especiales** para acceder a áreas restringidas, a **las estaciones de trabajo de otros empleados** y a los **activos físicos de la Institución.**

Una vez que se ha obtenido las ponderaciones de la Visibilidad, el Acceso y la Confianza de canal auditado, se procede a calcular el valor numérico total de la **Porosidad** u $\boldsymbol{OpSec_{sum}}$, para ello es necesario aplicar la Ecuación 1; así:

$$\boldsymbol{OpSec_{sum} = P_V + P_A + P_T}$$

$$\boldsymbol{OpSec_{sum} = 5 + 4 + 3}$$

$$\boldsymbol{OpSec_{sum} = 12}$$

4.4.3 CONTROLES

Se deben realizar pruebas para enumerar los tipos de controles utilizados para proteger el valor de los activos de la organización auditada. (Herzog, 2010)

4.4.3.1 *Autenticación (LC_{Au}).*

Enumerar y probar las deficiencias del personal de recepción y los privilegios que se requieren para interactuar con ellos, con el fin de asegurar que sólo las partes identificables, autorizadas y grupos destinados tengan acceso. Se requiere que la autorización e identificación conformen el proceso para el correcto uso del mecanismo de autenticación (Herzog, 2010). En la Tabla 19 se muestra el análisis aplicado para encontrar el valor numérico de este ítem.

Tabla 19: Resultados para el control de Autenticación para el canal humano

Autenticación		
Técnica	Observación y persuasión	
Instancias	Entrada principal Oficinas de servicios a la ciudadanía Bodegas Áreas restringidas	
Contabilización de Solicitudes	**Biométrico (*)** **Sistemas o aplicaciones de uso municipal (*)** **Oficios (*)** **Petición formal (*)**	 Alcaldía Oficinas de planta externa

Fuente: Elaboración propia.

Mediante la aplicación de la técnica de ingeniería social de observación y persuasión, se pudo contabilizar cuatro métodos para la autenticación en varias instancias del GADM-Mira y que permiten que se pueda interactuar con el personal de recepción (contabilizando los valores marcados de la tabla anterior); estos son: el sistema biométrico, sistemas de uso municipal, oficios y peticiones formales; por lo tanto el valor numérico de la **Autenticación** en este canal es igual a: $\boldsymbol{LC_{Au} = 4}$; cabe señalar que para poder acceder a la alcaldía previamente se debe haber dirigido un oficio al señor alcalde, y para acceder a las oficinas de planta externa se debe realizar una petición formal al jefe departamental que esté a cargo de la misma.

4.4.3.2 *Indemnización (LC_{Id}).*

Documentar y enumerar el abuso o la elución de las políticas del empleado, seguros, acuerdos de no divulgación, no competencia, de responsabilidad, o renuncias de uso/usuario con todo el acceso al personal dentro del alcance. (Herzog, 2010). Aplicando la técnica de la llamada telefónica falsa, se pudo descubrir que los

documentos legales que resguardan el recurso informático del GADM-Mira son los que se muestran en la siguiente lista:

- **Actas de responsabilidad en seguridad de la información (*)**
- **Acuerdo de confidencialidad e integridad (*)**
- **Pólizas de seguros con empresas privadas de seguridad (*)**
- **Renuncias de usuario o de uso (*)**

Por lo tanto, sumando los valores marcados de la lista anterior se tiene un valor numérico para la **Indemnización** de: $\boldsymbol{LC_{Id} = 4}$, ya que existen cuatro tipos de documentos legales que permiten proteger legalmente la integridad del recurso informático del GADM-Mira y para los cuales el personal debe someterse a cumplir.

4.4.3.3 *Resistencia (LC_{Re}).*

Enumerar y probar las insuficiencias del personal dentro del alcance, para lo cual la eliminación o la tranquilidad del personal de recepción, permitirá el acceso directo a los activos; en otras palabras a "fallar de forma segura" (Herzog, 2010).

En la Tabla 20 se pueden observar los resultados obtenidos para este ítem, en él se medirá la resistencia para el ingreso al cuarto de telecomunicaciones, ya que es el espacio más sensible del sistema informático.

Tabla 20: Resultados para el control de Resistencia para el canal humano

Resistencia	
Técnica	Observación y persuasión
Personal que pueden acceder a los activos del cuarto de telecomunicaciones	• **Encargado del Área de Sistemas (*)** • Personal de seguridad • Secretaria General • Secretaria Financiera • Comunicación

Fuente: Elaboración propia.

El valor numérico asignado para la **Resistencia** en este canal es de $\boldsymbol{LC_{Re} = 1}$, ya que de la tabla anterior se puede constatar que el único valor marcado corresponde al encargado del área de sistemas, quien es la única persona que posee acceso al cuarto de telecomunicaciones sin algún tipo de restricción, a pesar de que existen cuatro personas más que cuidan del mismo y poseen una confianza elevada.

4.4.3.4 *Subyugación (LC_{Su}).*

Enumerar y poner a prueba las insuficiencias de los activos comunicados a través de canales en los que los controles no son necesarios, pueden ser eludidos o ignorados, como el correo electrónico inseguro o sobre una línea telefónica pública. Difiere de ser una limitación de seguridad para un objetivo, ya que se aplica al diseño o a la implementación de los controles. (Herzog, 2010)

En control de **Subyugación,** para el canal auditado (humano), posee un valor numérico de $\boldsymbol{LC_{Su} = 0}$, ya que al momento de realizar la auditoría se comprobó que no existen ni física ni digitalmente instructivos que el personal deba seguir en el caso de interactuar con otra persona o con sus máquinas de trabajo o en caso de suscitarse algún tipo de error laboral, solo se los establecieron documentos en borrador y se ha hecho una socialización de los mismos, pero lamentablemente no se los aplica adecuadamente.

4.4.3.5 *Continuidad (LC_{Ct}).*

Enumerar y comprobar las insuficiencias de todo el personal con respecto a los retrasos de acceso y el tiempo de respuesta del servicio a través del personal de apoyo o medios automatizados para el acceso al personal alternativo de recepción. La Continuidad es el término general para características tales como la capacidad de supervivencia, balanceo de carga y redundancia. (Herzog, 2010). En la Tabla 21 se puede apreciar el análisis aplicado para calcular el valor numérico de este ítem, en donde además de los métodos de ingeniería social de observación y persuasión, se tomó algunos valores obtenidos de las encuestas realizadas.

Tabla 21: Resultados para el control de Continuidad para el canal humano

Continuidad		
Técnica	Observación y persuasión	
Situaciones	Enfermedad o calamidad Vacaciones Viaje Problemas externos	
Cargos aplicados	Directores departamentales Secretarias Guardias Personal de apoyo	**Genera conflictos (*)** No genera conflictos No genera conflictos No genera conflictos

Fuente: Elaboración propia.

El valor numérico obtenido para el control de **Continuidad** para este canal es de $\boldsymbol{LC_{Ct} = 1}$, ya que de la tabla anterior, se puede verificar que el valor marcado corresponde a los cargos de los directores departamentales, quienes generan conflictos cuando no se encuentran por alguna razón en su estación de trabajo.

4.4.3.6 *No repudio (LC_{NR}).*

Enumerar y probar el uso o las deficiencias del personal de recepción para identificar y registrar adecuadamente el acceso o las interacciones con los activos, mostrando evidencias específicas para desafiar el repudio. El control de No repudio depende de la identificación y la autorización para establecerse y ser aplicado adecuadamente sin limitaciones. Documentar la profundidad de la interacción que se registra (Herzog, 2010).

En la Tabla 22 se puede apreciar el análisis que se llevó a cabo para encontrar el valor numérico de este ítem.

Tabla 22: Resultados para el control de No repudio para el canal humano

No repudio		
Técnica	Observación	Encuestas
Aplicada al personal de recepción	Planta central	No posee registros
	Ex patronato municipal	No posee registros
	Centro gerontológico	**Posee registros (*)**
	Garajes	No posee registros
	Complejo deportivo	**Posee registros (*)**

Fuente: Elaboración propia.

El valor numérico asignado para el **No repudio** en este canal es de $\boldsymbol{LC_{NR} = 2}$, ya que el personal de recepción de tres partes externas del GADM-Mira diferentes, de las cinco tomadas en cuenta en la tabla anterior, poseen un registro de acceso de las personas que acceden a los activos de la Institución.

4.4.3.7 *Confidencialidad (LC_{Cf}).*

Enumerar y probar el uso o insuficiencias de todos los segmentos de comunicación con el personal dentro del alcance a través de un canal específico, o propiedades transportadas usando líneas seguras, encriptación, interacciones personales "cercanas" o "silenciosas" para proteger la confidencialidad de los activos de información que

sólo conocen los que tienen la debida autorización de seguridad de ese activo (Herzog, 2010). En la Tabla 23 se puede observar el análisis realizado para obtener el valor numérico de este ítem.

Tabla 23: Resultados para el control de Confidencialidad para el canal humano

Confidencialidad		
Técnicas	Observación y persuasión	Encuestas
Tipos de comunicación	**Líneas seguras**	**Eficiente (*)**
	Encriptación	**Eficiente (*)**
	Susurro	Ineficiente
	Verbal directa	Ineficiente
	Central telefónica	Ineficiente
	Documentos Físicos	Ineficiente
	Correo electrónico institucional	**Eficiente (*)**
	Aplicaciones de mensajería instantánea	Ineficiente

Fuente: Elaboración propia.

Contabilizando los valores marcados con un asterisco de la tabla anterior, se obtiene un valor numérico para el control de **Confidencialidad** en este canal de: $\boldsymbol{LC_{Cf} = 3}$**,** esto se debe a que de los 8 métodos utilizados para distribuir información importante entre el personal del GADM-Mira, cinco mostraron ser ineficientes: el susurro, la comunicación verbal directa, usando la central telefónica, el uso de documentos físicos, y haciendo uso de las aplicaciones de mensajería instantánea; por lo tanto se comprobó que los métodos más seguros son la comunicación por líneas seguras, hacer uso de algún método de encripción de datos y el uso del correo electrónico institucional.

4.4.3.8 *Privacidad (LC_{Pr}).*

Enumerar y probar el uso o deficiencias de todos los segmentos de comunicación con el personal dentro del alcance a través de un canal o propiedades transportadas utilizando específicamente firmas individuales, identificación personal, interacciones personales "calladas" o "a puerta cerrada" para proteger la privacidad de la interacción y el proceso de proporcionar activos sólo a aquellos dentro de la autorización de seguridad adecuada para ese proceso, información o activos físicos (Herzog, 2010).

En la Tabla 24 se puede apreciar el análisis aplicado apara obtener el valor numérico de este ítem.

Tabla 24: Resultados para el control de Privacidad para el canal humano

Privacidad		
Técnica	Observación	Encuestas
Métodos probados	Firmas individuales Identificaciones personales **Interacciones personales**	Deficiente Deficiente **Eficiente (*)**

Fuente: Elaboración propia.

Verificando los valores marcados de la tabla anterior, se concluye que el valor numérico para el control de **Privacidad** para este canal es de $\boldsymbol{LC_{Pr} = 1}$, ya que a pesar del uso de firmas e identificaciones es posible vulnerar este control y sólo pude ser logrado para este caso, mediante interacciones que se desarrollen de manera personal, en dónde intervengan sólo las partes involucradas en un ambiente cerrado o en una estación de trabajo privada.

4.4.3.9 *Integridad (LC_{It}).*

Enumerar y probar las insuficiencias en todos los segmentos de comunicación dentro del alcance, donde los activos son transportados por un canal mediante un proceso documentado, firmado, cifrado, encriptado, o con marcas para proteger y asegurar que la información de los activos físicos no puedan ser cambiados, conmutados, re-dirigidos o invertidos sin que las partes involucradas tengas conocimiento de ello (Herzog, 2010).

En la Tabla 25, se puede apreciar el análisis realizado para obtener el valor numérico de este ítem.

Tabla 25: Resultados para el control de Integridad para el canal humano

Integridad		
Técnica	Observación	Encuestas
Métodos probados	Procesos documentados **Firmas** Cifrado Encriptación **Sellos**	Ineficiente **Eficiente (*)** Ineficiente Ineficiente **Eficiente (*)**

Fuente: Elaboración propia.

El valor numérico para el control de **Integridad** para este canal es de: $\boldsymbol{LC_{It} = 2}$. En la tabla anterior se puede verificar que existen cinco métodos que permiten asegurar la integridad en el canal humano; de los cuales tres se aplican de manera ineficiente (procesos documentados, cifrado y encriptación), y sólo se aplican dos (firmas y sellos) de una manera eficiente en el GAM-Mira, siendo éstos los que se toman como valores válidos; cabe señalar que de la encuesta se puede resaltar que los términos "encriptación" y "cifrado" de la información, son términos que el personal de la Institución desconoce en su gran mayoría, es por ello que dichos métodos han sido omitidos por el personal del Área de Sistemas como un control de la integridad.

4.4.3.10 *Alarma (LC_{Al}).*

Verificar y enumerar la utilización de un sistema de advertencias o un sistema de alarma en todo el alcance, registro, o un mensaje en cada puerta de acceso sobre cada canal cuando una situación sospechosa es observada por el personal bajo sospechas de un intento de evasión, ingeniería social, o una actividad fraudulenta (Herzog, 2010).

En la Tabla 26 se puede apreciar el análisis realizado para obtener el resultado numérico de este ítem.

Tabla 26: Resultados para el control de Alarma para el canal humano

Alarma		
Técnica	Observación	Encuestas
Segmentos probados	**Sistema de antivirus**	**Utilizado (*)**
	Sistema de advertencias	No utilizado
	Sistema de alarma	**Utilizado (*)**
	Registros	No utilizado
	Mensajes personales	**Utilizado (*)**

Fuente: Elaboración propia.

Para este control, tal como se puede verificar en la tabla anterior, existen cinco métodos probados: antivirus, sistemas de advertencias, alarmas, registros, mensajes personales; de los cuales se utilizan eficientemente tres dentro del GADM-Mira (valores marcados en la tabla anterior). En consecuencia el valor numérico obtenido para el control de **Alarma** en el presente canal es de $\boldsymbol{LC_{Al} = 3}$.

Una vez que se ha realizado las pruebas necesarias para medir la ponderación individual de cada uno de los diez controles se procede a encontrar el valor total de la Suma de los Controles, para ello es necesario aplicar la ecuación 2.

Por lo tanto se obtiene:

$$\boldsymbol{TC_{sum} = TC_{Au} + TC_{Id} + TC_{Re} + TC_{Su} + TC_{Ct} + TC_{NR} + TC_{Cf} + TC_{Pr} + TC_{It} + TC_{Al}}$$

$$\boldsymbol{LC_{sum} = 4 + 4 + 1 + 0 + 1 + 2 + 3 + 1 + 2 + 3}$$

$$\boldsymbol{LC_{sum} = 21}$$

4.4.1 LIMITACIONES

4.4.1.1 *Vulnerabilidades (Lv).*

Contabilizar por separado cada falla o error que desafía las protecciones mediante el cual una persona o proceso pueden ganar el acceso, denegar el acceso a los demás, o se oculta o se activa dentro del alcance (Herzog, 2010). En la Tabla 27 se pueden apreciar el análisis llevado a cabo con el fin de obtener el valor numérico para este segmento.

Tabla 27: Resultados para la limitación de Vulnerabilidad para el canal humano

Vulnerabilidad		
Técnicas	Observación y persuasión	Encuestas
Resultados	• **Debido a la Ley de acceso a la información pública, se puede tener acceso a información sensible del GADM (*). Ejemplo ver Anexo 9.** • **Por inexperiencia de los ocupantes de nuevos cargos se da a conocer información clasificada de uso interno. (*)**	

Fuente: Elaboración propia.

El valor numérico obtenido para la **Vulnerabilidad** en este canal es de $\boldsymbol{Lv = 2}$, ya que tal como se puede verificar en la tabla anterior, en el GADM-Mira existen dos tipos de vulnerabilidades potenciales presentes al momento de realizar el proceso de auditoría del el canal humano. Cabe recalcar que para tener acceso a la información pública del personal de la Institución, se tiene que enviar una solicitud de acceso a la Información Pública, cuyo formato se encuentra en el Anexo 10.

4.4.1.2 *Debilidad (L_w).*

Para encontrar el valor de esta medida es necesario hacer un análisis de cuáles de los controles de Clase A mostrados anteriormente muestran algún tipo de fallo, debilidad o error.

- Los controles operacionales de la Autenticación que pueden presentar algún tipo de falla al momento de autenticar a una persona es el **biométrico (*)** y los **sistemas o aplicaciones de uso municipal (*)**, ya que pueden ser vulnerados; pero los oficios y las peticiones formales son verificadas por las secretarias departamentales.
- Para el control de Indemnización, las **pólizas de seguros con empresas privadas de seguridad (*);** presentan algún tipo de falla o error debido a que el encargado del área de Sistemas del GADM-Mira no conoce a ciencia cierta si son eludidas o abusadas por parte de los empleados de la Institución.
- Para los controles de Resistencia, Subyugación y Continuidad; no se encontraron fallas o errores en las medidas aplicadas.

En consecuencia, aplicando la ecuación 4, y tomando los valores marcados en el análisis de los defectos de los controles de clase A, mostrados anteriormente se tiene que el valor numérico para la D**ebilidad,** en este canal es de:

$$\boldsymbol{L_w = FC_{Au} + FC_{Id} + FC_{Re} + FC_{Su} + FC_{Ct}}$$

$$\boldsymbol{L_w = 2 + 1 + 0 + 0 + 0}$$

$$\boldsymbol{L_w = 3}$$

4.4.1.3 *Preocupación (L_C).*

Para encontrar el valor de esta medida es necesario hacer un análisis de cuáles de los controles de Clase B expuestos anteriormente muestran algún tipo de error.

- Para el control de No-repudio, las dos áreas del GADM-Mira que llevan un registro de acceso presentan defectos. El **complejo deportivo (*)** porque solo se registra a las personas que ingresan a la piscina; pero no a las personas que hacen uso de las demás instalaciones del complejo; y el **centro gerontológico (*)** porque se lleva un registro de los adultos mayores y de

las personas que se benefician de los servicios del centro, pero no de las personas acompañantes de los adultos mayores o de terceras personas.

- Para el control de Confidencialidad, de los tres tipos de comunicaciones seguras utilizados en el GADM-Mira, el que presenta defecto es el de **encriptación de los datos (*)**, esto se debe a que varios funcionarios la utilizan; pero a través de las encuestas realizadas se puede comprobar que la mayoría desconoce en qué consiste.
- Para los controles de Privacidad, Integridad y Alarma no se encontraron fallas.

En consecuencia, aplicando la ecuación 5, y contabilizando los valores marcados anteriormente, mismos que corresponden a los defectos o errores en los controles de clase B, se obtiene que el valor numérico para la **Preocupación** es de:

$$\boldsymbol{L_C = FC_{NR} + FC_{Cf} + FC_{Pr} + FC_{It} + FC_{Al}}$$

$$\boldsymbol{L_C = 2 + 1 + 0 + 0 + 0}$$

$$\boldsymbol{L_C = 3}$$

4.4.1.4 *Exposición (L_E).*

Contabilizar cada acción injustificable, falla o error que proporcione una visibilidad directa o indirecta de los objetivos, o los activos dentro del alcance del canal elegido (Herzog, 2010).

Aplicando la técnica de la observación directa se pudo verificar varias situaciones arrojadas por la encuesta realizada, tales como:

- **Varios empleados de la Institución dejan que otras personas inserten dispositivos de almacenamiento externo en sus ordenadores. (*)**
- **Varios empleados de la Institución olvidan cerrar la sesión en las aplicaciones de su ordenador. (*)**
- **Se otorga información a personas ajenas al GADM sobre los empleados que no se encuentran por algún motivo en su estación de trabajo (*)**

En consecuencia, contabilizando los valores marcados de la lista anterior, se tiene que el valor numérico para la **Exposición** en el canal humano es de $\boldsymbol{L_E = 3}$.

4.4.1.5 *Anomalía (L_A).*

Contabilizar cada elemento identificable o desconocido que no puede tenerse en cuenta en las operaciones normales, generalmente cuando el origen o el destino del elemento no pueden ser entendidas. Una anomalía puede ser una señal temprana de un problema de seguridad. Dado que las incógnitas son elementos que no pueden ser controlados, una auditoría adecuada requiere que se vaya tomando nota de todas las anomalías observadas (Herzog, 2010).

En base a la tabulación de las encuestas realizadas se puede obtener los siguientes resultados, mismos que permitirán encontrar el valor numérico para este segmento.

- **Varios funcionarios llevan documentos importantes de su trabajo fuera del espacio físico de la Institución. (*)**
- **Varios empleados aseguran que se ha perdido accidentalmente información de su estación de trabajo. (*)**
- **Ciertas secretarias se sintieron incomodas al saber que se estaba realizando un proceso de "auditoria", pero de seguridad informática. (*)**

En consecuencia, sumando los aspectos marcados así (*), en la lista anterior, se concluye que el valor numérico para las A**nomalías** en el canal humano es de: $\boldsymbol{L_A = 3}$.

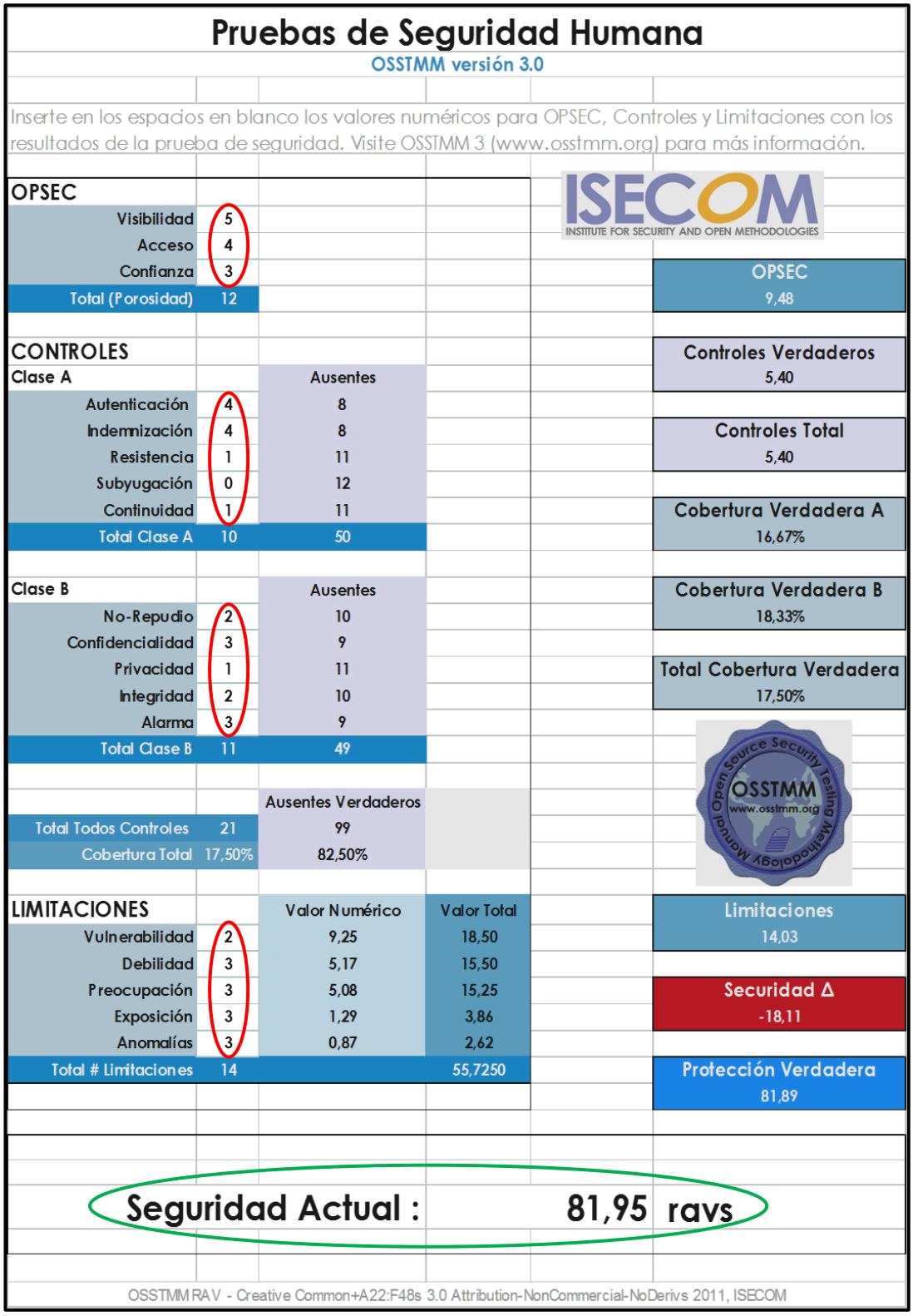
4.4.2 Calculadora RAV

En la Tabla 28 se pueden observar los valores obtenidos para la superficie de ataque, en la auditoría del canal humano para el GADM-Mira, para ello se debieron insertar los valores correspondientes en los cuadros en blanco específicos de cada inciso en la hoja de cálculo del RAV, cuyos valores se obtuvieron a partir de la página 96 de esta sección. Para la **porosidad (OPSEC):** Visibilidad = 5, Acceso = 4 y Confianza = 3; **controles:** Autenticación = 4, Indemnización = 4, Resistencia = 1, Subyugación = 0, Continuidad=1, No-Repudio=2, Confidencialidad = 3, Privacidad = 1, Integridad = 2 y Alarma = 3; y **limitaciones:** Vulnerabilidad = 2, Debilidad = 3, Preocupación = 3, Exposición = 3 y Anomalía = 3.

En el Anexo 11 se encuentra el respectivo reporte del canal auditado, en donde constan todos los valores de la hoja de cálculo del RAV, y los mecanismos de

verificación respectivos para cada inciso, los cuales se encuentran debidamente avalados por el representante del GADM-Mira.

Tabla 28: Resultados obtenidos en la auditoria del canal humano en el GADM-Mira



Pruebas de Seguridad Humana

OSSTMM versión 3.0

Inserte en los espacios en blanco los valores numéricos para OPSEC, Controles y Limitaciones con los resultados de la prueba de seguridad. Visite OSSTMM 3 (www.osstmm.org) para más información.

OPSEC		
Visibilidad	5	
Acceso	4	
Confianza	3	
Total (Porosidad)	12	

CONTROLES		
Clase A		Ausentes
Autenticación	4	8
Indemnización	4	8
Resistencia	1	11
Subyugación	0	12
Continuidad	1	11
Total Clase A	10	50
Clase B		Ausentes
No-Repudio	2	10
Confidencialidad	3	9
Privacidad	1	11
Integridad	2	10
Alarma	3	9
Total Clase B	11	49
		Ausentes Verdaderos
Total Todos Controles	21	99
Cobertura Total	17,50%	82,50%

LIMITACIONES		Valor Numérico	Valor Total
Vulnerabilidad	2	9,25	18,50
Debilidad	3	5,17	15,50
Preocupación	3	5,08	15,25
Exposición	3	1,29	3,86
Anomalías	3	0,87	2,62
Total # Limitaciones	14		55,7250

OPSEC	9,48
Controles Verdaderos	5,40
Controles Total	5,40
Cobertura Verdadera A	16,67%
Cobertura Verdadera B	18,33%
Total Cobertura Verdadera	17,50%
Limitaciones	14,03
Seguridad Δ	-18,11
Protección Verdadera	81,89

Seguridad Actual : 81,95 ravs

OSSTMM RAV - Creative Common+A22:F48s 3.0 Attribution-NonCommercial-NoDerivs 2011, ISECOM

Fuente: Elaboración propia. Recuperado de: Calculadora RAV de OSSTMM3.

4.4.3 Análisis de Resultados

Una vez que se han insertado los valores numéricos de la porosidad, los controles y las limitaciones en la hoja de cálculo del RAV, tal como se muestra en tabla anterior, los datos rotulados con color rojo; los demás valores se generan de forma automática, de los cuales, los valores más significativos, por el hecho de que permiten realizar un análisis evaluativo del canal auditado son: el **Seguridad** Δ (celda de color rojo), y la **Seguridad Actual** (valor rotulado con color verde).

Para el caso del **Seguridad** Δ**,** su valor puede ser ratificado haciendo uso de la ecuación 6, así:

$$\textbf{Seguridad } \Delta = \textbf{Controles Verdaderos} - \textbf{OPSEC} - \textbf{Limitaciones}$$

$$\textbf{Seguridad } \Delta = \mathbf{5,40 - 9,48 - 14,04}$$

$$\textbf{Seguridad } \Delta = \mathbf{-18,12}$$

Tal como se explicó en el párrafo dos de la página 93, el análisis se lo realiza en base al signo que posea el **Seguridad** Δ, para este canal posee un valor numérico de -18,11; es decir un valor negativo, lo que esto se podría interpretar como una insuficiencia en los controles adoptados por el GADM-Mira aplicados hacia su equipo de talento humano, con respecto a la protección de la seguridad de la información; también se puede aseverar que los controles actualmente vigentes en la Institución poseen limitaciones, por lo que es necesario actualizarlos para que se adapten a las necesidades de seguridad vigentes en la actualidad.

La otra expresión, la **Seguridad Actual**, permite analizar el riesgo de la superficie de ataque, la cual para este canal posee un valor aproximadamente de 82 ravs, lo que se traduce en que el alcance posee aproximadamente un 18% de deficiencia; por lo tanto se encuentra expuesto a ataques que puedan vulnerar el normal funcionamiento del sistema informático de la Institución.

La principal causa de que se tenga un valor de deficiencia que supera el 10% se debe a que prácticamente no existen mecanismos eficientes para los controles para la resistencia, subyugación, continuidad y privacidad; lo que a futuro podría desencadenar en consecuencias negativas para la Institución si no se toman las medidas interventivas y correctivas necesarias tales como: la creación de leyes, manual de

políticas interno, manuales de procedimientos, actualización de conocimientos por parte del personal en temas de seguridad de la información, y sobre todo, concienciación del valor real que se le debe dar a la información que se maneja dentro y fuera de la Institución, entre otras.

4.5 PRUEBAS DE SEGURIDAD FÍSICA

Este canal (PHYSSEC) cubre la interacción del analista con los objetivos físicos a ser auditados. Si bien algunos servicios consideran este proceso como un "allanamiento de propiedad", el verdadero objetivo del cumplimiento de las pruebas de seguridad en este canal es una valoración de la barrea física y lógica, a más de medir la brecha que existe con el estándar de seguridad requerido, políticas descritas en la compañía, regulaciones de la industria o la legislación regional. Probar este canal requiere de una interacción no-comunicativa con las barreras y los seres humanos en posiciones de cuidadores de los activos de la organización. (Herzog, 2010)

Un estudio previo antes de obtener cualquier resultado, es la revisión de las regulaciones normativas que rigen el espacio físico de los recursos informáticos del GADM-Mira, para no tener complicaciones legales en el lapso de tiempo que dure el proceso de ejecución de las pruebas para medir la seguridad actual de este canal.

4.5.1 POROSIDAD

Al igual que en el canal humano se deben obtener los valores cuantitativos para la visibilidad, el acceso y la confianza; pero en este caso aplicados al canal físico, cuyo proceso se detalla a continuación:

4.5.1.1 *Visibilidad (P_V).*

(Herzog, 2010), dice que para encontrar el valor numérico de este apartado se debe enumerar y verificar de manera visible los objetivos y los activos. En PHYSSEC, los activos deben también incluir suministros tales como alimentos, agua, combustible, etc., y los procesos operacionales que pueden afectar a dichos suministros como la eliminación adecuada de los residuos y otros contaminantes, la carga y descarga de los suministros enviados, los ciclos de descanso, climatización adecuada, etc. Para ello se debe realizar el siguiente procedimiento, cuyos resultados se muestran en la Tabla 29.

(a) Localizar y detallar el perímetro del alcance, determinando con técnicas de visualización, áreas de acceso público, planes y recursos públicos.

(b) Enumerar y detallar objetivos y activos visibles fuera del alcance.

(c) Enumerar y detallar los objetivos de las normas de tráfico, tráfico peatonal, áreas ocupadas, y sensores visibles fuera del alcance.

(d) Enumerar las direcciones y los directorios telefónicos internos identificando los lugares que faciliten el procesamiento de información susceptible que no es de acceso público.

(e) Localizar y enumerar la ubicación física y el diseño del objetivo, el tamaño, barreras y peligros que pueden aumentar con el tiempo.

Tabla 29: Resultados para la Visibilidad para el canal físico

Visibilidad		
Perímetro del alcance	Planta central del edificio del GADM-Mira	• **Salón máximo (*)** • **Áreas de recaudación (*)** • **Jefatura política (*)** • **Secretaría general (*)**
Activos fuera del alcance	• **Ex patronato municipal (*)** • **Centro gerontológico (*)** • **Garajes municipales (*)** • **Complejo deportivo (*)**	
Normas de tráfico	• **Sí existen normas de tráfico peatonal (*)** • **Dentro de la Institución sólo se permite acceso peatonal (*)** • No existen sensores visibles fuera del alcance	
Direcciones y directorios telefónicos	**Debido a la Ley de acceso a la información pública las direcciones y el directorio telefónico del personal es de dominio público (*)**	
Ubicación del objetivo	• Cuarto de telecomunicaciones Tercera planta del GADM, anexa a la oficina del jefe del departamento de sistemas; pero no es visible desde el exterior de la oficina.	

Fuente: Elaboración propia.

El valor numérico obtenido para la **Visibilidad** en este canal es de: $\boldsymbol{P_V}$ **= 11,** ya que tal como se puede verificar en la tabla anterior, se contabilizan los valores marcados que pertenecen a las áreas de acceso público dentro de la planta central del edificio del GADM-Mira, las cuatro dependencias externas que forman parte de los activos físicos de la Institución, en cuanto a los objetivos de las normas de tráfico dentro de la Institución se pudieron detectar dos, y para finalizar la información de los directorios

y direcciones del personal de la Institución es de dominio público, y por lo tanto cualquier persona puede acceder y hacer uso de él.

4.5.1.2 *Acceso (P_A).*

Pruebas para la enumeración de los puntos de acceso para interactuar con los objetivos y los activos dentro del alcance. Mientras el acceso a los muros y vallas que bordean la propiedad fuera del alcance es un escenario real y a menudo se utiliza un ataque, esta auditoría se limita al alcance de la interacción solamente para proteger los derechos de propiedad de terceras personas (Herzog, 2010).

En la Tabla 30, se muestra el análisis de los aspectos que se tomarán en cuenta para el cálculo del valor numérico de este ítem y en el Anexo 12 se muestran imágenes, en donde se puede evidenciar que se puede acceder fácilmente al interior del alcance (Planta central del GADM-Mira).

Tabla 30: Resultados para el Acceso para el canal físico

Acceso		
Enumeración	Objetivo: Cuarto de telecomunicaciones	Fácil acceso Sistema de video-vigilancia **Suficientes barreras físicas (*)** **Una sola vía (*)**
Localización	Ex patronato municipal Centro gerontológico Garajes Complejo deportivo	**Una cuadra del GADM (*)** **Tres cuadras del GADM (*)** **Seis cuadras del GADM (*)** **Cinco cuadras del GADM (*)**
Penetración	Barreras y obstáculos	**Calor (*)** **Niveles altos de ruido (*)** **Frío (*)** **Humo (*)** **Humedad (*)** **Olores perjudiciales (*)** Campos magnéticos intensos **Luz dañina (*)** Contaminantes

Fuente: Elaboración propia.

El valor numérico obtenido apara el **acceso** en este canal es de: $\boldsymbol{P_A}$**= 13.** Este valor se obtiene contabilizando los valores marcados en la tabla anterior, mismos que corresponden a la existencia de un número adecuado de barreras físicas para proteger el objetivo y se tiene una sola ruta para acceder al mismo; las dependencias externas

del GADM-Mira son físicamente ubicables; y las barreras y obstáculos que aseguran al objetivo no permiten la penetración de calor, niveles altos de ruido, frío, humo, humedad, olores perjudiciales y luz dañina.

4.5.1.3 *Confianza (P_T).*

Probar la confianza entre los procesos dentro del alcance, donde la confianza se refiere al acceso a los activos sin necesidad de identificación o autenticación (Herzog, 2010).

El valor numérico para la **confianza** en este canal es de: $\boldsymbol{P_T = 0}$**,** ya que para acceder a cualquier activo que se encuentre dentro de la planta central del GADM-Mira, no necesariamente se requiere de algún método de autenticación, pero la identificación se la realiza en base a un conocimiento previo de los trabajadores de la Institución en base a sus relaciones interpersonales.

Una vez que se ha obtenido las ponderaciones de la Visibilidad, el Acceso y la Confianza, se procede a calcular el valor numérico total de la **Porosidad** u $\boldsymbol{OpSec_{sum}}$ para el canal físico, para ello es necesario aplicar la Ecuación 1; así:

$$\boldsymbol{OpSec_{sum} = P_V + P_A + P_T}$$

$$\boldsymbol{OpSec_{sum} = 11 + 13 + 0}$$

$$\boldsymbol{OpSec_{sum} = 24}$$

4.5.2 CONTROLES

Realizar pruebas para enumerar los tipos de controles que se utilizan para proteger el valor de los activos.

4.5.2.1 *Autenticación (LC_{Au}).*

(Herzog, 2010), expone lo siguiente:

(a) Enumerar y examinar las deficiencias de los privilegios que se requieren para obtener acceso, el proceso de obtención de dichos privilegios, y asegurar que sólo los identificables, autorizados se permita el acceso.
(b) Verificar el proceso de autenticación de los elementos que pueden ser llevados dentro del alcance tanto por el personal autorizado y no autorizado.

(c) Verificar el proceso de autenticación de los artículos que pueden ser extraídos fuera del alcance tanto por el personal autorizado y no autorizado.

(d) Verificar el proceso de registro de acceso y los elementos que fueron introducidos y retirados.

El análisis aplicado para encontrar los resultados para este ítem se pueden apreciar detalladamente en la Tabla 31, en donde se detallan cada uno de los literales sugeridos por el manual.

Tabla 31: Resultados para el control de Autenticación para el canal físico

Autenticación			
Privilegios requeridos para obtener acceso al objetivo	Jefes departamentales Empleados Guardias Secretarias Personas particulares Proveedores Personal de apoyo	Autorizados No autorizados No autorizados No autorizados No autorizados No autorizados No autorizados	**Autorización (*)**
Elementos que pueden ser llevados dentro del alcance	Documentos departamentales Dispositivos terminales Unidades almacenamiento Oficios Nóminas Planes de área	Aplica a todo el personal	Ninguno
Elementos que pueden ser extraídos fuera del alcance	Documentos departamentales Dispositivos terminales Unidades almacenamiento Oficios Nóminas Objetos del GADM	Aplica a todo el personal	Ninguno
Elementos introducidos y retirados	No se lleva registro de los elementos que son introducidos y extraídos del GADM		

Fuente: Elaboración propia.

En consecuencia, contabilizando los valores marcados de la tabla anterior, se tiene que el valor numérico obtenido para el control de **Autenticación** para este canal es de $\boldsymbol{LC_{Au} = 1}$, ya que el único método utilizado para asegurar este control es la aprobación del encargado del Área de Sistemas de la Institución, y de esta manera se puede acceder al cuarto de telecomunicaciones.

4.5.2.2 *Indemnización (LC_{Id}).*

(Herzog, 2010), expone lo siguiente:

(a) Documentar y enumerar la habilidad para abusar o eludir la política de los empleados, seguros, no divulgación, de incompetencia, contratos de responsabilidad, o el uso de renuncias del personal dentro del alcance.
(b) Enumerar la utilización de señales de advertencia de peligro, sistemas vigilancia o alarmas en uso, problemas de salud, y avisos de entrada restringida.
(c) Verificar el alcance y la finalidad de la acción legal usada para mantener la indemnización.

El análisis aplicado para obtener el valor numérico de este ítem se lo puede observar más detalladamente en la Tabla 32.

Tabla 32: Resultados para el control de Indemnización para el canal físico

Indemnización		
Personal del alcance	Políticas	**Se pueden eludir (*)**
	Seguros	**Se pueden eludir (*)**
	Acuerdos de no divulgación	**Se pueden eludir (*)**
	Acuerdos de Incompetencia	No se pueden eludir
	Contratos de responsabilidad	**Se pueden eludir (*)**
	Renuncias de uso/usuario	No se pueden eludir
Interior del Alcance	Señales de advertencia de peligro	**Sí se utiliza (*)**
	Vigilancia o Alarmas	**Sí se utiliza (*)**
	Problemas de salud	No se utiliza
	Áreas restringida	**Sí se utiliza (*)**
La finalidad de utilizar una acción legal para alguien que infringe los acuerdos firmados por el representante del GADM y una contraparte es la de salvaguardar los bienes, recursos, activos y patrimonio del mismo (*)		

Fuente: Elaboración propia.

En base al análisis realizado en la tabla anterior, se concluye que el valor numérico de la **Indemnización** para este canal es de: $\boldsymbol{LC_{Id} = 8}$**,** para ello se suman los valores marcados, mismos que pertenecen a los cuatro tipos de documentos legales, de los seis planteados por la metodología, que se pueden eludir por parte del personal del GADM-Mira, y existen tres métodos que aseguran el control de indemnización en el interior de la Institución; a este valor se le suma uno más debido a que se muestra la finalidad

de utilizar acciones legales en caso de que se infrinja los acuerdos establecidos para salvaguardar los activos de la Institución.

4.5.2.3 *Resistencia (LC_{Re}).*

(Herzog, 2010), expone lo siguiente:

(a) Enumerar y verificar que la distracción, la remoción o tranquilización del personal de recepción no permitan el acceso directo a los activos u operaciones.
(b) Enumerar y verificar que la inhabilitación o destrucción de las medidas de seguridad operacional o controles no permitirán el acceso directo a los activos u operaciones.
(c) Verificar que el aislamiento del alcance de recursos tales como: combustible, energía, alimentos, agua, comunicaciones, etc., no permitan el acceso directo a los activos u operaciones.
(d) Verificar que las condiciones de alerta de amenaza alta, no cierren o minimicen las medidas de seguridad operacional o controles que permiten el acceso directo a los activos u operaciones.

En la Tabla 33 se puede apreciar con detalle el análisis aplicado para obtener el valor numérico de este control.

Tabla 33: Resultados para el control de Resistencia para el canal físico

Resistencia		
Personal de recepción	Distracción Remoción Aquietamiento	**No permite el acceso (*)** Permite el acceso **No permite el acceso (*)**
Medidas de seguridad operacional	Inhabilitación Destrucción	**No permite el acceso (**$*$**)** Permite el acceso
Falta de recursos	Combustible Energía eléctrica Alimentos Agua Comunicaciones	**No permite el acceso (**$*$**)** Permite el acceso Permite el acceso Permite el acceso **No permite el acceso (**$*$**)**
No existe un plan de contingencia que permita que se minimicen o cierren las medidas de seguridad operacional en caso de una amenaza alta.		

Fuente: Elaboración propia.

En base al análisis realizado en la tabla anterior, se puede concluir que el valor numérico de la **Resistencia** para este canal es de $\boldsymbol{LC_{Re} = 5}$, ya que la distracción o la remoción del personal de recepción no permiten el acceso directo a los activos, la inhabilitación de los mecanismos de seguridad no permiten el acceso a los activos u operaciones y para el caso de la falta de recursos, el combustible y las comunicaciones no permiten el acceso a los activos del GADM-Mira. El valor de la resistencia se calcula de esta manera en base a las recomendaciones del tipo de prueba que se deben realizar por parte de la metodología, la cual manifiesta que se contabilicen todos los valores que no permiten el acceso a los activos de la Institución.

4.5.2.4 *Subyugación (LC_{Su}).*

Enumerar y probar las deficiencias en el acceso a los activos no controlados por la fuente que proporciona el acceso (es decir, números PIN, fotos de identificación, etc., seleccionados por el actor, signos con números de identificación escritos por el actor, etc.) (Herzog, 2010)

El valor numérico para este control es de $\boldsymbol{LC_{Su} = 1}$**,** ya que el encargado del Área de Sistemas del GADM-Mira recomienda al personal de la Institución que se memoricen sus claves personales y prohíbe totalmente que se expongan de alguna manera, ya que estas son de uso personal y son el medio para obtener el acceso tanto a los bienes como a los activos de la Institución, solamente por el personal autorizado.

4.5.2.5 *Continuidad (LC_{Ct}).*

(Herzog, 2010), expone lo siguiente:

(a) Enumerar y verificar las condiciones donde los retrasos en el acceso son abordados apropiadamente a través del personal de apoyo o de un medio automatizado para el acceso oportuno a los servicios, procesos y operaciones.
(b) Enumerar y verificar que la distracción, la eliminación o el silencio del personal de recepción no detendrá o negará el acceso oportuno a los servicios, procesos y operaciones.

(c) Enumerar y verificar que la inhabilitación o destrucción de las medidas de seguridad operacional o controles no negarán el acceso oportuno a los servicios, procesos y operaciones.

(d) Verificar que el aislamiento del alcance de los recursos, tales como combustible, energía eléctrica, alimentos, agua, comunicaciones, etc., no se detengan o denieguen el acceso a los servicios, procesos y operaciones.

(e) Verificar que la incapacidad para eliminar los residuos y contaminantes del alcance no detendrán o impedirán el acceso a los servicios, procesos y operaciones.

(f) Verificar que las condiciones de alerta de amenaza alta no detengan o denieguen el acceso a los servicios, procesos y operaciones.

El análisis aplicado para obtener el valor numérico de este ítem se lo puede apreciar de manera más detallada en la Tabla 34.

Tabla 34: Resultados para el control de Continuidad para el canal físico

Continuidad		
Retraso en el acceso	Personal de apoyo Medio automatizado	No son afrontados No son afrontados
Personal de recepción	Distracción Remoción Aquietamiento	**No detiene el acceso (*)** **No detiene el acceso (*)** **No detiene el acceso (*)**
Medidas de seguridad operacional	Inhabilitación Destrucción	**No niega el acceso (*)** Niega el acceso
Falta de recursos	Combustible Energía eléctrica Alimentos Agua Comunicaciones	**Niega el acceso (∗)** No niega el acceso No niega el acceso No niega el acceso **Niega el acceso (∗)**
Incapacidad para eliminar	Basura Residuos Otros contaminantes	**No impiden el acceso (*)** **No impiden el acceso (*)** **No impiden el acceso (*)**
Las condiciones de alerta de alta amenaza niegan el acceso a los servicios, procesos y operaciones ya que todo se paraliza en el GADM.		

Fuente: Elaboración propia.

En consecuencia, se tiene que el valor numérico para la **Continuidad** en este canal es de: $\boldsymbol{LC_{Ct} = 9}$, contabilizando los valores marcados en la tabla anterior, mismos que

pertenecen a las recomendaciones de la metodología; para el caso de la distracción, remoción o aquietamiento personal de recepción no detiene el acceso, la inhabilitación de los mecanismos de seguridad operacional no niegan el acceso a los activos, la falta de recursos como el combustible y comunicaciones niegan el acceso a los activos y la incapacidad para eliminar basura residuos y otros contaminantes no impiden el acceso a los activos de la Institución.

4.5.2.6 *No repudio (LC_{NR}).*

Enumerar y examinar el uso o insuficiencias de los monitores y sensores, e identificar correctamente y registrar el acceso o la interacción con los activos para una evidencia específica a desafiar el repudio. Documentar la profundidad de la interacción que es registrada (Herzog, 2010).

Aplicando la técnica de la observación directa en todo el alcance, se verificó que el único método utilizado para asegurar el control del No-Repudio, ya sea para comprobar el acceso o la interacción con los activos del GADM-Mira es el uso de un sistema de video-vigilancia (ver Figura 16); por lo tanto el valor numérico para este ítem es de: $\boldsymbol{LC_{NR} = 1}$.

Figura 16: Varias cámaras del sistema de video-vigilancia del GADM Mira

Fuente: Elaboración propia.

4.5.2.7 *Confidencialidad (LC_{Cf}).*

Enumerar y examinar el uso o insuficiencias de todas las señales, la comunicación física y objetos transportados entre los procesos de alcance interno y externo usando códigos del personal, lenguaje indescifrable, interacciones personales "calladas" o "cercanas" para promover la confidencialidad de la comunicación solamente a aquellos con la clasificación debida de la autorización de seguridad para esa comunicación (Herzog, 2010).

El valor numérico para el control de **Confidencialidad** para este canal es de $\boldsymbol{LC_{Cf} = 1}$, ya que utilizando la técnica de la observación directa se pudo verificar que se utiliza el espacio físico de una oficina y a puerta cerrada para realizar interacciones personales que requieran el uso de este control.

4.5.2.8 *Privacidad (LC_{Pr}).*

Enumerar y examinar el uso o deficiencias de todas las interacciones dentro del alcance usando paquetes no marcados o no evidentes, o etiquetadas, las interacciones "calladas" o a "cuarto cerrado", y dentro de cuartos aparte elegidos al azar para ocultar o proteger la privacidad de la interacción y solamente a aquellos con la debida autorización de seguridad para el proceso o activo (Herzog, 2010).

Utilizando la técnica de la observación directa se pudo verificar que existen varios métodos para aprovechar el control de la privacidad; pero en la práctica se aplican preferencialmente los descritos a continuación:

1. **El uso de sobres sin etiquetar para transportar documentos importantes dentro de la Institución (*).**
2. **El uso de una oficina a puerta cerrada para proteger las interacciones que se hacen de manera oral o que poseen el valor de restringidas para terceras personas (*).**

En consecuencia, sumando los dos criterios antes descritos que se encuentran marcados con un asterisco, el valor numérico de la **Privacidad** para este canal es de: $\boldsymbol{LC_{Pr} = 2}$

4.5.2.9 *Integridad (LC_{It}).*

(Herzog, 2010), expone lo siguiente:

(a) Enumerar y examinar las insuficiencias en todas las señales y la comunicación entre todos los procesos y el personal utilizando un proceso documentado, sellos, firmas, enredos, marcas cifradas para proteger y asegurar que los activos no puedan ser cambiados, redirigidos, o revertidos sin que las partes involucradas tengan conocimiento de ello.

(b) Enumerar y examinar las insuficiencias en todos los procesos en interacciones con los activos en transporte los cuales utilizan un proceso documentado, firmas sellos, cintas de embalar, marcas, etiquetas, sensores, o marcas cifradas para proteger y asegurar que los activos no puedan ser cambiados, redirigidos o revertidos sin que las partes involucradas tengan conocimiento de ello.

(c) Verificar todos los medios de almacenamiento de la información que no están en peligro de descomposición natural, tales como el calor o daños de humedad, decoloración por la luz solar directa, o degradación magnética.

En la Tabla 35, se puede apreciar más detalladamente el análisis aplicado para obtener el valor numérico de este ítem.

Tabla 35: Resultados para el control de Integridad para el canal físico

Integridad		
Procesos Operacionales	Señales	**Insuficientes (*)**
	Comunicación entre procesos	Aceptable
	Proceso documentado	**Personalmente (*)**
Procesos con los activos en transporte	Recursos informáticos	**Inventario (*)**
Medios de almacenamiento de la información	Cuando un medio de almacenamiento de la información se encuentra en peligro de descomposición natural, el jefe de sistemas realiza un informe sobre el estado actual del mismo y en el caso de que ya no se lo pueda seguir utilizando se hace la recomendación para darlo de baja.	

Fuente: Elaboración propia.

En consecuencia, el valor numérico obtenido para el control de **integridad** para este canal es de $\boldsymbol{LC_{It} = 3}$, contabilizando los valores marcados de la tabla anterior, que

para el caso de los procesos operacionales se constató que el uso de señales dentro del GADM-Mira son insuficientes, para los procesos documentados cada empleado procura realizarlo personalmente y para los activos en transporte, el único documento que garantiza su desaparición es el inventario de los activos.

4.5.2.10 *Alarma (LC_{Al}).*

Verificar y enumerar la utilización de un sistema de alerta localizado en todo el alcance, ingreso o mensaje para cada puerta de acceso en una situación sospechosa observada por el personal en caso de sospecha de intentos de burla, actividad fraudulenta, infracción, o violación. Asegurarse que los sensores/sistemas estén instalados de acuerdo a las normas nacionales, regionales o internacionales y regularmente probados para cubrir todos los puntos de acceso (Herzog, 2010).

Aplicando la técnica de la observación directa se pudo verificar que no se hace uso de este control en el GADM-Mira, ya que se pudo constatar que no existe un sistema de alerta localizado contra intrusos que prevenga al personal de guardia, para que ellos apliquen las medidas necesarias en caso de observar una actividad sospechosa; por lo tanto el valor numérico para este ítem en este canal es de: $\boldsymbol{LC_{Al} = 0}$.

4.5.3 LIMITACIONES

4.5.3.1 *Vulnerabilidad (Lv).*

En PHYSEC, una vulnerabilidad puede ser tan simple como una puerta de cristal, una puerta de metal corroída por el tiempo, una puerta que puede ser sellada por apilamiento de monedas en el espacio entre ella y su marco, los equipos electrónicos no controlados contra plagas como hormigas o ratones, una unidad de CD de arranque en un PC o un proceso que permite que un empleado tenga un cubo los suficientemente grande para ocultar o transportar bienes fuera del alcance (Herzog, 2010).

Aplicando la técnica de la observación, y corroborándolos con una lista de chequeo (ver Anexo 12) aplicada a la persona encargada del Área de Sistemas, se pudo verificar que en el GADM-Mira existen las siguientes vulnerabilidades:

1. **Puerta de composición mixta (madera y vidrio) para el acceso al cuarto de telecomunicaciones (*).**

2. **No se maneja un control de plagas con el fin de proteger los equipos (*)**
3. **No se utiliza techo ni piso falso en el cuarto de telecomunicaciones para proteger la integridad de los cables de interconexión de equipos. (*)**
4. **Ingreso al cuarto de telecomunicaciones no automatizado (*)**
5. **Varios empleados pueden transportar activos fuera de la Institución (*)**
6. **El cuarto de telecomunicaciones del GADM-Mira no está diseñado en base a algún tipo de estándar o norma (*)**
7. **La ubicación física del cuarto de telecomunicaciones no fue escogida en base a un principio técnico fundamentado (*)**

En consecuencia, sumandos los criterios anteriormente descritos marcados con un asterisco, el valor numérico de las **Vulnerabilidades** para este canal es de: $\boldsymbol{L_V = 7}$.

4.5.3.2 *Debilidad (L_w).*

Una debilidad puede ser una cerradura de una puerta que se abre cuando se introduce una tarjeta entre ésta y el marco de la puerta, un generador de respaldo sin combustible, o un seguro que no cubre daños por inundaciones en una zona de inundación (Herzog, 2010).

- Para el control de Indemnización, de las medidas utilizadas para salvaguardar la información del GADM-Mira, tres presentan algún tipo de defecto: las **renuncias de uso/usuario (*),** porque el encargado del Área de Sistemas no conoce a ciencia cierta si son eludidas por el personal, **las señales de advertencias de peligro (*),** y los avisos de **áreas restringidas (*),** debido a que sí se las utiliza; pero todavía existen muchos espacios sin identificar.
- Para el control de Continuidad, **la inhabilitación de las medidas de seguridad operacional (*)** presenta falla, ya que no debería negar el acceso oportuno a los servicios, procesos y operaciones de la Institución; pero en el departamento en donde se suscite el fallo si presenta problemas de acceso.
- Para los controles de Autenticación, Resistencia y Subyugación no se presentaron fallas o defectos.

Aplicando el concepto de la ecuación 4, la cual consiste en sumar los defectos o errores de los controles de Clase A, se tiene que el valor numérico para la **Debilidad** para este canal es de:

$$L_w = FC_{Au} + FC_{Id} + FC_{Re} + FC_{Su} + FC_{Ct}$$

$$L_w = 0 + 3 + 0 + 0 + 1$$

$$L_w = 4$$

4.5.3.3 *Preocupación (L_C).*

Una preocupación puede ser un mecanismo de bloqueo de la puerta cuyos controles y tipos de claves de operación son públicos, un generador de respaldo sin medidor de potencia o indicador de combustible, un proceso de equipos que no requiere que el empleado firme la salida de materiales cuando se reciben, o una alarma de incendio no lo suficientemente fuerte para ser escuchada por los trabajadores de maquinaria pesada que usa tapones para los oídos (Herzog, 2010).

- Para el control de Privacidad, **el uso de sobres sin etiquetar para transportar documentos importantes dentro del GADM (*)** presenta fallas ya que al no etiquetar el sobre puede caer en manos equivocadas.
- Para el control de Integridad, el uso del **inventario (*)** para protección de los activos en transporte puede presentar algún tipo de falla, ya que este mecanismo está sujeto a las inconsistencias de la persona que lleva dicho inventario.
- Para los controles de No-repudio, Confidencialidad y Alarma no se encontraron fallas o defectos.

Aplicando el concepto de la ecuación 5, la cual consiste en sumar los defectos o errores de los controles de Clase B, se tiene un valor numérico para la **Preocupación** en este canal de:

$$L_C = FC_{NR} + FC_{Cf} + FC_{Pr} + FC_{It} + FC_{Al}$$

$$L_C = 0 + 0 + 1 + 1 + 0$$

$$L_C = 2$$

4.5.3.4 *Exposición (L_E).*

Puede ser una ventana que permite divisar activos y procesos, o un medidor de potencia que muestra la cantidad de energía que consume un edificio y su fluctuación en el tiempo (Herzog, 2010).

Aplicando el la técnica de la observación, y corroborándolos con la lista de chequeo (ver Anexo 12), aplicado al director del Área de sistemas del GADM, se pudo verificar que existen varias exposiciones dentro del GADM tales como:

1. **Jefes departamentales extraen documentos fuera de la Institución sin autorización (*)**
2. **Ventanas que permiten la visibilidad directa de los activos (*).**
3. **Documentos que ya no se utilizan mal almacenados (*)**

En consecuencia, sumando los criterios anteriormente descritos, se tiene que el valor numérico para la Exposición para este canal es de: $\boldsymbol{L_E = 3}$

4.5.3.5 *Anomalía (L_A).*

Pueden ser pájaros muertos en un edificio en torno a los equipos de comunicaciones (Herzog, 2010).

Para este canal no se observaron anomalías; por lo tanto $\boldsymbol{L_A = 0}$

4.5.4 Calculadora RAV

En la Tabla 36 se pueden observar los valores obtenidos para la superficie de ataque en la auditoría del canal físico para el GADM del cantón Mira, para ello se ha seguido el procedimiento que dicta la metodología, es decir, insertar los valores correspondientes en los cuadros específicos de cada ítem requerido tanto en la **porosidad (OPSEC):** Visibilidad = 11, Acceso = 13 y Confianza = 0; **controles:** Autenticación=1, Indemnización=8, Resistencia=5, Subyugación=1, Continuidad=9, No-Repudio = 1, Confidencialidad = 1, Privacidad = 2, Integridad = 3 y Alarma = 0; y **limitaciones:** Vulnerabilidad = 7, Debilidad = 4, Preocupación = 2, Exposición = 3 y Anomalía = 0.

En el Anexo 12 se encuentra el respectivo reporte del canal físico auditado en donde constan todos los valores de la hoja de cálculo del RAV, mismos que deben ser avalados por el representante del GADM.

Tabla 36: Resultados obtenidos en la auditoria del canal humano en el GADM-Mira

Pruebas de Seguridad Física

OSSTMM versión 3.0

Inserte en los espacios en blanco los valores numéricos para OPSEC, Controles y Limitaciones con los resultados de la prueba de seguridad. Visite OSSTMM3 (www.osstmm.org) para más información.

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

OPSEC				
Visibilidad	11			
Acceso	13			
Confianza	0			
Total (Porosidad)	24			

CONTROLES				
Clase A		Ausentes		
Autenticación	1	23		
Indemnización	8	16		
Resistencia	5	19		
Subyugación	1	23		
Continuidad	9	15		
Total Clase A	24	96		
Clase B		Ausentes		
No-Repudio	1	23		
Confidencialidad	1	23		
Privacidad	2	22		
Integridad	3	21		
Alarma	0	24		
Total Clase B	7	113		
		Ausentes Verdaderos		
Total Todos Controles	31	209		
Cobertura Total	12,92%	87,08%		

LIMITACIONES		Valor Numérico	Valor Total
Vulnerabilidad	7	9,71	67,96
Debilidad	4	5,00	20,00
Preocupación	2	5,71	11,42
Exposición	3	1,41	4,24
Anomalías	0	0,54	0,00
Total # Limitaciones	16		103,6125

OPSEC	11,43
Controles Verdaderos	6,21
Controles Total	6,21
Cobertura Verdadera A	20,00%
Cobertura Verdadera B	5,83%
Total Cobertura Verdadera	12,92%
Limitaciones	16,12
Seguridad Δ	-21,34
Protección Verdadera	78,66

Seguridad Actual : 78,79 ravs

OSSTMM RAV - Creative Common+A22:F48s 3.0 Attribution-NonCommercial-NoDerivs 2011, ISECOM

Fuente: Elaboración propia. Recuperado de: Calculadora RAV de OSSTMM3.

4.5.5 Análisis de Resultados

Una vez que se han insertado los valores numéricos de la porosidad, los controles y las limitaciones en la hoja de cálculo del RAV, tal como se muestra en tabla anterior, los datos rotulados con color rojo; los demás valores se generan de forma automática, de los cuales, los valores más significativos, por el hecho de que permiten realizar un análisis evaluativo del canal auditado son: el **Seguridad** Δ (celda de color rojo), y la **Seguridad Actual** (valor rotulado con color verde).

Para el caso del **Seguridad** Δ**,** su valor puede ser ratificado haciendo uso de la ecuación 6, así:

$$\textbf{Seguridad } \Delta = \textbf{Controles Verdaderos} - \textbf{OPSEC} - \textbf{Limitaciones}$$

$$\textbf{Seguridad } \Delta = 6,21 - 11,43 - 16,12$$

$$\textbf{Seguridad } \Delta = -21,34$$

Tal como se explicó en el párrafo dos de la página 93, el análisis se lo realiza en base al signo que posea el **Seguridad** Δ, para este canal posee un valor numérico de -21,34; es decir un valor negativo, lo que significa que existe una falta de barreras físicas que permitan proteger los activos del GADM-Mira de una manera adecuada, y más aún los controles implementados actualmente no pueden proteger de manera efectiva al objetivo más sensible de la Institución, que es el cuarto de telecomunicaciones, ya que varias de las pruebas realizadas fueron dirigidas a este espacio específicamente.

Por otra parte se puede decir que entre los controles implementados en el entorno físico del GADM-Mira poseen limitaciones, la principal causa de esto se debe a que para este canal no se han implementado sistemas de alarmas para la detección de intrusos dentro del alcance, por lo que lo más recomendable seria el uso de sensores en las puertas de acceso para que se envíe una alerta en caso de presentarse alguna actividad sospechosa u otras medidas que permitan evitar la aplicación de técnicas de ingeniería social dentro de la Institución por personas malintencionadas.

Analizando la otra medida que permite generar un criterio de riesgo cuantitativo de los mecanismos de seguridad, la **Seguridad Actual**, que para este canal posee un valor numérico aproximado de 79 ravs, se puede expresar que los mecanismos de seguridad

operacional del GADM-Mira poseen una deficiencia aproximada del 21%, lo que se considera como un valor prácticamente alto en relación al número de activos que se tienen que resguardar.

Los mecanismos interventivos que permitirían reducir notablemente el valor de la deficiencia es el uso de señales de advertencias dentro de la planta central de la Institución y el uso de normas de tráfico peatonal, ya que las personas que tengan que realizar trámites públicos dentro de la Institución o terceras personas ajenas a la misma, podrían ser claramente identificadas en caso de que intenten acceder a un área catalogada como restringida para el acceso público, o por lo menos les permitiría conocer que a dichas áreas no se puede acceder más que con una debida autorización entregada por el ente pertinente y en caso de intentar acceder a la fuerza se tienen que someter a la regulación normativa de la Institución; por otro lado, la implementación de normas de tráfico peatonal permitirían tener una afluencia más ordenada de las personas dentro de las instalaciones de la Institución.

4.6 PRUEBAS DE SEGURIDAD INALÁMBRICA

Para iniciar de manera adecuada las pruebas aplicadas para este canal se debe estudiar la regulación legislativa que existe para el espectro electromagnético y similares, en primer lugar dentro de la organización, en su manual de políticas de seguridad de la información, que para este caso no existe; así que se recurre a la legislación contemplada a nivel regional, descrita en el capítulo II, esto con el fin de realizar procesos que se encuentren estipulados dentro del marco normativo y no tener complicaciones legales con la organización.

Cabe señalar que para llevar a cabo los procesos indicados por el manual para el cálculo de cada uno de los incisos de la porosidad, controles y limitaciones fue necesario el uso de un software detector de redes inalámbricas, el escogido para este caso fue Vistumbler, debido a que el auditor ya ha realizado varias prácticas anteriormente con él. Las capturas de pantalla, con los valores encontrados en los puntos de acceso inalámbricos del GADM-Mira se muestran en el Anexo 13.

4.6.1 POROSIDAD

Para obtener el valor de la porosidad es necesario calcular antes los valores de la visibilidad, el acceso y la confianza mediante las pruebas contempladas en la metodología.

4.6.1.1 *Visibilidad (P_V).*

Pruebas de enumeración y verificación para la visibilidad del personal con el cual la interacción es posible a través de todos los canales (Herzog, 2010). En la Tabla 37, se muestra detalladamente el análisis aplicado para obtener el valor numérico de este apartado.

Tabla 37: Resultados de la visibilidad para el canal inalámbrico

Visibilidad		
Interceptación (Localización)	Control de acceso Seguridad perimetral Canales inalámbricos	No se utiliza **Firewall (*)** **Sí se pueden interferir (*)**
Detección de la señal pasiva	Frecuencias Señales	**2,4 GHz, 5 GHz (*)** **Wi-Fi (*)**
Detección de la señal activa	Sistemas de RFID Sistemas de infrarrojos	No se utilizan No se utilizan

Fuente: Elaboración propia.

El valor numérico para la **Visibilidad** para el canal inalámbrico es de: $\boldsymbol{P_V = 4}$, esto se debe a que mediante la información proporcionada por la entrevista realizada al director del Área de sistemas del GADM (ver Anexo 13) se pudo comprobar los valores para la interceptación de la tabla anterior, y mediante la utilización del software detector de redes inalámbricas se puede descubrir las frecuencias que se utilizan en el GADM del cantón Mira y por ende las señales que se emplean en dichas frecuencias.

4.6.1.2 *Acceso (P_A).*

Realizar pruebas para la enumeración de los puntos de acceso para el personal dentro del alcance. Si bien el acceso al personal fuera del alcance es un escenario real y uno a menudo utilizado para el robo de propiedad de la información, el analista puede limitarse solamente a la interacción con el alcance, para proteger los derechos de privacidad independientes del personal en su vida privada (Herzog, 2010). A continuación se muestra el análisis realizado para obtener el valor numérico:

- **Los puntos de acceso (AP) del GADM se encuentran encendidos durante todo el día, independientemente de sí están en uso o no (*)**
- **Los dispositivos inalámbricos del GADM se encuentran configurados en su potencia de funcionamiento más baja para mantener las transmisiones dentro de los límites seguros de la organización. (*)**
- **Los SSID de los puntos de acceso sí se han cambiado (*)**
- Solo varios puntos de acceso poseen seguridad física que los controlan (cajas con llaves, etc.).

Contabilizando los valores marcados con un asterisco de la lista anterior, los cuales se obtienen de la entrevista realizada al encargado del Área de Sistemas del GADM-Mira (Ver Anexo 13), se concluye que el valor numérico para el **Acceso** en el canal inalámbrico es de: $\boldsymbol{P_A}$ **= 3.**

4.6.1.3 *Confianza (P_T).*

Pruebas para la confianza entre el personal dentro del alcance, donde la confianza se refiere al acceso a la información o propiedad física sin la necesidad de una identificación o autenticación (Herzog, 2010).

El valor numérico de la **Confianza** para este canal es de: $\boldsymbol{P_T}$ **= 1**; esto se debe a que el único método utilizado para la autenticación que genera confianza dentro del GADM-Mira es el uso de contraseñas (ver Anexo 13).

4.6.2 CONTROLES

Realizar pruebas para enumerar los tipos de controles utilizados para proteger la información (Herzog, 2010).

4.6.2.1 *Autenticación (LC_{Au}).*

Enumerar y probar las insuficiencias de los métodos de autenticación y autorización que se hacen uso en los puntos de acceso inalámbricos (Herzog, 2010).

En la Tabla 38 se puede observar el análisis aplicado para obtener el valor numérico de este apartado, para ello fue necesario el uso de los datos entregados por el director

del Área de sistemas del GADM-Mira y para la comprobación de esos datos el uso del software detector de redes inalámbricas.

Tabla 38: Resultados del control de autenticación para el canal inalámbrico

Autenticación		
Autenticación	Contraseñas	**WPA-Personal (*)** Abierta **WPA2-Personal (*)**
	Cifrado	**TKIP (*)** Ninguno **CCMP (*)**
Autorización	**No se necesita autorización para acceder a los puntos de acceso del GADM ya que son exclusivamente para el uso de invitados (*)**	

Fuente: Elaboración propia.

Contabilizando los valores marcados con un asterisco de la tabla anterior se tiene que el valor numérico para el control de **Autenticación** en este canal es de: $\boldsymbol{LC_{Au}}$ **= 5**, esto se debe a que en los puntos de acceso inalámbricos del GADM-Mira se utilizan dos tipos de contraseñas: WPA-Personal y WPA2-Personal (ver en las capturas de pantalla del Anexo 13 los valores encerrados con color azul); y también se utilizan dos tipos de cifrado para las contraseñas: TKIP y CCMP (ver en las capturas de pantalla del Anexo 13 los valores encerrados con color verde), a esto se le suma uno por el método de autorización aplicado para los puntos de acceso.

4.6.2.2 *Indemnización (LC_{Id}).*

Documentar y enumerar que los objetivos y servicios están protegidos contra el abuso o elusión de la política de los empleados, estén asegurados contra el robo o daños, o uso de responsabilidades y renuncias de permisos (Herzog, 2010).

En base a la encuesta realizada al director del Área de sistemas, se obtuvo las siguientes conclusiones:

- No existe una política que dicte alguna norma sobre los equipos inalámbricos de comunicaciones utilizados en GADM.
- Ningún equipo inalámbrico utilizado en el GADM para comunicaciones está protegido contra robo o daños.

- No existen acuerdos de responsabilidad para la manipulación de los equipos inalámbricos del GADM.
- No existen renuncias de permiso por parte del personal del GADM para los equipos inalámbricos del GADM.

En consecuencia, el valor numérico para el control de **Indemnización** en este canal es de: $\boldsymbol{LC_{Id} = 0}$, debido a que no existe ningún mecanismo que asegure este control, aplicado a los equipos inalámbricos de comunicación dentro del GADM-Mira.

4.6.2.3 *Resistencia (LC_{Re}).*

Esquematizar y documentar el proceso que realizan los guardias para desconectar los canales debido a incumplimientos o preocupaciones de seguridad como un análisis de la brecha con la regulación y la política de seguridad (Herzog, 2010).

El procedimiento del guardia de los activos cuando existe algún tipo de incumplimiento o preocupación de seguridad es dictar la sanción que contemple la ley regional vigente según la gravedad del acto cometida. (*)

En consecuencia, el valor numérico del control de **Resistencia** para este canal es de: $\boldsymbol{LC_{Re} = 1}$, debido a que solo existe un procedimiento que se realiza para asegurar este control, tal como se explicó en el criterio anterior.

4.6.2.4 *Subyugación (LC_{Su}).*

Enumerar y poner a prueba las insuficiencias de todos los canales a utilizar o habilitar los controles que no estén activados de forma predeterminada (Herzog, 2010).

El valor numérico para este control es de: $\boldsymbol{LC_{Su} = 0}$, ya que la persona encargada del Área de Sistemas asegura que el único procedimiento que se realiza al instalar un equipo nuevo es su configuración básica, más no se revisa los controles que este brinda, los cuales no se activan por defecto.

4.6.2.5 *Continuidad (LC_{Ct}).*

Enumerar y examinar las insuficiencias desde el objetivo en relación con el retraso al acceso y el tiempo de respuesta del servicio a través del personal de apoyo o medios automatizados (Herzog, 2010).

- **Debido a que no existe personal de apoyo adherido al departamento de sistemas, en caso de presentarse algún tipo de problema fuera de la planta central del GADM, el tiempo de respuesta para activar un servicio puede demorarse de uno a dos días, dependiendo de la ubicación del equipo. (*)**
- En planta central el tiempo de respuesta es mínimo, al igual que el acceso a los activos.

Contabilizando los valores marcados con un asterisco de la lista anterior, se obtiene un valor numérico para el control de **Continuidad** para este canal de: $\boldsymbol{LC_{Ct}}$ **= 1** ya que se presentan muchas insuficiencias cuando se tiene que realizar algún tipo de procedimiento de soporte técnico en los dispositivos inalámbricos que se encuentren fuera del GADM**.**

4.6.2.6 *No repudio (LC_{NR}).*

Enumerar y probar el uso o las deficiencias de los daemons y sistemas para identificar y registrar adecuadamente el acceso o interacciones a la propiedad para tener una evidencia específica que permita resistir el repudio, y documentar la profundidad de la interacción registrada y el proceso de identificación (Herzog, 2010).

El valor numérico para este control es de: $\boldsymbol{LC_{NR}}$ **= 0**, ya que apegados a la entrevista dirigida al director del Área de sistemas del GADM, asegura que no existe ningún sistema que permita identificar cuando alguien ha accedido a un activo de tipo inalámbrico del GADM.

4.6.2.7 *Confidencialidad (LC_{Cf}).*

Enumerar y examinar el uso de equipos para amortiguar las señales de transmisión electromagnética fuera de la organización y los controles en el lugar para asegurar y encriptar las transmisiones inalámbricas (Herzog, 2010).

- No se utiliza ningún equipo que permita amortiguar las señales de transmisión electromagnética fuera del GADM.
- No se hace uso de la encriptación de las transmisiones inalámbricas.

- **El único método utilizado para amortiguar las señales de transmisión electromagnética para evitar que salgan fuera del GADM es encerrar el equipo que genere dicha señal en una caja cerrada. (*)**

En consecuencia, el valor numérico del control de **Confidencialidad** para este canal es de: $\boldsymbol{LC_{Cf}}$**= 1,** ya que haciendo referencia a los valores marcados de la lista anterior, se obtiene que sólo existe un método que permite amortiguar las señales de transmisión electromagnética fuera de las instalaciones del GADM-Mira.

4.6.2.8 *Privacidad (LC_{Pr}).*

Determinar el nivel de los controles de acceso físico a los puntos de acceso y dispositivos que los controlan (cerraduras con llave, lectores de tarjetas, cámaras, etc.) (Herzog, 2010).

En base a la entrevista realizada al responsable del Área de Sistemas del GADM-Mira, se concluye que los controles que aseguran a los puntos de acceso dentro de planta central son las cámaras de vigilancia, y para los de planta externa cerraduras con llave. Por lo tanto el valor numérico para el control de **Privacidad** para este canal es de: $\boldsymbol{LC_{Pr}}$ **= 2.**

4.6.2.9 *Integridad (LC_{It}).*

Determinar que los datos sólo puedan ser consultados y modificados por aquellos que están autorizados y garantizar que el adecuado cifrado este en uso para garantizar la firma y la confidencialidad de las comunicaciones (Herzog, 2010).

- **El único método que garantiza que los datos sean consultados y modificados por aquellos que estén autorizado es el uso de contraseñas (*)**
- **Se utiliza el cifrado para los equipos de planta central (*)**

Por lo tanto, se concluye que el valor numérico para el control de **Integridad** para este canal es de: $\boldsymbol{LC_{It}}$ **= 2,** sumando los criterios anteriormente descritos.

4.6.2.10 *Alarma (LC_{Al}).*

Verificar y enumerar el uso de un sistema de alerta localizado en todo el alcance, registro o mensaje para cada puerta de acceso sobre cada canal donde una situación

sospechosa es observada por el personal en caso de sospecha de intentos de elusión, la ingeniería social, o una actividad fraudulenta (Herzog, 2010).

El valor numérico para este control es de: $\boldsymbol{LC_{Al}}$ **= 0**, ya que el director del Área de sistemas del GADM asegura que existen los mecanismos de alerta, pero que no se los ha puesto en funcionamiento.

4.6.3 LIMITACIONES

Examinar y documentar los tipos de entradas y canales alternativos de accesibilidad para las personas con limitaciones físicas dentro de este canal. (Herzog, 2010)

4.6.3.1 *Vulnerabilidad (Lv).*

Una vulnerabilidad puede ser un hardware que puede ser sobrecargado y quemado por las versiones de mayor potencia en la misma frecuencia o una frecuencia cercana, un receptor estándar sin configuraciones especiales que puede tener acceso a los datos de la señal, un receptor que puede ser obligado a aceptar una señal de terceros en lugar de la prevista, o un AP inalámbrico cuando cae su conexión cerca de un horno microondas (Herzog, 2010).

El valor numérico para este segmento es de: $\boldsymbol{Lv}$ **= 0**, ya que el encargado del Área de sistemas del GADM-Mira aseguró que no ha observado ninguna situación que genere vulnerabilidad a los equipos inalámbricos de la Institución.

4.6.3.2 *Debilidad (L_w).*

Una debilidad puede ser un AP inalámbrico con autenticación de usuario basado en direcciones MAC (que se puede suplantar) o una tarjeta de seguridad RFID que ya no recibe las señales y por lo tanto queda "abierta" después de recibir una señal procedente de una fuente de energía alta (Herzog, 2010).

- Para el control de Autenticación, se comete un error al **no hacer uso de algún método de autorización para acceder a los equipos inalámbricos de red del GADM-Mira (*).**
- Para el control de Resistencia existe un grave error ya que en caso de suscitarse algún tipo de incumplimiento o preocupación de seguridad no se

puede dictar una sanción razonables ya que **no existe una normativa de manejo interno (*)** por parte de la Institución para dictar sanciones.

- Para el control de Continuidad se comete un error al **no contar con personal de apoyo para el Área de Sistemas de GADM-Mira (*),** para dar una solución más rápida a los problemas que puedan presentarse.
- Para los controles de Indemnización y Subyugación no se presentaron errores.

En consecuencia, aplicando el concepto de la ecuación 4, el cual consiste en sumar los defectos o errores de los controles de Clase A, descritos en la explicación anterior, se obtiene que el valor numérico para la **Debilidad** en este canal es de:

$$\boldsymbol{L_w = FC_{Au} + FC_{Id} + FC_{Re} + FC_{Su} + FC_{Ct}}$$

$$\boldsymbol{L_w = 1 + 0 + 1 + 0 + 1}$$

$$\boldsymbol{L_w = 3}$$

4.6.3.3 *Preocupación (L_C).*

Una preocupación pude ser un AP inalámbrico que utiliza un cifrado de datos débil un abridor de puertas con sistema infrarrojo que no puede leer el remitente en la lluvia (Herzog, 2010).

- Para el control de Confidencialidad se presenta defecto en **el método utilizado para amortiguar las señales de transmisión electromagnética en los equipos de la planta central del GADM (*),** ya que es más recomendable utilizar softwares que permitan hacer esto con más facilidad.
- Para el control de Integridad existe **ineficiencia en el método utilizado para garantizar que los datos no sean consultados o modificados por aquellas personas que no estén autorizadas (*)** ya que se puede utilizar otros métodos a parte del uso de contraseñas.
- Para los controles de No-repudio, Privacidad y Alarma, no se encontraron errores o defectos.

En consecuencia, aplicando el concepto de la ecuación 5, el cual consiste en sumar los defectos o errores en los controles de Clase B, mismos que se describen en la explicación anterior, se tiene que el valor numérico de la **Preocupación** es de:

$$L_C = FC_{NR} + FC_{Cf} + FC_{Pr} + FC_{It} + FC_{Al}$$

$$L_C = 0 + 1 + 0 + 1 + 0$$

$$L_C = 2$$

4.6.3.4 *Exposición (L_E).*

Una exposición pude ser una señal que interrumpe otra maquinaria o un dispositivo de infrarrojos cuyo funcionamiento es visible por las cámaras de vídeo estándar con capacidad de noche (Herzog, 2010).

El valor numérico para este segmento en este canal es igual a: $L_E = 0$, debido a que los equipos inalámbricos del GADM se configuran a de tal manera que no interrumpan el funcionamiento de las máquinas o dispositivos que funcionen cerca.

4.6.3.5 *Anomalía (L_A).*

Una anomalía puede ser una señal local que no puede ser correctamente situada o provoca algún daño conocido (Herzog, 2010).

- **Ciertos equipos inalámbricos siguen conectados a pesar de que ya no tienen ninguna utilidad (*)**

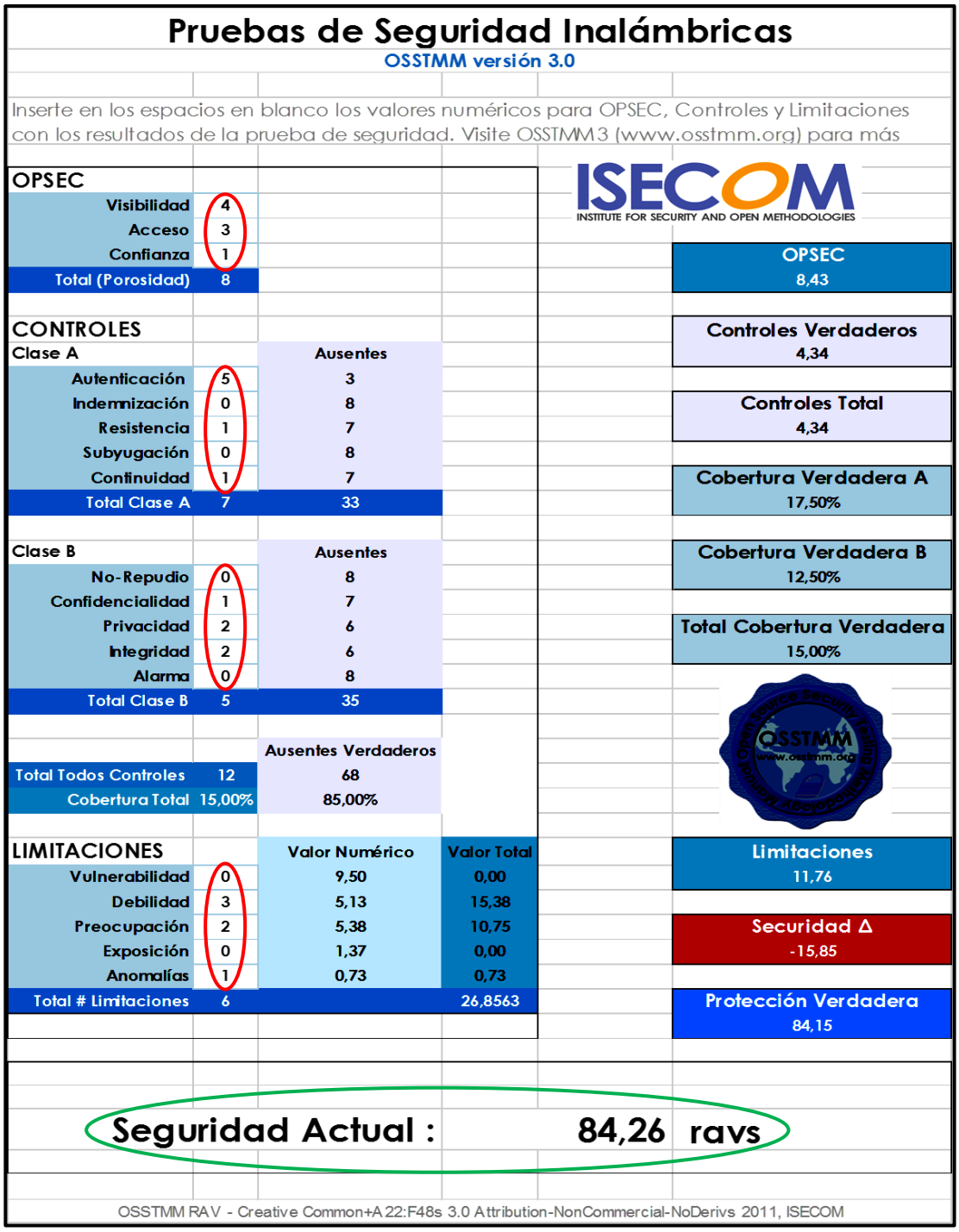
Por lo tanto, tomando el criterio anteriormente descrito, se tiene un valor numérico para este segmento en este canal de: $L_A = 1$.

4.6.4 Calculadora RAV

En la Tabla 39 se pueden observar los valores obtenidos para la superficie de ataque en la auditoría del canal de seguridad inalámbrica para el GADM del cantón Mira, para ello se ha seguido el procedimiento que dicta la metodología, es decir, insertar los valores correspondientes en los cuadros específicos de cada ítem requerido tanto a la **porosidad (OPSEC):** Visibilidad = 4, Acceso = 3 y Confianza = 1; **controles:** Autenticación = 5, Indemnización = 0, Resistencia = 1, Subyugación = 0, Continuidad=1, No-Repudio=0, Confidencialidad = 1, Privacidad = 2, Integridad = 2 y Alarma = 0; y **limitaciones**: Vulnerabilidad = 0, Debilidad = 3, Preocupación = 2, Exposición = 0 y Anomalía = 1.

En el Anexo 13, se encuentra el respectivo reporte del canal de comunicaciones inalámbricas auditado, en donde constan todos los valores de la hoja de cálculo del RAV, mismos que deben ser avalados por el representante del GADM, a este informe se adjuntan las capturas de pantalla extraídas del software detector de redes inalámbricas Vistumbler.

Tabla 39: Resultados obtenidos en la auditoria del canal de seguridad inalámbrica en el GADM Mira



Pruebas de Seguridad Inalámbricas

OSSTMM versión 3.0

Inserte en los espacios en blanco los valores numéricos para OPSEC, Controles y Limitaciones con los resultados de la prueba de seguridad. Visite OSSTMM 3 (www.osstmm.org) para más

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

OPSEC		
Visibilidad	4	
Acceso	3	
Confianza	1	
Total (Porosidad)	8	

OPSEC: 8,43

CONTROLES		
Clase A		Ausentes
Autenticación	5	3
Indemnización	0	8
Resistencia	1	7
Subyugación	0	8
Continuidad	1	7
Total Clase A	7	33

Controles Verdaderos: 4,34

Controles Total: 4,34

Cobertura Verdadera A: 17,50%

Clase B		Ausentes
No-Repudio	0	8
Confidencialidad	1	7
Privacidad	2	6
Integridad	2	6
Alarma	0	8
Total Clase B	5	35

Cobertura Verdadera B: 12,50%

Total Cobertura Verdadera: 15,00%

		Ausentes Verdaderos
Total Todos Controles	12	68
Cobertura Total	15,00%	85,00%

LIMITACIONES		Valor Numérico	Valor Total
Vulnerabilidad	0	9,50	0,00
Debilidad	3	5,13	15,38
Preocupación	2	5,38	10,75
Exposición	0	1,37	0,00
Anomalías	1	0,73	0,73
Total # Limitaciones	6		26,8563

Limitaciones: 11,76

Securidad Δ: -15,85

Protección Verdadera: 84,15

Seguridad Actual : 84,26 ravs

Fuente: Elaboración propia. Recuperado de: Calculadora RAV de OSSTMM3.

4.6.5 Análisis de Resultados

Una vez que se han insertado los valores numéricos de la porosidad, los controles y las limitaciones en la hoja de cálculo del RAV, tal como se muestra en tabla anterior, los datos rotulados con color rojo; los demás valores se generan de forma automática, de los cuales, los valores más significativos, por el hecho de que permiten realizar un análisis evaluativo del canal auditado son: el **Seguridad** Δ (celda de color rojo), y la **Seguridad Actual** (valor rotulado con color verde).

Tal como se explicó en el párrafo dos de la página 93, el análisis se lo realiza en base al signo que posea el **Seguridad** Δ, para este canal posee un valor numérico de -15,85; es decir un valor negativo, lo que se considera como una deficiencia en los controles de seguridad operacional adoptados por el GADM-Mira, para su infraestructura de comunicaciones inalámbricas.

Cabe aclarar que se realizó pruebas solamente para los equipos que se utilizan en la planta central, porque para poder acceder a toda la infraestructura inalámbrica del GADM-Mira hubiese implicado un gasto innecesario de recursos y tiempo, ya que en algunos casos se han implementado pequeñas infraestructuras con torres para las repetidoras que se encuentran en lugares de difícil acceso, por lo que fue necesario que el director del Área de sistemas de la Institución resumiera como se encuentran establecidos los controles operacionales para dichos enlaces.

Analizando la otra medida que permite generar un criterio de riesgo cuantitativo de los mecanismos de seguridad, la **Seguridad Actual**, que para este canal posee un valor numérico de 84,26 ravs, lo que se traduce en un porcentaje de deficiencia de alrededor del 16% de los controles implementados por el GADM-Mira para proteger las interacciones por medio de las comunicaciones inalámbricas; y considerando que apenas existen cinco puntos de acceso inalámbricos dentro de la infraestructura de la planta central de la Institución, este valor es poco aceptable, ya que con las miles de herramientas que existen en la actualidad para vulnerar los enlaces inalámbricos es de vital importancia proteger la información que generan los usuarios de la infraestructura inalámbrica de la Entidad. De igual manera se debería dar un tratamiento especial a los puntos de acceso, ya que son equipos que no están diseñados para permanecer encendidos todo el tiempo y por lo menos los fines de semana deberían permanecer fuera de funcionamiento.

Si bien los puntos de acceso inalámbricos son utilizados por las personas invitadas y por el personal que necesita de su uso para desarrollar sus actividades laborales, es necesario que por lo menos se haga uso de un servicio de encripción de la información que circula por dichos enlaces, ya que en muchos casos es utilizado para el envió de información, haciendo uso los servicios de mensajería instantánea, para enviar información privada de los empleados de la Institución.

4.7 PRUEBAS DE SEGURIDAD DE LAS TELECOMUNICASIONES

Es una clasificación de COMSEC para la seguridad material dentro del entorno de ELSEC el cual se encuentra dentro de los límites de las telecomunicaciones por cables. Mientras que algunos servicios consideran esto simplemente como “piratear”, el verdadero objetivo del cumplimiento de las pruebas de seguridad en este canal es examinar la barrera lógica y la medición de la brecha que existe con el estándar de seguridad requerido, política de la empresa, regulaciones de la industria, o la legislación regional (Herzog, 2010).

La metodología sugiere que los vectores de ataque para este canal son:

- Pruebas de PBX
- Pruebas de buzón de voz
- Encuesta, sondeo y pruebas de FAX y módem
- Pruebas de Servicio de Acceso Remoto (RAS)
- Pruebas de líneas RDSI de respaldo
- Pruebas de voz sobre IP
- Pruebas de conmutación de paquetes en redes X.25

Tal como se puede apreciar en el Anexo 12 (ver literal 4 de la lista de chequeo), para este canal solo existen dos objetivos que pueden ser probados dentro del GADM-Mira ya que solo se cuenta una central telefónica analógica y un sistema de fax; de los cuales, la central telefónica no sería considerada como un dispositivo de telecomunicaciones ya que está limitada para uso exclusivo dentro del espacio físico de la Institución.

En consecuencia para este canal se apelará al recurso que dicta el manual de la metodología para reportarlo como un "objetivo no probado", por el hecho de que el entorno de la prueba no permite recoger la información necesaria para emitir un informe que arroje resultados acordes a la realidad actual de la Institución. Lo más recomendable es tomar este aspecto para futuras pruebas, y en caso de que se cuente con los vectores necesarios a probar, se debe emitir un criterio sobre el grado de la seguridad operacional que tendrá este canal.

4.8 PRUEBAS DE SEGURIDAD DE LAS REDES DE DATOS

Las pruebas para el canal de seguridad de redes de datos (COMSEC) requieren interacciones con los seguros operacionales de la red de datos existente, utilizados para controlar el acceso a la propiedad. Este canal cubre la implicación de los sistemas informáticos, principalmente las redes de funcionamiento dentro del alcance. Mientras que algunas organizaciones consideran a esto simplemente como "pruebas de penetración", el verdadero objetivo del cumplimiento de las pruebas de seguridad en este canal es la interacción del sistema y las pruebas de calidad operacional con las mediciones de distancia con el estándar de seguridad requerido en la política de la empresa, regulaciones de la industria, o la legislación regional. (Herzog, 2010).

Por motivos del Acuerdo de Confidencialidad firmado entre el responsable del Área de Sistemas del GADM-Mira (Sr. Damián Bastidas) y el Auditor (Sr. Cristian Bracho) no se muestra el procedimiento completo llevado a cabo en este canal y sólo se muestran varias pantallas de los resultados de las pruebas realizadas.

4.8.1 POROSIDAD

4.8.1.1 *Visibilidad (P_V).*

La enumeración e indexación de los objetivos en el alcance a través de la interacción directa e indirecta con o entre los sistemas activos (Herzog, 2010).

(a) Identificar el perímetro de segmento(s) de red destino y el vector que serán examinados.

Siguiendo el procedimiento de autenticación que se aplica en el GADM-Mira para un invitado nuevo, se pudo verificar que el **perímetro de la red está comprendida en**

una red de clase C o /24 (*), tal como se puede observar en la Figura 17, ya que realizando una traza hacia una dirección externa el primer salto que se observa es el servidor de Internet de la Institución.

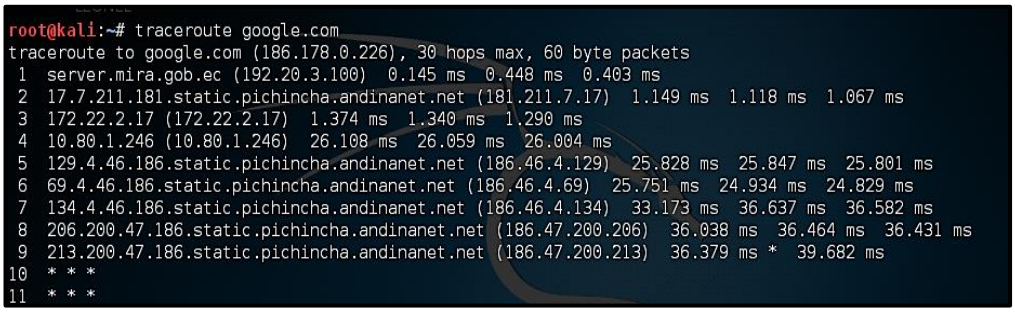


Figura 17: Traza hacia google.com

Fuente: Elaboración propia. Recuperado de: Kali-Linux

(b) Usar el sniffing para identificar el protocolo que procede de las respuestas de los servicios de red o peticiones aplicables. Por ejemplo, NetBIOS, ARP, BGP, NFS, OSPF, MPLS, RIPv2, etc.

Para verificar el procedimiento que indica el manual, se hiso uso del sniffer Wireshark, con el cual se pudo verificar que los únicos protocolos que proceden de las respuestas de los servicios de red son **NetBIOS (*) y ARP (*),** tal como se pude apreciar en la Figura 18.

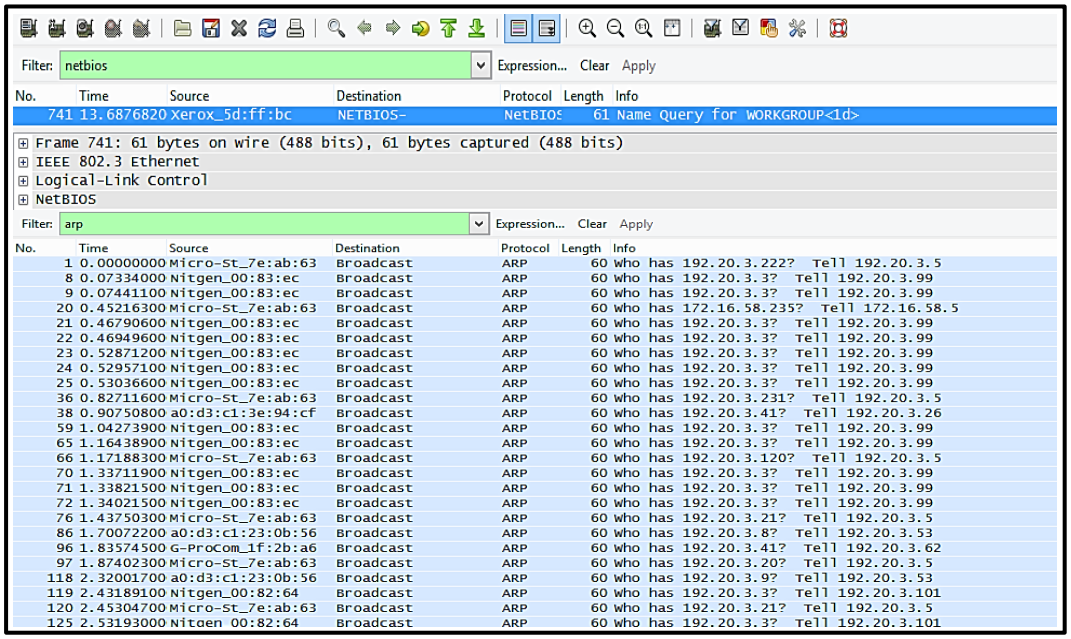


Figura 18: Protocolos observados en Wireshark

Fuente: Elaboración propia. Recuperado de: Sniffer Wireshark

(c) Consultar todos los nombres de los servidores y los nombres de los servidores del ISP o proveedor de hosting, si se encuentran disponibles, así como la capacidad para realizar transferencias de zona para determinar la existencia de todos los objetivos en la red y cualquier redundancia relacionada al balanceo de carga, almacenamiento en caché, proxies y hosting virtual.

Con ayuda del comando *dnsenum* y conociendo el nombre de la página web del GADM Mira (www.mira.gob.ec) se procedió a buscar información sobre los nombres de los servidores, mismos que se muestran en la Figura 19.

Figura 19: Ejemplos de los nombres de los servidores encontrados

Fuente: Elaboración propia. Recuperado de: Kali Linux

Cabe señalar que los nombres de los servidores encontrados fueron: **servidor de internet (*), servidor web (*), servidor de hosting (*) y servidor de bases de datos (*);** para encontrar los nombres de los proveedores de hosting se hiso uso del comando *whois* a la página web del GADM, proporcionando como resultado **NIC.EC (*);** redundancias relacionadas al balanceo de carga, almacenamiento en caché y proxies no se encontraron disponibles dentro del GADM.

(d) Verificar peticiones de difusión y las respuestas de todos los objetivos.

Con el uso del sniffer Wireshark se pudo comprobar las peticiones y respuestas de todos los objetivos del GADM, mismas que consisten tanto en peticiones como en respuestas **Unicast (*), Multicast (*) y Broadcast (*).** En la Figura 20 se pueden observar algunos ejemplos de cada una de las difusiones verificadas.

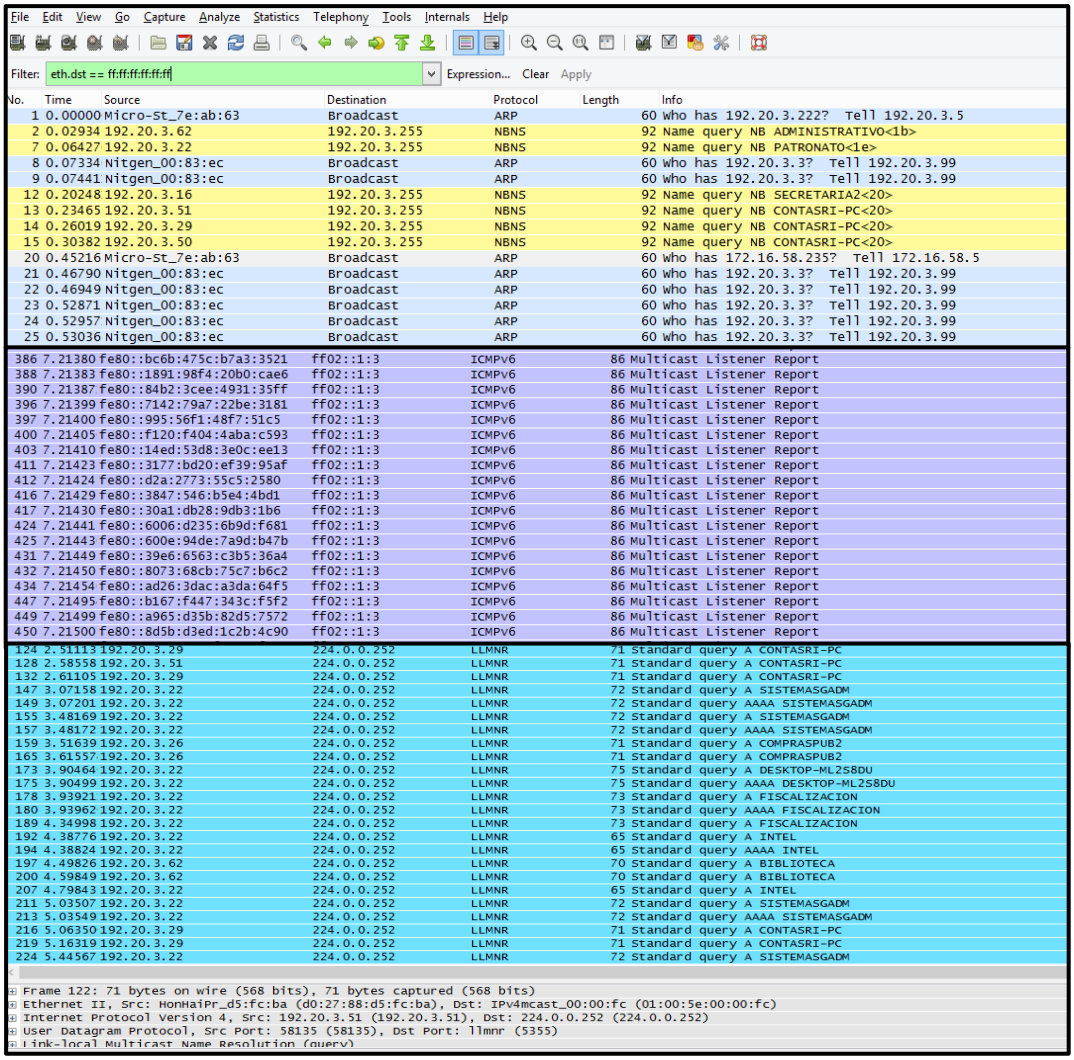


Figura 160: Tipos de peticiones y respuestas observadas en Wireshark

Fuente: Elaboración propia. Recuperado de: Sniffer Wireshark

(e) Verificar y examinar el uso de tráfico y los protocolos de enrutamiento de todos los objetivos.

En la Figura 21, se pude observar que el protocolo que genera más tráfico desde todos los objetivos del GADM es **ARP (*)**, pero dentro de esta institución no se maneja un protocolo de enrutamiento específico, solo se hace uso de direcciones estáticas.

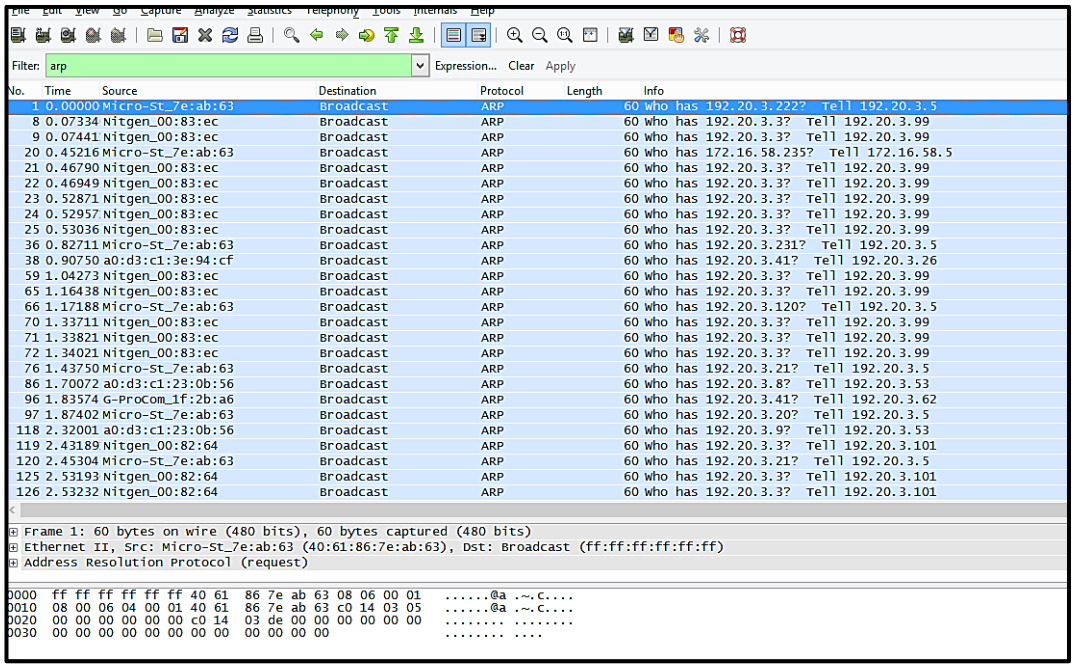


Figura 171: Protocolos observados en Wireshark

Fuente: Elaboración propia. Recuperado de: Sniffer Wireshark

(f) Verificar respuestas ICMP para los tipos de ICMP 0-255 y los códigos ICMP 0-2 de todos los objetivos.

En la Figura 22, se puede observar un extracto de todas las comunicaciones mediante el uso del protocolo ICMP entre todos los objetivos del GADM, cabe señalar que los objetivos que se tomaron en cuenta hacen uso del protocolo ICMPv6, ya que en el lapso de tiempo que estuvo activo el sniffer solo se observó una petición de eco con ICMPv4 de tipo 3 (Destination unreachable); pero con ICMPv6 se pudo encontrar los siguientes tipos: **130 Multicast Listener Query (*), 131 Multicast Listener Report (*), 132 Multicast Listener Done (*), 133 Router Solicitation (*), 134 Router Advertisement (*), 135 Neighbor solicitation (*), 143 Multicast Listener Report Message v2 (*)** y todos con código 0.

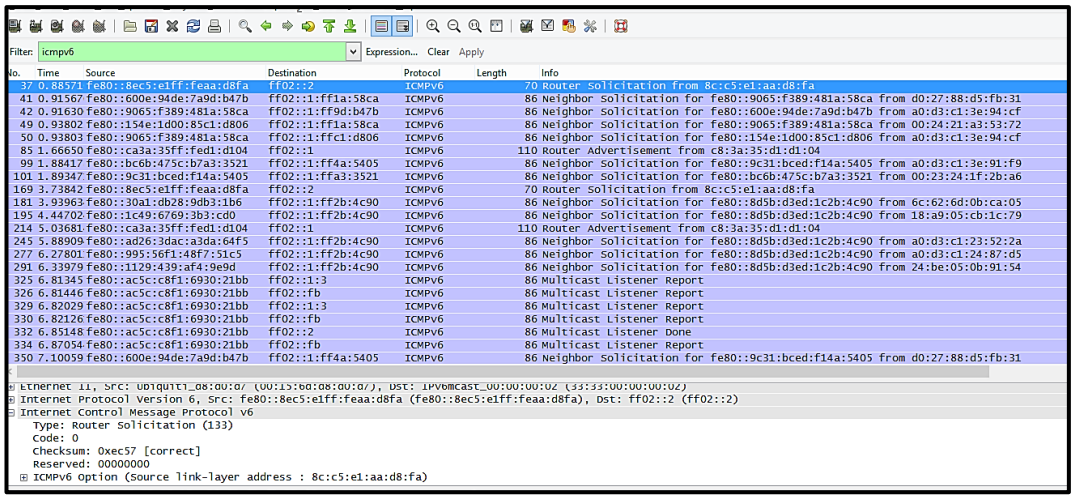


Figura 182: Respuestas del protocolo ICMPv6

Fuente: Elaboración propia. Recuperado de: Sniffer Wireshark

(g) Verificar defectos y probables nombres de comunidades SNMP en uso están de acuerdo al desarrollo práctico de todas las versiones de SNMP.

En la Figura 23, se puede apreciar que a pesar de que no existe ningún nombre de alguna comunidad SNMP configurada, con ayuda del comando ***snmpwalk***, se puede apreciar que se hace uso de una **comunidad pública en una impresora en red, misma que responde a la versión 1 y 2 de SNMP (*)**.

```
root@kali:~# snmpwalk -c public 192.20.3.159 -v 2c
iso.3.6.1.2.1.1.1.0 = STRING: "Xerox WorkCentre 6505DN; Net 95.48,ESS 201306131116,IOT 02.00.06,Boot 20140623163
3"
iso.3.6.1.2.1.1.2.0 = OID: iso.3.6.1.4.1.253.8.62.1.19.4.34.2.1
iso.3.6.1.2.1.1.3.0 = Timeticks: (27728622) 3 days, 5:01:26.22
iso.3.6.1.2.1.1.4.0 = ""
iso.3.6.1.2.1.1.5.0 = STRING: "WorkCentre 6505DN-5DFFBC"
iso.3.6.1.2.1.1.6.0 = ""
iso.3.6.1.2.1.1.7.0 = INTEGER: 64
iso.3.6.1.2.1.2.1.0 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.1.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.2.1 = STRING: "XEROX Ethernet Interface Controller, 10/100/1000 Mbps, RJ45, v1.0, 100Mbps fu
ll duplex"
iso.3.6.1.2.1.2.2.1.3.1 = INTEGER: 6
iso.3.6.1.2.1.2.2.1.4.1 = INTEGER: 1500
iso.3.6.1.2.1.2.2.1.5.1 = Gauge32: 100000000
iso.3.6.1.2.1.2.2.1.6.1 = Hex-STRING: 9C 93 4E 5D FF BC
iso.3.6.1.2.1.2.2.1.7.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.8.1 = INTEGER: 1
iso.3.6.1.2.1.2.2.1.9.1 = Timeticks: (0) 0:00:00.00
iso.3.6.1.2.1.2.2.1.10.1 = Counter32: 360576374
iso.3.6.1.2.1.2.2.1.11.1 = Counter32: 3641112
iso.3.6.1.2.1.2.2.1.12.1 = Counter32: 1054523
iso.3.6.1.2.1.2.2.1.13.1 = Counter32: 0
iso.3.6.1.2.1.2.2.1.14.1 = Counter32: 0
iso.3.6.1.2.1.2.2.1.15.1 = Counter32: 0
iso.3.6.1.2.1.2.2.1.16.1 = Counter32: 34017474
iso.3.6.1.2.1.2.2.1.17.1 = Counter32: 337630
```

Figura 193: Respuesta de NMAP en la búsqueda de comunidades SNMP activas

Fuente: Elaboración propia. Recuperado de: Kali Linux

(h) Buscar grupos de noticias, foros, VoIP y sistemas de comunicaciones basadas en la Web para las conexiones de información del objetivo y así determinar los sistemas de Gateway salientes y el direccionamiento interno.

En la Figura 24, se puede observar un extracto del método utilizado para determinar el sistema de Gateway y el direccionamiento interno del GADM, de los cuales el Gateway ya era conocido y para el direccionamiento interno se utiliza una dirección /24, haciendo uso de la siguiente nomenclatura: **192.20.3.XXX (*).**

Figura 204: Respuesta de NMAP en la búsqueda del direccionamiento interno

Fuente: Elaboración propia. Recuperado de: Kali Linux

En consecuencia, sumando todos los valores marcados con un asterisco (*), en cada uno de los literales descritos para este apartado, se tiene un valor numérico para la V**isibilidad** en este canal de: $\boldsymbol{P_V = 21}$

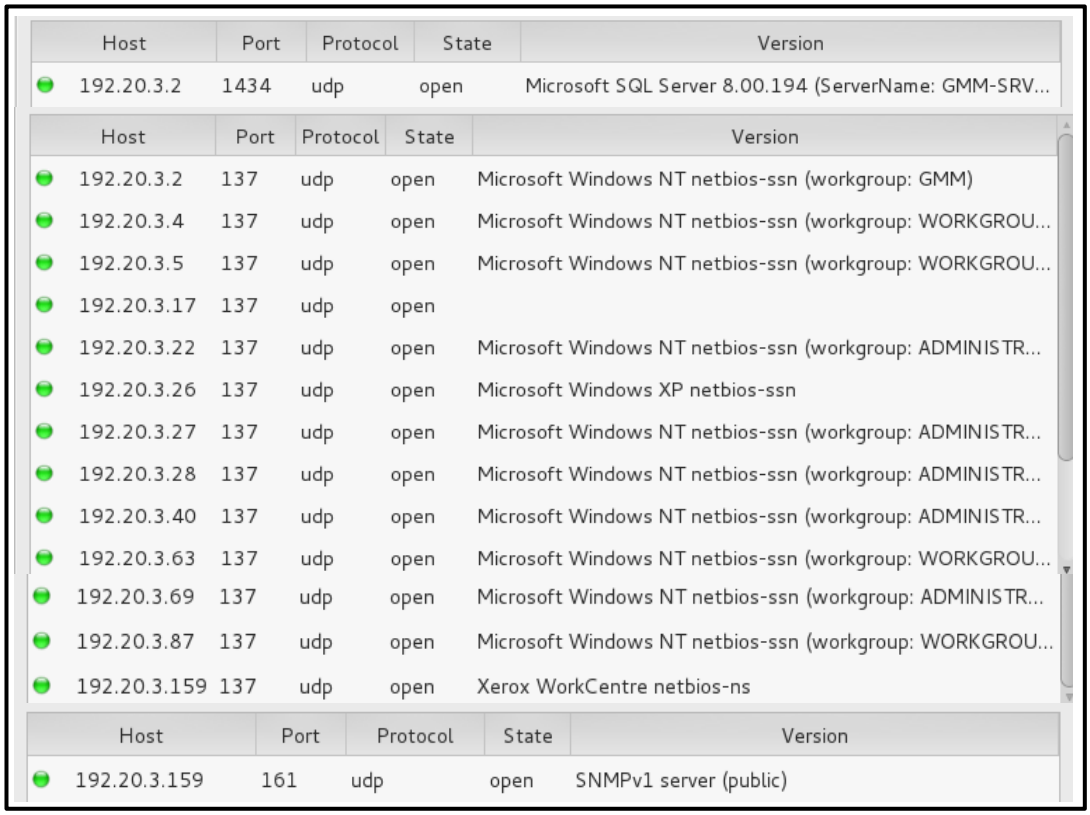
4.8.1.2 *Acceso (P_A).*

Realizar pruebas para la enumeración de los principales puntos de acceso dentro del alcance (Herzog, 2010).

(a) Solicitar servicios comunes conocidos los cuales utilizan UDP para las conexiones desde todas las direcciones.

Para encontrar los servicios que hacen uso del protocolo UDP para sus conexiones se hiso uso de la aplicación Sparta.py del software de auditorías de seguridad, Kali Linux 4.0. En la Figura 25, se puede observar los resultados que se obtuvieron al

escanear la red interna del GADM en búsqueda de los puertos UDP abiertos y sus respectivos servicios: puerto 1432 **ms-sql-m (*),** puerto 137 **netbios-ns (*)** y puerto 161 **snmp (*).**



Host	Port	Protocol	State	Version
192.20.3.2	1434	udp	open	Microsoft SQL Server 8.00.194 (ServerName: GMM-SRV...

Host	Port	Protocol	State	Version
192.20.3.2	137	udp	open	Microsoft Windows NT netbios-ssn (workgroup: GMM)
192.20.3.4	137	udp	open	Microsoft Windows NT netbios-ssn (workgroup: WORKGROU...
192.20.3.5	137	udp	open	Microsoft Windows NT netbios-ssn (workgroup: WORKGROU...
192.20.3.17	137	udp	open	
192.20.3.22	137	udp	open	Microsoft Windows NT netbios-ssn (workgroup: ADMINISTR...
192.20.3.26	137	udp	open	Microsoft Windows XP netbios-ssn
192.20.3.27	137	udp	open	Microsoft Windows NT netbios-ssn (workgroup: ADMINISTR...
192.20.3.28	137	udp	open	Microsoft Windows NT netbios-ssn (workgroup: ADMINISTR...
192.20.3.40	137	udp	open	Microsoft Windows NT netbios-ssn (workgroup: ADMINISTR...
192.20.3.63	137	udp	open	Microsoft Windows NT netbios-ssn (workgroup: WORKGROU...
192.20.3.69	137	udp	open	Microsoft Windows NT netbios-ssn (workgroup: ADMINISTR...
192.20.3.87	137	udp	open	Microsoft Windows NT netbios-ssn (workgroup: WORKGROU...
192.20.3.159	137	udp	open	Xerox WorkCentre netbios-ns

Host	Port	Protocol	State	Version
192.20.3.159	161	udp	open	SNMPv1 server (public)

Figura 215: Escaneo de puertos UDP con el software Sparta.py

Fuente: Elaboración propia. Recuperado de: Kali Linux

(b) Solicitar servicios comunes conocidos VPN, incluidos aquellos que utilizan IPSEC e IKE para conexiones desde todas las direcciones.

El GADM del cantón Mira no posee servicios que hagan uso de Redes Privadas Virtuales o VPN

(c) Solicitar servicios comunes conocidos los cuales utilizan TCP para las conexiones desde todas las direcciones y puertos sin filtrar que no han enviado ninguna respuesta a un SYN TCP.

En la Figura 26, se puede apreciar los servicios que hacen uso del protocolo TCP para sus conexiones, los que se utilizan comúnmente en el GAD son: **NetBIOS (*), telnet (*), ssh (*), smtp (*), https (*), http (*), ftp (*) y printer (*).**

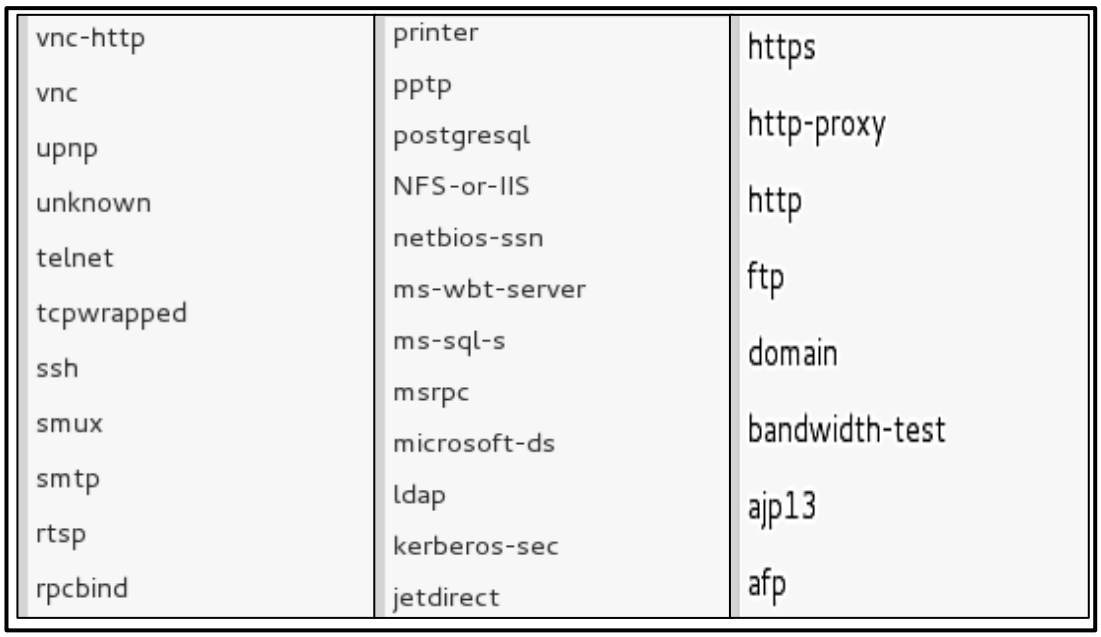


Figura 226: Escaneo de los servicios que hacen uso de TCP con ayuda de la aplicación Sparta.py
Fuente: Elaboración propia. Recuperado de: Kali Linux

(d) Relacionar cada puerto abierto a un proceso (servicio), la aplicación (código específico o producto que utiliza el servicio), y el protocolo (los medios para interactuar con dicho servicio o aplicación)

En la Tabla 40, se pude puede observar los puertos abiertos de la red LAN del GADM del Cantón Mira que sirven para ciertos servicios o aplicaciones. Puertos UDP: **137 (*)** y **161 (*);** y los puertos TCP **22 (*), 53 (*), 80 (*) y 443 (*) y 1432 (*).**

Tabla 40: Relación de puertos abiertos con los servicios

Puertos abiertos		
137	UDP	Este puerto es necesario para establecer una conexión con el servicios de NetBIOS que posee el GADM
161	UDP	Este puerto sirve para la impresión de documentos en red
22	TCP	Este puerto es de gran utilidad para establecer una conexión de acceso remoto segura al servidor de bases de datos para la extracción diaria de los respaldos del servidor
53	TCP	Este puerto se encuentra habilitado en el servidor de Internet para proveer de un servicio de DNS a los usuarios
80	TCP	Solo se encuentra habilitado para ciertas máquinas que hacen uso de contenidos de http.
443	TCP	Este puerto sirve para establecer conexiones seguras de http en páginas que así lo requieran.

1432	TCP	Este puerto se encuentra habilitado obligatoriamente en el servidor de bases de datos para almacenar los datos enviados por el biométrico

Fuente: Elaboración propia

(e) Verificar la disponibilidad del sistema operativo en comparación con las últimas vulnerabilidades y liberación del parche.

En la Figura 27, se pueden observar los Sistemas Operativos instalados actualmente en los ordenadores del GADM, mismos que se obtuvieron después del escaneo de la red LAN del GADM con ayuda de la aplicación Sparta.py

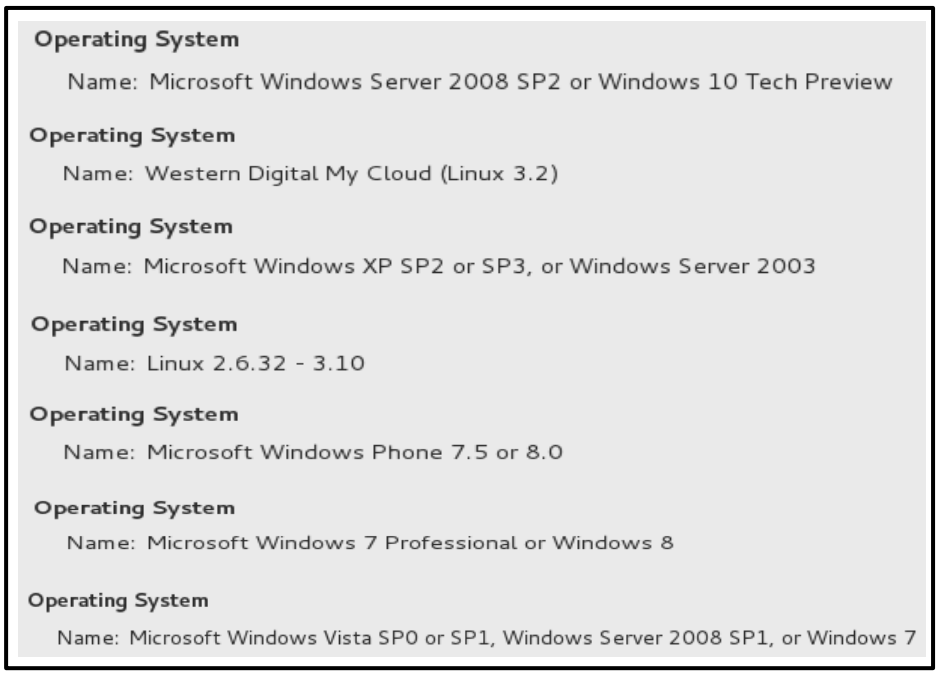


Figura 27: Sistemas Operativos vigentes encontrados con la aplicación Sparta.py

Fuente: Elaboración propia. Recuperado de: Kali Linux

Los sistemas operativos vulnerables actualmente son: **Microsoft Windows XP SP2 o SP3 (*) y Microsoft Windows Vista SP0 o SP1 (*),** esto debido a que la empresa Microsoft ya no brinda soporte para este tipo de versiones de Sistemas Operativos.

(f) Verificar los servicios de VoIP.

El GADM del Cantón Mira no posee servicios de VoIP.

En consecuencia, sumando todos los valores marcados con un asterisco (*) en cada uno de los literales de este apartado, se tiene un valor numérico para el A**cceso** en este canal de $\boldsymbol{P_A = 20.}$

4.8.1.3 *Confianza (P_T).*

Realizar pruebas de confianza entre los sistemas dentro del alcance donde la confianza se refiere al acceso a la información o propiedad física sin la necesidad de una identificación o autenticación (Herzog, 2010).

A la **Confianza** se le asignará un valor numérico de $\boldsymbol{P_T = 1}$ para este canal, esto debido a que para poder acceder tanto a la información como a la propiedad física del GADM-Mira se requiere únicamente la autorización del empleado encargado del activo donde se maneja la información o en su defecto a su estación de trabajo.

4.8.2 CONTROLES

Determinar los controles activos y pasivos para detectar los intentos de intrusión para filtrar o negar, los intentos deben probarse antes de la prueba real para mitigar el riesgo de dañar los datos del resultado de la prueba, así como cambiar el personal o los agentes de monitoreo de los estados de alarma. Puede ser necesario coordinar estas pruebas con las personas adecuadas dentro del alcance (Herzog, 2010)

4.8.2.1 *Autenticación (LC_{Au}).*

(a) Enumerar el proceso de autenticación para la solicitud de acceso y documentar todos los privilegios descubiertos que pueden ser utilizados para proporcionar acceso.

El proceso de autenticación consiste en **asignar una dirección IP manualmente por parte del Jefe del Área de Sistemas a un ordenador debidamente autorizado, con el que se pretenda acceder a la información del GADM (*)**, pero para poder acceder a la información de los servidores el Administrador asigna privilegios de: **lectura y escritura (*), solo lectura (*), o solo escritura (*).**

(b) Verificar el método para obtener una apropiada autorización para la autenticación.

El método de autorización, para la autenticación consiste en **la verificación personal por parte del Jefe del Área de Sistemas, al ordenador con el que se va a acceder a la información del GADM (*).**

(c) Verificar el método para ser identificado correctamente y poder contar con la autenticación.

El método para ser identificado consiste en el **registro de la dirección IP (*)**, que no debe ser cambiada por nadie más que por el Jefe del Área de Sistemas, ya es la única manera de poder identificar a un usuario válido dentro de la LAN del GADM.

(d) Verificar la solidez de la autenticación a través del descifrado de contraseñas y volver a aplicar las contraseñas descubiertas a todos los puntos de acceso que requieren autenticación.

La solidez de la autenticación es baja, ya que un usuario nuevo no requiere de contraseñas para acceder a la información del GADM, sino de un ordenador autorizado y la asignación de una dirección IP.

Por lo tanto, sumando los valores marcados con un asterisco (*) en cada uno de los literales de este ítem, se tiene un valor numérico para el control de **Autenticación** de $\boldsymbol{LC_{Au} = 6}$.

4.8.2.2 *Indemnización (LC_{Id}).*

(a) Documentar y enumerar los objetivos y servicios que están protegidos contra el abuso o elusión de la política de los empleados, están asegurados por robo o daños, o utilizan renuncias de responsabilidad y permisos.

No existen objetivos que se encuentren protegidos contra el abuso o la elusión de políticas de los empleados, los objetivos que se encuentran asegurados contra el robo o daños son **los equipos de computación (*)**, **ordenadores móviles (*), y el equipo de comunicación (*)** y los objetivos que hacen uso de las renuncias de responsabilidad son **los sistemas informáticos (*).**

(b) Verificar el efecto de las limitaciones de responsabilidad en la seguridad o medidas de seguridad.

El efecto que causan las limitaciones de responsabilidad es **que usuarios que no deben acceder a la información reservada del GADM, intenten acceder a ella sin una debida autorización (*).**

(c) Examinar el lenguaje de la póliza de seguro por limitaciones en los tipos de daños o activos.

Las limitaciones contempladas en las pólizas de seguros son: **golpes intencionados a los equipos (*), daños por descargas eléctricas (*), daños por mal manejo (*) y robos o hurtos no comprobables (*).**

En consecuencia, sumando los valores marcados con un asterisco (*) en cada uno de los literales contemplados para este ítem se tiene un valor numérico para el control de **Indemnización** de: $\boldsymbol{LC_{Id} = 9}$.

4.8.2.3 *Resistencia (LC_{Re}).*

(a) Verificar los puntos únicos de fallo (cuellos de botella) en la infraestructura donde el cambio o el fracaso pueden causar una interrupción del servicio.

Uno de los puntos más críticos dentro de la infraestructura de la red LAN del GADM es **su sistema de cableado estructurado (*),** ya que prácticamente ha cumplido con su periodo de vida útil y necesita que sea cambiado, otro punto crítico es que **la escalabilidad con la que contaba la red ya ha colapsado (*),** y para poder afrontar este problema temporalmente se conectan switches en cascada.

(b) Verificar el impacto al acceso del objetivo que causará un fallo del sistema o servicio.

Los posibles impactos al acceso de los objetivos que pueden causar fallos a los sistemas son: **los equipos que han cumplido con el tiempo de vida útil (*), cuando se satura los equipos de sistemas con mucha información de la ciudadanía (*)**

(c) Verificar los privilegios disponibles del acceso inducido por fallos.

No se manejan privilegios de acceso en caso de fallas.

(d) Verificar la funcionalidad operacional de los controles para evitar el acceso o permisos por encima de posibles privilegios más bajos en caso de fallo.

No se manejan privilegios de acceso dentro de los controles del GADM

Contabilizando los valores marcados (*) en los literales anteriores, se tiene un valor numérico total para la **Resistencia** en este canal de: $\boldsymbol{LC_{Re} = 4}$

4.8.2.4 *Subyugación (LC_{Su}).*

En una auditoría de redes de datos COMSEC, si un log-in puede hacerse en HTTP, así como en HTTPS, pero requiere que el usuario haga esa distinción, entonces se produce un error al contar la subyugación. Sin embargo, si la aplicación requiere el modo seguro por defecto, tal como un sistema de mensajería interna PKI, entonces cumple con el requisito del control de subyugación para el alcance (Herzog, 2010).

Las aplicaciones que manejan por defecto el uso de HTTPS son las del **Departamento Jurídico (*), y las que acceden a las plataformas financiera**s **públicas (*).** El servicio de acceso remoto se puede manejar vía Telnet o SSH, pero este valor no se tomará en cuenta ya que el uso de uno u otro protocolo depende del usuario.

El valor numérico para el control de **Subyugación**, en este canal es de: $\boldsymbol{LC_{Su} = 2}$ sumando los dos criterios descritos en la explicación anterior.

4.8.2.5 *Continuidad (LC_{Ct}).*

(a) Enumerar y probar las insuficiencias de todos los objetivos con respecto a los retrasos de acceso y los tiempos de respuesta del servicio a través de los sistemas de back-up o el cambio a canales alternativos.

Debido a que los equipos de comunicaciones no poseen un adecuado respaldo y dependiendo del equipo que haya sufrido una falla, **el tiempo de reposición del equipo pude demorarse alrededor de un mes (*),** pero el acceso se lo trata de reponer lo más rápido posible.

(b) Verificar que los esquemas de bloqueo contra intrusos no puedan ser usados contra los usuarios válidos.

En el GADM no se manejan bloqueos contra intrusos.

Por lo tanto, el valor numérico para el control de **Continuidad**, en este canal es de: $\boldsymbol{LC_{Ct} = 1}$, tomando en cuenta la insuficiencia que se marca en el literal (a) de las descripciones anteriores.

4.8.2.6 *No repudio (LC_{NR}).*

(a) Enumerar y evaluar el uso o insuficiencias de los procesos y sistemas para identificar correctamente y registrar el acceso o las interacciones con la propiedad.
(b) Verificar que todos los métodos de interacciones sean registrados adecuadamente con la identificación apropiada.

El único método que permite identificar el acceso a la propiedad del GADM-Mira es el **sistema de video-vigilancia (*).** Por lo tanto el control de **No-Repudio** tiene un valor numérico de $\boldsymbol{LC_{NR} = 1}$**,** para este canal.

4.8.2.7 *Confidencialidad (LC_{Cf}).*

(a) Enumerar todas las interacciones con los servicios dentro del alcance de las comunicaciones o activos transportados a través del canal mediante el uso de líneas seguras, encriptación, interacciones "silenciadas" o "cerradas" para proteger la confidencialidad de la propiedad de la información entre las partes involucradas.
(b) Verificar los métodos aceptables utilizados para la confidencialidad.
(c) Probar la resistencia y el diseño del método de cifrado u ofuscación.
(d) Verificar los límites exteriores de comunicación el cual puede ser protegido por medio de los métodos aplicados para la confidencialidad.

En el GADM no se hace uso de un control específico de **Confidencialidad**, por lo tanto se tiene un valor numérico de este control de: $\boldsymbol{LC_{Cf} = 0}$.

4.8.2.8 *Privacidad (LC_{Pr}).*

(a) Enumerar los servicios dentro del alcance de las comunicaciones o los activos transportados mediante firmas específicas, firmas individuales, identificación personal, interacciones personales "silenciosas" o "habitaciones cerradas" para proteger la privacidad de la interacción y el proceso de proporcionar activos sólo a aquellos dentro de la habilitación de seguridad apropiada para ese proceso, comunicación o activo.

Los servicios que requieren de una identificación personal son los sistemas de información: **Sistema Integral de Catastros (*), Sistema de Agua Potable (*) y los Sistemas Financieros (*)**

(b) Relacionar la información con los puertos TCP y UDP que no responden, para determinar si la disponibilidad depende de un tipo privado de contacto o protocolo.

En la Figura 28, se puede verificar que existen varios puertos TCP que no responden, debido a que se encuentran filtrados, ya que son de uso exclusivo para un protocolo privado en particular, el cual corresponde para el uso de Ubiquiti Networks, entre ellos se encuentran los siguientes: **17 (*), 37 (*), 119 (*), 616 (*), 617 (*), 687 (*), 726 (*), 990 (*), 1053 (*), 1434 (*), 2701 (*), 4445 (*), 5822 (*), 5901 (*), 7625 (*) y 8084 (*).**

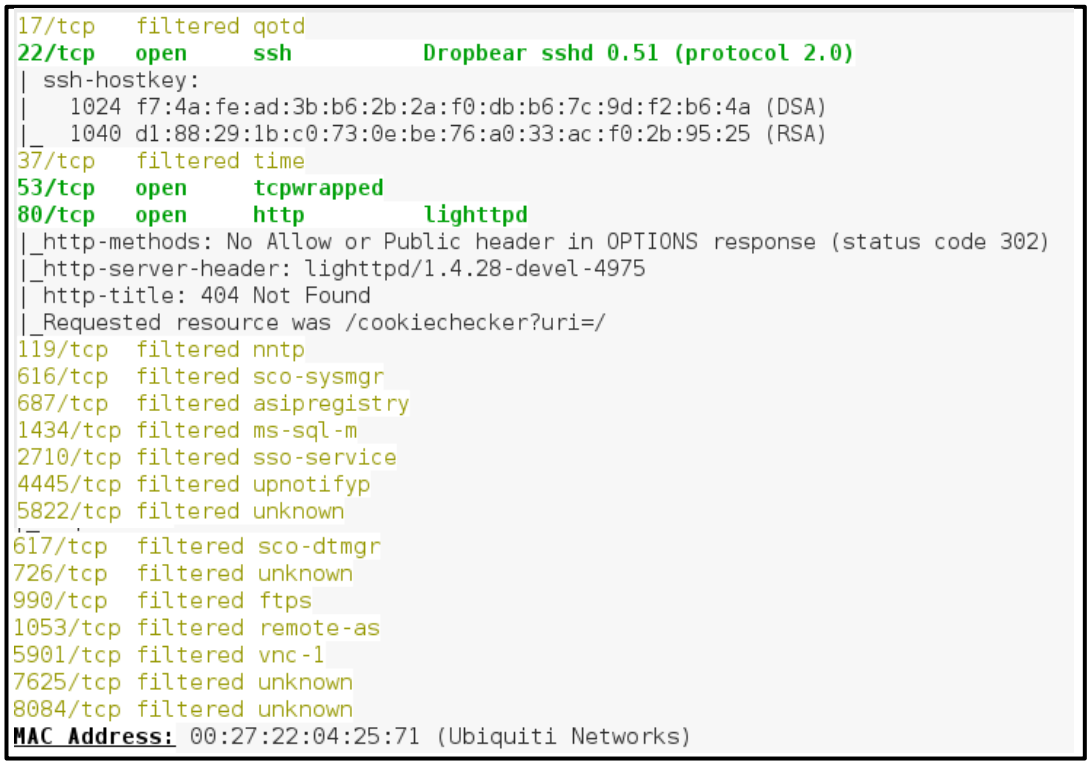


Figura 28: Puertos TCP filtrados, encontrados en la aplicación Zenmap

Fuente: Elaboración propia. Recuperado de: Kali Linux

En consecuencia, sumando los valores marcados (*) en los literales anteriores, se tiene un valor numérico total para la **Privacidad** para este canal de: $\boldsymbol{LC_{Pr} = 19}$.

4.8.2.9 *Integridad (LC_{It}).*

Enumerar y probar las deficiencias de la integridad cuando se utiliza un proceso documentado, firmas, cifrado, hash, o marcas para asegurar que el activo no pueda ser cambiado, redirigido, o invertido sin que sea conocido por las partes involucradas.

En el GADM del cantón Mira no se maneja algún tipo de control que asegure que la integridad de la información no sea vulnerada, por lo tanto el valor numérico de este ítem es de: $\boldsymbol{LC_{It} = 0}$.

4.8.2.10 *Alarma (LC_{Al}).*

Verificar y enumerar la utilización de un sistema de alerta localizado en todo el alcance, registro, o un mensaje para cada Gateway de acceso a través de cada canal donde una situación sospechosa es observada por el personal, en caso de duda de elusión por parte de intrusos, ingeniería social, o una actividad fraudulenta.

El sistema de alarma que manejan los equipos de cómputo del GADM es el **servicio de anti-virus que mantienen contratado a la empresa ESET (*)**, el cual también provee los servicios de **Firewall (*)**, los cuales se encargan de enviar una notificación a cualquier usuario en caso de que encuentre algún tipo de actividad sospechosa dentro de la red.

En consecuencia, el valor numérico para el control de **Alarma** en este canal es de: $\boldsymbol{LC_{Al} = 2}$.

4.8.3 LIMITACIONES

4.8.3.1 *Vulnerabilidad (Lv).*

Una vulnerabilidad puede ser un defecto en el software que permite a un atacante sobrescribir en el espacio de memoria para tener acceso, una falla de cálculo que permite a un atacante bloquear al 100% el uso del CPU, o un sistema operativo que permite que los datos suficientes sean copiados en el disco hasta que ya no pueda funcionar más.

La **Vulnerabilidad** más visible, encontrada dentro de este canal es la **utilización de 25 ordenadores que utilizan el Sistema Operativo de Microsoft Windows XP (*),** por lo tanto se tiene un valor numérico para este ítem de: $\boldsymbol{Lv}$ **= 25.**

4.8.3.2 *Debilidad (L_w).*

Una debilidad puede ser un inicio de sesión que permite intentos ilimitados a una granja de servidores web. (Herzog, 2010)

- Para el control de Autenticación existe un error **al verificar el ordenador con el que una persona intente acceder a la red municipal del GADM (*)**, ya que no se puede conocer a ciencia cierta todo el contenido del ordenador, y debería tener algún tipo de sustento en un documento legal en caso de que se utilicen los recursos del GADM de manera malintencionada; también existe un error al llevar **un registro manual de direcciones IP (*)** ya que están sujetas a los errores humanos.
- Para el control de Indemnización existe una **descompensación con los usuarios de los sistemas informáticos del GADM-Mira (*),** ya que ellos deberían someterse no sólo a renuncias de responsabilidad, sino también a renuncias de uso/usuario y a acuerdo de confidencialidad y no divulgación de los datos.
- Para el control de Resistencia existen fallas en el **sistema de cableado estructurado de la Institución (*)** porque ya es prácticamente obsoleto**, en la escalabilidad de la red municipal (*), en el uso de ordenadores que ya han cumplido con el tiempo de vida útil (*).**
- Para el control de Continuidad existe error en el **tiempo de reposición de un equipo de comunicación (*),** ya que un mes no es tiempo prudencial para tratar los errores que puedan presentarse por la falta de dicho equipo.
- Para el control de Subyugación no existen errores.

En consecuencia, aplicando el concepto de la ecuación 4, el cual consiste en contabilizar los defectos o errores en los controles de Clase A, mismos que se describen en las explicaciones anteriores, se tiene un valor numérico para la **Debilidad**, en este canal de:

$$\boldsymbol{L_w = FC_{Au} + FC_{Id} + FC_{Re} + FC_{Su} + FC_{Ct}}$$

$$\boldsymbol{L_w = 2 + 1 + 3 + 0 + 1}$$

$$\boldsymbol{L_w = 7}$$

4.8.3.3 *Preocupación (L_C).*

Una preocupación puede ser el uso de certificados del servidor web generados localmente para HTTPS o archivos que registran solo los participantes en las operaciones y no la fecha y la hora correcta del registro de transacciones.

- Para el control de No-repudio existe una deficiencia en el **uso de un sistema de video-vigilancia (*),** ya que se pueden aplicar otras medidas para prever que las personas no puedan negar que han establecido una conexión.
- Para el control de Privacidad existe un defecto al utilizar identificaciones personales sólo a los sistemas que maneja el GADM, a ellos deberían sumarse también el acceso a las **áreas restringidas (*) y las bodegas (*).**
- Para el control de Alarma existe una deficiencia en el **firewall (*)** ya que a este se le debería sumar el filtrado de páginas con acceso restringido.
- Para los controles de Confidencialidad e Integridad no se encontraron errores o deficiencias.

En consecuencia, aplicando el concepto de la ecuación 5, la cual consiste en contabilizar los defectos o errores en los controles de clase B, se tiene un valor numérico para la **Preocupación**, en este canal de:

$$\boldsymbol{L_C = FC_{NR} + FC_{Cf} + FC_{Pr} + FC_{It} + FC_{Al}}$$

$$\boldsymbol{L_C = 1 + 0 + 2 + 0 + 1}$$

$$\boldsymbol{L_C = 4}$$

4.8.3.4 *Exposición (L_E).*

Una exposición puede ser una bandera descriptiva y válida acerca de un servicio, o una respuesta de eco ICMP desde un host.

Los hosts que se encuentran dentro de la red sí **responden a las peticiones de eco independientemente del objetivo que lo genere (*)**

Al realizar un proceso de traza, **se muestra el nombre del servidor de Internet que funciona como Gateway de salida y entrada (*).**

En consecuencia, contabilizando los valores marcados con un asterisco de la lista anterior, se tiene un valor numérico para la **Exposición**, en este canal es de $\boldsymbol{L_E = 2}$**.**

4.8.3.5 *Anomalía (L_A).*

Una anomalía pueden ser respuestas correctas a un sondeo de una dirección IP diferente de la que fue sondeada o esperada.

La única anomalía manifestada por el director de Área de sistemas del GADM es que **a pesar de que se han hecho varias peticiones de que se ajuste el sistema de alimentación eléctrica a las condiciones de funcionamiento que necesitan los equipos de comunicaciones que se encuentran dentro del data center del GADM, no se han tomado acciones correctivas por parte de los altos funcionarios (*).**

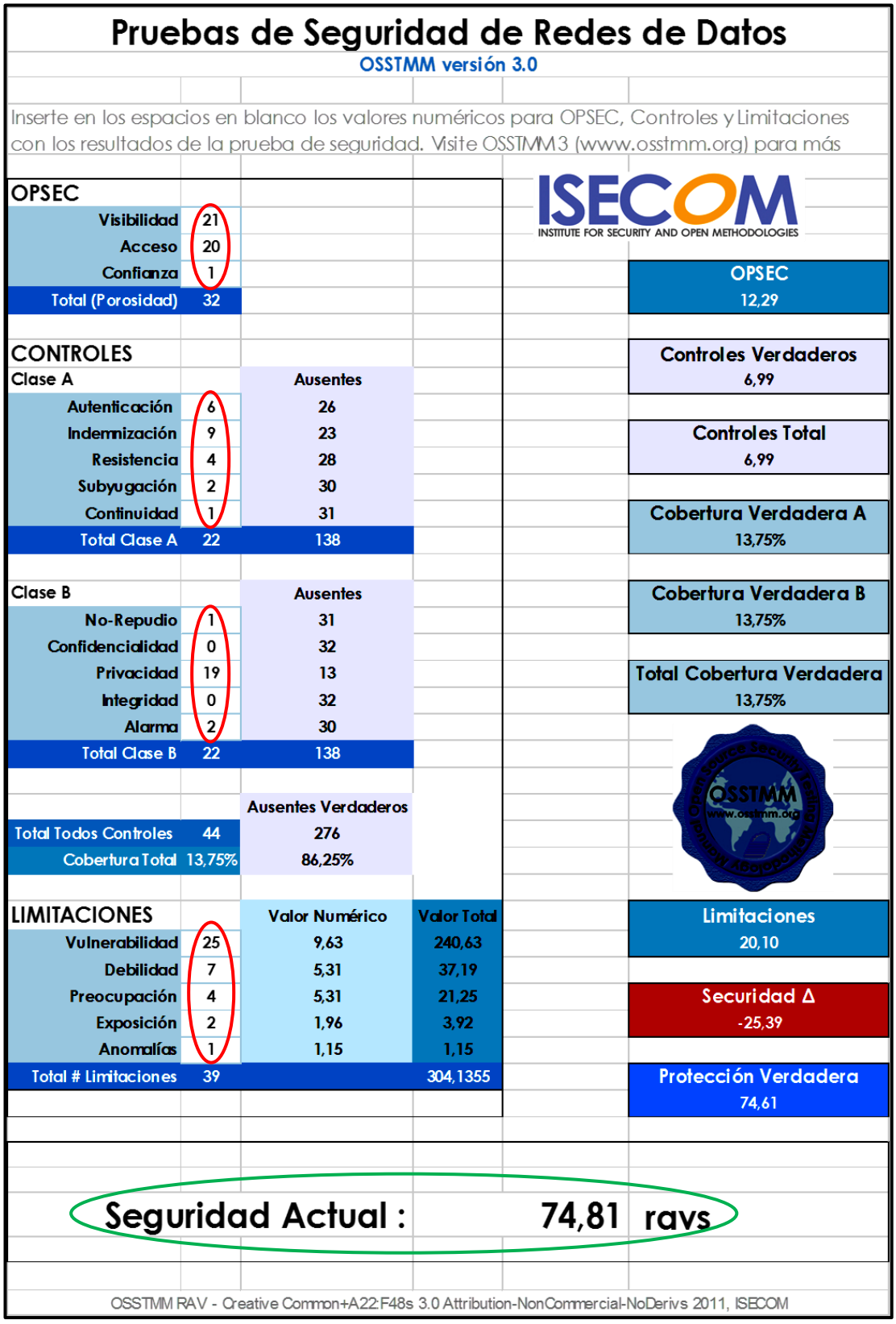
Por lo tanto, considerando el criterio anteriormente descrito, se tiene un valor numérico para las **Anomalías**, en este canal de: $\boldsymbol{L_A = 1}$.

4.8.4 Calculadora RAV

En la Tabla 41, se pueden observar los valores obtenidos para la superficie de ataque en las pruebas de seguridad aplicadas al canal de redes de datos para el GADM del cantón Mira, para ello se ha seguido el procedimiento que dicta la metodología, es decir, insertar los valores correspondientes en los cuadros específicos de cada ítem requerido tanto a la **porosidad (OPSEC):** Visibilidad=21, Acceso=20 y Confianza=1; **controles:** Autenticación = 6, Indemnización = 9, Resistencia = 4, Subyugación = 2, Continuidad=1, No-Repudio=1, Confidencialidad = 0, Privacidad = 19, Integridad = 0 y Alarma = 2; y **limitaciones**: Vulnerabilidad = 25, Debilidad = 7, Preocupación = 4, Exposición = 2 y Anomalía = 1.

En el Anexo 14, se encuentra el respectivo reporte del canal de redes de datos auditado en donde constan todos los valores de la hoja de cálculo del RAV, mismos que deben ser acreditados por el representante del GADM-Mira, a éste también se anexan las evidencias de los métodos que se aplicaron, para obtener datos que no se pudieron generar con el software de auditoría.

Tabla 41: Resultados obtenidos en la auditoria del canal de seguridad de redes de datos para el GADM-Mira



Pruebas de Seguridad de Redes de Datos

OSSTMM versión 3.0

Inserte en los espacios en blanco los valores numéricos para OPSEC, Controles y Limitaciones con los resultados de la prueba de seguridad. Visite OSSTMM3 (www.osstmm.org) para más

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

OPSEC		
Visibilidad	21	
Acceso	20	
Confianza	1	
Total (Porosidad)	32	

CONTROLES		
Clase A		Ausentes
Autenticación	6	26
Indemnización	9	23
Resistencia	4	28
Subyugación	2	30
Continuidad	1	31
Total Clase A	22	138
Clase B		Ausentes
No-Repudio	1	31
Confidencialidad	0	32
Privacidad	19	13
Integridad	0	32
Alarma	2	30
Total Clase B	22	138
		Ausentes Verdaderos
Total Todos Controles	44	276
Cobertura Total	13,75%	86,25%

LIMITACIONES		Valor Numérico	Valor Total
Vulnerabilidad	25	9,63	240,63
Debilidad	7	5,31	37,19
Preocupación	4	5,31	21,25
Exposición	2	1,96	3,92
Anomalías	1	1,15	1,15
Total # Limitaciones	39		304,1355

OPSEC	12,29
Controles Verdaderos	6,99
Controles Total	6,99
Cobertura Verdadera A	13,75%
Cobertura Verdadera B	13,75%
Total Cobertura Verdadera	13,75%
Limitaciones	20,10
Seguridad Δ	-25,39
Protección Verdadera	74,61

OSSTMM
www.osstmm.org

Seguridad Actual : 74,81 ravs

Fuente: Elaboración propia. Recuperado de: Calculadora de RAV de OSSTMM3.

4.8.5 Análisis de Resultados

Una vez que se han insertado los valores numéricos de la porosidad, los controles y las limitaciones en la hoja de cálculo del RAV, tal como se muestra en tabla anterior, los datos rotulados con color rojo; los demás valores se generan de forma automática, de los cuales, los valores más significativos, por el hecho de que permiten realizar un análisis evaluativo del canal auditado son: el **Seguridad** Δ (celda de color rojo), y la **Seguridad Actual** (valor rotulado con color verde).

Para el caso del **Seguridad** Δ**,** su valor puede ser ratificado haciendo uso de la ecuación 6, así:

$$\textbf{Seguridad } \Delta = \textbf{Controles Verdaderos} - \textbf{OPSEC} - \textbf{Limitaciones}$$

$$\textbf{Seguridad } \Delta = 6,99 - 12,29 - 20,10$$

$$\textbf{Seguridad } \Delta = -25,40$$

Al igual que en los canales anteriores, se concluirá realizando un análisis en primer lugar del **Seguridad** Δ**,** que para este caso posee un valor negativo de -25,39; lo que se interpreta como una limitación muy grave en los controles operacionales implementados por el GADM del Cantón Mira en sus infraestructura de red de datos, ya que este es el recurso más sensible de la información que se genera no solo por el personal de la Institución, sino también de la información que se maneja por medio de los servicios que brinda a la ciudadanía del cantón, y a terceras personas.

La **seguridad actual** posee un valor numérico de 74,81 ravs, lo que se traduce un valor aproximado de deficiencia en los controles operacionales para este canal del 25%, este es un valor se considera demasiado alto ya que para este canal se debería considerar un valor aceptable cuando fluctué entre el ±10% del nivel de 100 ravs, en tal virtud se deberían considerar muchas medidas de prevención, para ir implementando las medidas de seguridad que son necesarias para asegurar la información generada por la infraestructura de red de la Institución paulatinamente, tales como la restructuración del sistema de cableado estructurado y por ende el debido etiquetado, implementación de equipos de comunicaciones como routers o switches administrables y de propiedad de la entidad, firewall, sistemas de alarmas, sistemas de redundancia, entre otros.

Una recomendación que para este caso es práctica y que va dirigida al director del Área de sistemas es que se debería hacer las diligencias del caso para que se contrate a un equipo de soporte aunque sea por una temporada pertinente, para restructurar la red de datos del GADM-Mira desde sus bases y en caso de ser necesario trabajar en horarios extras para no perturbar las actividades que realiza el personal en sus horarios de trabajo; y si se considera pertinente rediseñar el cuarto de comunicaciones pero tomando en cuenta su adaptación a algún tipo de estándar.

Al finalizar todo el proceso de la auditoría, y una vez que se han obtenido los reportes de los cuatro canales auditados, se procedió a redactar un informe final de la auditoría (ver Anexo 15), mismo que debe ser aprobado por el representante del Área de sistemas del GADM. En dicho informe se hace una pequeña propuesta de mejoramiento con las recomendaciones de cada canal.

4.9 Resultados Finales

En la Tabla 42, se pueden observar de mejor manera los resultados finales obtenidos, luego de haber realizado las pruebas para cada canal, mismos que son recogidos de las tablas: 28, 36, 39 y 41; con estos resultados se da fin al proceso evaluativo del estado actual del sistema de seguridad del GADM-Mira. Cabe señalar que la finalidad de hacer un promedio de los valores numéricos obtenidos de los diferentes canales es hacer un análisis general del **Seguridad Δ,** que muestra de manera global la deficiencia de los mecanismos de seguridad adoptados actualmente por el GADM-Mira, que es aproximadamente del 20%.

Tabla 42: Resultados Finales

VALORES DE ANÁLISIS					
Canal Ítem	**Humano**	**Físico**	**Inalámbrico**	**Redes de Datos**	**Promedio**
OpSec	9.48	11.43	8.43	12.29	10.41
Limitaciones	14.04	16.12	11.76	20.10	15.51
Controles Verdaderos	5.4	6.21	4.34	6.99	5.74
Seguridad Δ	-18.11	-21.34	-15.85	-25.39	-20.17
Protección Verdadera	81.89	78.66	84.15	74.61	79.83
Seguridad Actual	81.95 ravs	78.79 ravs	84.26 ravs	74.81 ravs	79.95 ravs

Fuente: Elaboración propia

4.10 MEDIDAS INTERVENTIVAS

La primera medida interventiva que se extendió al GADM-Mira consta de una propuesta técnica de mejoramiento (literal 8 del Anexo 15), en base a los resultados obtenidos de las pruebas realizadas y del proceso de la auditoría en sí; si bien las medidas correctivas no constan con un cronograma de aplicación, esto se debe a que en ella se hace la recomendación de la adquisición de varios equipos, y este fundamento depende de la asignación presupuestaría con la que cuente el Área de Sistemas de la Institución, por lo que podría ser una propuesta a largo plazo.

Como una segunda medida interventiva que se consideró de vital importancia para el GADM-Mira es la elaboración de la primera versión de su Manual Interno de Políticas de Seguridad de la Información, esto con el fin de regular las actividades que se realizan dentro de la infraestructura de la Institución por parte tanto del personal como de terceras personas y en caso de que sea necesario aplicar las medidas sancionarías pertinentes.

En la sección dos se hace referencia al uso de los catalizadores de COBIT para implementar la seguridad de la información en la práctica (principios, políticas y marcos de referencia; procesos; estructuras organizativas; cultura, ética y comportamiento; información; servicios, infraestructura y aplicaciones; personas habilidades y competencias), y en contexto se expresa la utilidad de las políticas relacionadas con la seguridad de la información dentro de una organización; por lo tanto se utiliza únicamente el catalizador de principios, políticas y marcos de referencia para la generación de las políticas de seguridad de la información en el GADM-Mira. (ISACA, 2012).

4.10.1 MANUAL DE POLÍTICAS DE SEGURIDAD

Basándose en el Apéndice A del estándar COBIT 5 para la Seguridad de la Información: guía detallada del catalizador de principios, políticas y marcos de referencia se detalla la distribución de las políticas de seguridad de la información, las cuales se encuentran distribuidas en dos grupos de políticas específicas de seguridad de la información: las que son dirigidas por la función de seguridad de la información y las que son dirigidas por otras funciones dentro de la organización.

En las dirigidas por la función de seguridad de la información se encuentran las siguientes políticas: de control de acceso, de seguridad de la información relativa al personal, de seguridad física y ambiental, de respuesta a incidentes de seguridad. En las políticas dirigidas por otras funciones dentro de la organización se encuentran las siguientes: de recuperación ante desastres, de gestión de activos, reglas de conducta; de adquisición, desarrollo y mantenimiento de sistemas de información; de gestión de proveedores, de gestión de las comunicaciones y operaciones, de cumplimiento, de gestión de riesgos.

Las políticas dirigidas por la función de seguridad de la información deben destinarse de forma independiente a las diferentes unidades departamentales de la organización, a los proveedores, visitantes y a terceras personas; y su actualización y revalidación debe involucrar por lo menos a los departamentos: de recursos humanos, jurídico, personal de apoyo (guardias) y a los empleados encargados del departamento de sistemas y de la seguridad de la información; por lo tanto toda política nueva o actualizada debe distribuirse a los empleados (fijos como temporales), contratistas, proveedores (dependiendo de las especificaciones del contrato), y a terceras personas.

Para las políticas dirigidas por otras funciones dentro de la organización, se debe contar con la opinión explicita del departamento que se encuentre encargado de la seguridad de la información y sus alcances deben medirse conjuntamente con las unidades departamentales que se encuentran incluidas en las mismas.

El manual consta de la siguiente estructura:

4.10.2 INTRODUCCIÓN

La base para que cualquier organización pueda operar de una forma confiable en materia de Seguridad Informática comienza con la definición de políticas y estándares adecuados.

Este documento se encuentra estructurado en trece políticas generales de seguridad para usuarios de informática, en base a la referencia de un estándar el considera los siguientes puntos:

- Políticas generales de seguridad de la información.
- Política de control de accesos.
- Política de seguridad de la información del personal.

- Política de seguridad física y ambiental.
- Política de gestión de incidentes.
- Política de continuidad de las operaciones y recuperación ante desastres.
- Política de gestión de activos.
- Reglas de comportamiento.
- Políticas de adquisición, desarrollo de software y mantenimiento de sistemas informáticos.
- Política de gestión de proveedores.
- Política de gestión de comunicaciones y operaciones
- Política de cumplimiento.
- Política de gestión de riesgos.

4.10.3 DEFINICIÓN

La Seguridad de la Información, es una función en la que se deben evaluar y administrar los riesgos, basándose en políticas y estándares que cubran las necesidades de la organización en materia de seguridad. Una política de seguridad de la información es un conjunto de reglas aplicadas a todas las actividades relacionadas al manejo de la información de una entidad, teniendo el propósito de proteger la información, los recursos y la reputación de la misma.

4.10.4 OBJETIVO

Proporcionar dirección y apoyo directivo para brindar seguridad a todo el recurso informático del Gobierno Autónomo Descentralizado Municipal del Cantón Mira. El nivel directivo debe establecer una dirección y política clara, demostrar apoyo y compromiso con respecto a la seguridad de la información, mediante la formulación y mantenimiento de una política de seguridad de la información a través de toda la organización.

4.10.5 ALCANCE

El documento define las Políticas de Seguridad de la Información que deberán conocer de manera obligatoria todo el personal del GADM del Cantón Mira para el buen uso de sus recursos informáticos, activos, aplicaciones y servicios que se encuentren bajo el dominio de la Institución.

4.10.6 BENEFICIO

Las Políticas de Seguridad de la Información establecidas en el presente documento son la base fundamental para la protección de los activos informáticos y de toda la información generada por medio de herramientas de las Tecnologías de la Información y Comunicación (TIC´s) en el GADM-Mira.

4.10.7 VIGENCIA

Al ser la primera versión de un manual de políticas de seguridad de la información que se implementa en el GADM del Cantón Mira, se entregará en primer lugar como un borrador al encargado del área de sistemas en turno, quien deberá realizar las revisiones pertinentes y en caso de ser necesario las adecuaciones que competan, de allí se deberá realizar el procedimiento administrativo pertinente con las autoridades competentes de la Institución quienes verán la necesidad de su aprobación, momento en el cual entrará legalmente en vigencia.

4.10.8 DIFUSIÓN DE LA POLÍTICA

Será responsabilidad del Departamento de Sistemas difundir los temas relevantes en materia de seguridad informática. Las políticas de seguridad de la información deberán ser comunicadas a todo el personal de planta del Gobierno Autónomo Descentralizado del cantón Mira y a terceros que presten servicios en la Institución y a las entidades externas relevantes.

Para la difusión de los contenidos de las políticas de seguridad la información al interior de la institución se deberá utilizar los medios de difusión que disponga el Departamento de Comunicación, así como también instancias de capacitación llevadas a cabo para este efecto.

Los principales medios serán:

- Intranet institucional
- Circulantes informativas
- Inducción al personal que ingresen al servicio
- Comunicaciones a través de charlas y reuniones

Para cumplir lo anteriormente mencionado se deberá definir, implementar y evaluar las acciones e iniciativas contenidas en un Plan de Difusión, Sensibilización y Capacitación en materia de seguridad informática.

4.10.9 FRECUENCIA DE EVALUACIÓN DE LAS POLÍTICAS

Dependiendo de la experiencia que se vaya ganando con el presente manual y en caso de ser necesario, después de un tiempo prudencial, recomendablemente seis meses, se deberá hacer la debida actualización, adecuación, modificación del mismo.

4.10.10SANCIONES POR INCUMPLIMIENTO

El incumplimiento del presente Manual de Políticas de Seguridad de la Información podrá presumirse como causa de responsabilidad administrativa y/o penal, dependiendo de su naturaleza y gravedad, cuya aplicación de la sanción dependerá de las autoridades competentes, ya sea a nivel interno o en su defecto a los jueces de la región.

4.10.11EXCEPCIONES

Las excepciones a cualquier cumplimiento del Manual de Políticas de Seguridad de la Información deben ser aprobadas por el organismo o departamento competente dentro del GADM del Cantón Mira, y dichas excepciones deben ser formalmente documentadas, registradas y revisadas.

El Manual consta de 220 Artículos en donde se recogen muchas de las falencias encontradas en cada uno de los cuatro canales auditados y para constancia de la entrega del mismo se emitirá un documento de recibido por parte del representante del GADM (ver Anexo 16) seguidamente se puede contemplar todo el contenido del Manual; en lo posterior deberá entrar a un proceso de revisión, para una futura aprobación por parte del ente pertinente dentro del GADM.

CONCLUSIONES

- El primer paso para tener un buen sistema de seguridad de la información es tener una buena gestión de la red, cosa que en la infraestructura física y lógica de la red LAN del GADM del cantón Mira no se ha logrado aún, si bien esto implica de mucho esfuerzo y por ende de una asignación presupuestaria, es necesario reestructurar la LAN del GADM-Mira desde sus bases, es decir desde su sistema de cableado estructurado; tomando en cuenta estudios de diseño que se basen en normas o estándares técnicos, y de ser necesario, aplicar las medidas correctivas necesarias en sus controles operacionales para mantener un porcentaje aceptable de eficiencia del sistema de seguridad en el tiempo.
- Si bien aún no se ha desarrollado la versión en español del Manual de Metodologías para Pruebas de Seguridad de Fuente Abierta (OSSTMM) versión 3, para este caso fue necesaria la contratación de un traductor certificado, quien se encargó de verificar que la traducción al español de este manual se apegue lo más posible a la realidad del idioma que se maneja en la región; además cabe recalcar que este manual divide la seguridad en 5 subgrupos: humano, de la infraestructura física, de comunicaciones inalámbricas, de telecomunicaciones y de redes de datos, es por ello que en la redacción del informe final, se deben hacer las debidas recomendaciones por separado, para cada subgrupo, dependiendo de dónde se encuentre la debilidad de cada uno.
- La aplicabilidad de la metodología OSSTMM versión 3 permite conocer resultados puntuales sobre los canales en los que se requiere una mayor atención, para poder dar una solución oportuna a ciertas vulnerabilidades que pueden darse dentro del entorno organizacional, ya sea por limitaciones financieras, humanas, de procedimientos o estratégicas, normativas; así como también la mala aplicación de los controles de seguridad que pueden verse subutilizados.
- A pesar de que COBIT versión 5 para la Seguridad de la Información es un estándar aplicable a entornos de negocio, se lo adaptó a la naturaleza pública del Gobierno Autónomo Descentralizado Municipal del Cantón Mira, ya que los trece capítulos que se plantean en el estándar para la implantación de un Manual de Políticas de Seguridad cubren los puntos más importantes de cualquier institución, tales como: la información que genera el talento humano, los activos, el entorno donde se genera la información y todo lo que engloba las comunicaciones.

- El hecho de que la metodología separe en canales individuales las pruebas que se deben realizar es muy beneficioso, no solo para el auditor; sino también para la institución ya que esto permite conocer a ciencia cierta en que parte de la infraestructura del sistema de seguridad de la red se encuentra un mayor número de vulnerabilidades y así poder aplicar los métodos correctivos necesarios en el canal que lo necesite.
- El canal en el que se invirtió mayor tiempo fue el canal de redes de datos, esto debido a que fue necesario aplicar en primer lugar, una entrevista al Director de Sistemas del GADM del Cantón Mira, con la finalidad de tener un punto de partida, con información relevante sobre dicho canal; y en segundo lugar porque fue necesario ejecutar varias aplicaciones del software de auditoría (Kali-Linux), para poder obtener la mayor cantidad de información posible los equipos de comunicaciones que conforman la red de datos de la Institución.
- Con el presente caso de estudio, se deja sentado un precedente de la actuación normativa que debería adoptar el GADM-Mira en caso de que se presente algún tipo de delito informático, ya que si bien aún no se han suscitado dentro de la Institución casos que hayan llegado a instancias mayores, no se puede asegurar a ciencia cierta que ésta se encuentre exenta de este tipo de delitos a futuro.
- El caso de estudio, puede servir de base para futuros procesos evaluativos de los mecanismos de seguridad del GADM-Mira, y así proveer de herramientas de valoración estadística, donde se puedan comprobar las mejoras o deficiencias que se van produciendo en el tiempo.
- El Manual de Políticas de Seguridad de la Información que se creó luego de finalizado el estudio, servirá como un componente de mejoramiento que dará en cierta medida un valor agregado a los mecanismos de seguridad del GADM-Mira, ya que en él se hacen recomendaciones de varias de las deficiencias de los controles de seguridad operacionales encontrados.
- Al finalizar el trabajo investigativo se recogen varias experiencias personales que servirán de apoyo para tomar decisiones en la vida profesional, ya que con este proceso se enriquece la experticia para futuros escenarios en los que se deban aplicar los conocimientos técnicos adquiridos en casos aplicativos de estudio futuros.

RECOMENDACIONES

- Dentro del ámbito de las auditorias informáticas existen un sinnúmero de metodologías que se pueden tomar como referencia para obtener resultados sobre la seguridad de la información que mantiene una determinada organización, en tal virtud se debe hacer un análisis técnico de la que brinde mejores prestaciones para realizar una medición evaluativa no sólo cualitativa, sino también cuantitativa de los mecanismos de seguridad vigentes en la Institución.
- La persona encargada del Área de Sistemas del GADM-Mira, deberá acoger las medidas interventiva y correctivas dispuestas en el informe final de la auditoría y tratar de adoptarlas en el tiempo en la medida que sea posible, ya que de ello dependerá la seguridad de la información que se maneje en la Institución y de cierta manera en el cumplimiento de los decretos presidenciales estipulados por la actual Administración Central Gubernamental sobre la implementación del gobierno electrónico.
- Es recomendable, que por parte del Área de Sistemas del GADM del Cantón Mira se haga una petición formal al Departamento Financiero para la adquisición de equipos de red que presten mejores características para la administración de la red, entre los más imperantes: un router de borde, switches administrables, equipos de alimentación eléctrica de respaldo o UPS, un firewall; esto con la finalidad de realizar las configuraciones necesarias que brinden mejores prestaciones a la red municipal.
- Si bien la metodología no hace referencia a pruebas que se deban realizar para medir el nivel de eficiencia del sistema eléctrico de una Institución, es recomendable realizar una evaluación exhaustiva del sistema eléctrico del GADM-Mira, ya que en varias instancias, tales como el cuarto de telecomunicaciones se pudo observar que las acometidas eléctricas se encuentran en condiciones de inoperatividad y no cumplen con las especificaciones técnicas pertinentes, por lo que podrían presentarse posibles descargas y problemas con los equipos de comunicación.
- Sería factible que en base al Orgánico Estructural por Procesos del GADM-Mira vigente a la fecha, se haga una modificación al Área de Sistemas, para que se cuente con varias instancias departamentales que permitan manejar de una manera más eficiente los problemas que se suscitan con los diferentes usuarios tanto de

planta interna como de planta externa, y así designar de una manera más ordenada las tareas específicas de cada instancia departamental en favor del desarrollo de las Tecnologías de la Información y Comunicación.

- Se debería adoptar como una política regular del GADM-Mira, aplicar constantemente capacitaciones continuas con el talento humano que posee poco conocimiento en temas de seguridad de la información, ya que las personas se consideran uno de los elementos más vulnerables de las redes de comunicaciones por la facilidad que éstos presentan para la extracción de información aplicando técnicas de ingeniería social.

BIBLIOGRAFÍA

Almeida Romo, O. R. (02 de 2011). *Repositorio UTN*. Obtenido de http://repositorio.utn.edu.ec/handle/123456789/539

Álvarez Marañón, G., & Pérez García, P. P. (2000). *Seguridad informática para empresas y particulares.* Madrid, España: McGraw-Hill.

Aranda Vera, A. (2014). Instalación y parametrización del software. (1ª Edición). Andalucia, España: IC Editorial. Obtenido de http://site.ebrary.com/lib/utnortesp/detail.action?docID=11148767

Asamblea Nacional de la República del Ecuador. (21 de 09 de 2009). Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional. Quito, Pichincha, Ecuador. Obtenido de http://www.justicia.gob.ec/wp-content/uploads/2015/05/LEY-ORGANICA-DE-GARANTIAS-JURISDICCIONALES-Y-CONTROL-CONSTITUCIONAL.pdf

Asamblea Nacional de la República del Ecuador. (20 de 04 de 2010). Ley Orgánica de Participación Cuidadana. Quito, Pichincha, Ecuador.

Asamblea Nacional de la República del Ecuador. (10 de 02 de 2014). Código Orgánico Integral Penal. Quito, Pichincha, Ecuador. Obtenido de http://www.asambleanacional.gob.ec/es/system/files/document.pdf

Asamblea Nacional de la República del Ecuador. (18 de 02 de 2015). Ley Organica de Telecomunicaciones. Quito, Pichincha, Ecuador. Obtenido de ley de telecomunicaciones reformada: http://www.arcotel.gob.ec/wp-content/uploads/downloads/2013/07/ley_telecomunicaciones_reformada.pdf

Bellido Quintero, E. (07 de 2014). Equipos de interconexión y servicios de red. (1ª Edición). Andalucía, España: IC Editorial. Obtenido de http://site.ebrary.com/lib/utnortesp/reader.action?docID=11148763#

Boud, D., & Molloy, E. (2015). *El feedback en educación superior y profesional.* Madrid: NARCEA S.A.

Cabello García, J. M. (2000). Operaciones auxiliares con tecnologías de la información y la comunicación. (1ª Edición). Andalucía, España: IC Editorial. Obtenido de http://site.ebrary.com/lib/utnortesp/detail.action?docID=10721635

Chicano Tejada, E. (2014). *Auditoría de seguridad informática.* Andalucía: IC Editorial.

Congreso Nacinoal del Ecuador . (17 de 04 de 2002). Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos. Quito, Pichincha , Ecuador. Obtenido de http://www.derechoecuador.com/productos/producto/catalogo/registros-oficiales/2002/abril/code/17544/registro-oficial-17-de-abril-del-2002-suplemento

Congreso Nacional del Ecuador. (18 de 05 de 2004). Ley Organica de Transparencia y Acceso a la Información Pública. Quito, Pichincha, Ecuador. Obtenido de http://www.seguridad.gob.ec/wp-content/uploads/downloads/2015/04/ley_organica_de_transparencia_y_acceso_a_la_informacion_publica.pdf

Congreso Nacional del Ecuador. (28 de 12 de 2006). Ley de Propiedad Intelectual. Quito, Pichincha, Ecuador. Obtenido de https://www.correosdelecuador.gob.ec/wp-content/uploads/downloads/2015/05/LEY_DE_PROPIEDAD_INTELECTUAL.pdf

Costas Santos, J. (2010). *Seguridad Informática.* Madrid: Ra-Ma Editorial.

Endara Néjer, F. G. (Febrero de 2011). *http://repositorio.utn.edu.ec.* Obtenido de http://repositorio.utn.edu.ec/bitstream/123456789/542/1/04%20ISC%20160%20TESIS.pdf

Escrivá, G., Romero, R., Ramada, D., & Onrabia, R. (2013). *Seguridad Informática.* Madrid: Macmillan Iberia.

Estupiñán Gaitán, R. (2007). *Pruebas selectivas en auditoría.* Bogotá: Ecoe Ediciones.

Fernández López, F. (2015). *Sistemas de archivos y clasificación de documentos.* San Millán: Editorial Tutor Formación .

GAD-Mira. (2014). *Alcaldía Mira*. Obtenido de Reglamento Orgánico Funcional por Procesos : http://www.mira.gob.ec/index.php?option=com_k2&view=item&id=159:literalk&Itemid=291

Galdámez, P. (2013). Seguridad Informática. *Actualidad TIC*, 4-7.

García, A., & Alegre, M. d. (2011). *Seguridad Informática.* Madrid: Paraninfo.

Gómez, Á. (2011). *Enciclopedia de la seguridad informática.* México: Alfaomega Ra-Ma.

González Manzano, L., De Fuentes, J. M., & Romero de Tejada, G. (2014). Sistemas seguros de acceso y transmisión de datos. (1ª Edición). Andalucía, España: IC Editorial. Obtenido de http://site.ebrary.com/lib/utnortesp/reader.action?docID=11126449#

Gutierrez, A. (06 de Septiembre de 2015). *about en español*. Obtenido de WEP o WPA para proteger tu red Wi-Fi: http://windowsespanol.about.com/od/RedesYDispositivos/a/Wep-O-Wpa-Para-Proteger-Tu-Red-Wi-Fi.htm

Herzog, P. (2010). *OSSTMM 3. Manual de la Metodología Abierta de Testeo de Seguridad.* New York: ISECOM.

ISACA. (2012). *COBIT 5 para Seguridad de la Información.* Madrid: ISACA Framework.

Jaramillo Remache, D. D. (10 de 07 de 2014). *repositorio.utn.edu.ec.* Obtenido de http://repositorio.utn.edu.ec/bitstream/123456789/3774/1/04%20RED%20034%20TESIS.pdf

Kats, M. (2013). *Redes y Seguridad.* Buenos Aires: Alfaomega.

López López, E. (23 de Marzo de 2014). *Seguridad Informática*. Obtenido de http://redyseguridad.fi-p.unam.mx/proyectos/seguridad

López Santoyo, R. (2015). *Propuesta de implementación de una metodología de seguridad infromática*. Madrid.

Merino, C., & Cañizares, R. (2013). *Implantación de un sistema de gestión de seguridad de la información según ISO.* Madrid: FC.

Molina Robles, F. J. (2014). Redes locales. Madrid, España: RA-MA Editorial. Obtenido de http://site.ebrary.com/lib/utnortesp/detail.action?docID=11038603

Opentesting. (31 de Diciembre de 2010). *Liberado OSSTMM 3*. Obtenido de https://opentesting.wordpress.com/2010/12/31/liberado-osstmm-3/

Padilla Ulloa, A., & otros, y. (2013). *Mira-Balcón de los Andes*. Obtenido de http://www.mira.ec

Prandini, P., & Szuster, R. (2012). *SEGURINFO*. Obtenido de www.segurinfo.org: http://www.isaca.org/Knowledge-Center/cobit/Documents/COBIT5-and-InfoSec-Spanish.ppt.

Racciati, H. (12 de Mayo de 2013). Tiempos de Cambio: OSSTMM 3 - Una Introducción. *OSSTMM 3*, 29-30.

Ramos Varón, A., Barbero Muñoz , C., Martínez Sanchez, R., García Moreno, Á., & Gonzáles Nava, J. (2015). *Hacking y seguridad de páginas web.* Bogotá: Ediciones de la U.

Secretaría Nacional de la Administración Pública. (31 de 11 de 2016). PLAN NACIONAL DE GOBIERNO ELECTRÓNICO. Quito, Pichincha, Ecuador.

SECRETARÍA NACIONAL DE LA ADMINISTRACIÓN PÚBLICA. (31 de 11 de 2016). Plan Nacional de Gobierno Electrónico. Quito, Pichincha, Ecuador.

SECRETARÍA NACIONAL DE LA ADMINISTRACIÓN PÚBLICA. (31 de 11 de 2016). Plan Nacional de Gobierno Electrónico. Quito, Pichincha, Ecuador.

Stallings, W. (2 004). *FUNDAMENTOS DE SEGURIDAD EN REDES. APLICACIONES Y ESTÁNDARES* (Segunda edición ed.). Madrid: PEARSON EDUCACIÓN S.A.

TELECOMUNICACIONES, U. I. (22 de 03 de 1991). ARQUITECTURA DE SEGURIDAD DE LA INTERCONEXIÓN DE SISTEMAS ABIERTOS PARA APLICACIONES DEL CCITT. *Recomendación X.800*. Ginebra: CCITT.

Toth, G. A. (31 de 03 de 2014). *Implementación de la guía NIST SP800-30 mediante la utilización de OSSTMM*. Recuperado el 10 de 01 de 2016, de http://tesis-toth.com.ar

GLOSARIO DE TÉRMINOS

- **Acceso:** privilegio de una persona para utilizar un objeto o infraestructura.
- **Acceso Remoto: c**onexión entre dos dispositivos de cómputo ubicados en diferentes lugares físicos por medio de líneas de comunicación, ya sean telefónicas o por medio de redes de área amplia, que permiten el acceso de aplicaciones e información de la red. Este tipo de acceso normalmente viene acompañado de un sistema robusto de autenticación.
- **Activo**: cualquier componente (humano, tecnológico, software, documental o de infraestructura) que soporta uno o más procesos y, en consecuencia, debe ser protegido.
- **Acuerdo de Confidencialidad:** documento en los que los funcionarios de una entidad o los provistos por terceras partes manifiestan su voluntad de mantener la confidencialidad de la información de dicha institución, comprometiéndose a no divulgar, usar o explotar la información confidencial a la que tengan acceso en virtud de la labor que desarrollan dentro de la misma.
- **Acuerdo de No Divulgación:** acuerdo legal que evita la difusión de información más allá de los propósitos informativos, entre las partes que mantienen dicho acuerdo de no divulgación.
- **Alcance:** el ambiente operativo donde producen las interacciones con los activos.
- **Alineamiento: e**stado en el que los elementos facilitadores del gobierno y de la gestión de TI de la institución contribuyen a las metas y las estrategias de la misma.
- **Ámbito**: la descripción de lo que está permitido en un test de seguridad.
- **Amenaza:** circunstancia que tiene el potencial de causar algún daño, pérdida o difusión no autorizada de información.
- **Anomalía:** elemento desconocido que no se encuentra dentro de las operaciones normales. Es una de las categorías en las que se dividen las limitaciones.
- **Antivirus:** programa que busca y eventualmente elimina los virus informáticos que pueden haber infectado un disco rígido, o cualquier sistema de almacenamiento electrónico de información.
- **Ataque**: actividades encaminadas a quebrantar las protecciones establecidas de un activo específico, con la finalidad de obtener acceso a un archivo y lograr afectarlo.
- **Auditoría de Seguridad**: inspección manual con privilegios de acceso del sistema operativo y de los programas de aplicación de un sistema. En los Estados Unidos

y Canadá, “Auditor” representa un vocablo y una profesión oficiales, solamente utilizado por profesionales autorizados. Sin embargo, en otros países, una “auditoría de seguridad” es un término de uso corriente que hace referencia a Test de Intrusión o test de seguridad.

- **Autenticación:** procedimiento de comprobación de la identidad de un usuario o recurso tecnológico al tratar de acceder a un recurso de procesamiento o sistema de información.
- **Bases de Datos:** conjunto de datos interrelacionados y un conjunto de programas para procesarlos. Una recopilación de datos estructurados y organizados de una manera disciplinada para que el acceso a la información de interés sea rápida.
- **Buenas Prácticas:** actividad o proceso probado que ha sido usado con éxito por múltiples empresas y ha demostrado que produce resultados fiables.
- **Caja Blanca**: el testeador posee conocimiento previo integral de los elementos o del entorno a ser testeados.
- **Caja Gris:** el testeador tiene un conocimiento previo de los elementos o del entorno a testear.
- **Caja Negra**: el testeador no tiene conocimiento previo de los elementos o del entorno a testear.
- **Canales:** son todos los medios por los cuales se pueden llevar a cabo las interacci ones. Existen cinco canales definidos por OSSTMM: humano, físico, medios inalámbricos, telecomunicaciones y redes de datos.
- **Certificación:** evaluación independiente que declara que un producto, persona, proceso o sistema de gestión cumplen con requerimientos específicos.
- **COBIT:** (Control Objectives for Information Systems and related Technology) Objetivos de Control para la Información y Tecnologías Relacionadas. Es un modelo para auditar la gestión y control de los sistemas de información y tecnología, orientado a todos los sectores de una organización. El COBIT es un modelo de evaluación y monitoreo que enfatiza en el control de negocios y la seguridad IT y que abarca controles específicos de IT desde una perspectiva de negocios.
- **Confianza:** interacción que no requiere autenticación entre dos elementos dentro del alcance. Es uno de los tres elementos que componen la porosidad.
- **Contraseña:** serie secreta de caracteres que permite a un usuario tener acceso a un archivo, a un ordenador, o a un programa.

- **Controles**: garantía de que los activos físicos y de información, así como los propios canales están protegidos de los distintos tipos de interacciones no válidos según lo definido por el canal.
- **Cortafuegos**: herramientas de software o hardware que impone una Lista de Control de Acceso en un sistema o red.
- **Criptografía:** disciplina que agrupa los principios, medios y métodos para la transformación de datos con el fin de ocultar el contenido de su información, establecer su autenticidad, prevenir su modificación no detectada, prevenir su repudio, y/o prevenir su uso no autorizado.
- **Debilidad: f**alla que reduce o anula los efectos de los controles de interacción.
- **Disponibilidad:** propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.
- **Estándares de seguridad:** son productos, procedimientos y métricas aprobadas, que definen en detalle como las políticas de seguridad serán implementadas para un ambiente en particular, teniendo en cuenta las fortalezas y debilidades de las características de seguridad disponibles. Deben estar reflejadas en un documento que describe la implantación de una guía para un componente específico de hardware, software o infraestructura.
- **Exposición:** acción injustificada que permite dejas visible, ya sea de forma directa o indirecta a un activo.
- **Gobierno de la institución:** conjunto de responsabilidades y prácticas ejercidas por el Consejo Administrativo y los gestores ejecutivos con el objetivo de dotar de dirección estratégica, asegurando que los objetivos son conseguidos, verificando que el riesgo es gestionado de forma apropiada y verificando que los recursos de la empresa son usados de forma responsable. También podría referirse a una visión de gobierno que ve el conjunto de la institución; la visión más alta del gobierno con la que todos los demás deben alinearse.
- **Hacker:** persona inteligente que tiene una curiosidad natural, le gusta aprender como las cosas funcionan, y le interesa conocer técnicas de evasión o abusar de procesos para ver qué sucede.
- **Hacking ético:** conjunto de actividades para ingresar a las redes de datos y voz de la institución con el objeto de lograr un alto grado de penetración en los sistemas, de forma controlada, sin ninguna intensión maliciosa, ni delictiva y sin generar daños en los sistemas o redes, con el propósito de mostrar el nivel efectivo de

riesgo a lo cual está expuesta la información, y proponer eventuales acciones correctivas para mejorar el nivel de seguridad.

- **Información**: elemento fundamental que manejan los ordenadores en forma de datos binarios.
- **Ingeniería Social:** técnicas y métodos utilizados para engañar a las personas y conseguir información valiéndose de su ignorancia e inocencia.
- **Integridad:** propiedad de salvaguardar la exactitud y el estado completo de los activos.
- **IP - Internet Protocol:** parte de la familia de protocolos TCP/IP, que describe el software que supervisa las direcciones de nodo internet, encamina mensajes salientes y reconoce los mensajes entrantes.
- **ISACA:** (Information Systems Audit and Control Association) Asociación de Auditoría y Control de Sistemas de Información. Asociación internacional que apoya y patrocina el desarrollo de metodologías y certificaciones para la realización de actividades auditoría y control en sistemas de información.
- **ISECOM:** (Institute for Security and Open Methodologies) Instituto de Seguridad y Metodologías Abiertas. Organización sin fines de lucro dedicada al desarrollo de metodologías de libre utilización para la verificación de la seguridad, la programación segura, la verificación de software y la concientización en seguridad.
- **Kali Linux:** es la nueva generación de la conocida distribución Linux BackTrack, la cual se utiliza para realizar Auditorías de Seguridad y Pruebas de Penetración.
- **Limitaciones: s**on los inconvenientes que presentan los controles para mantener la protección de los activos ante las amenazas.
- **Metodología de prueba de penetración:** define un conjunto de reglas, prácticas, procedimientos y métodos a seguir e implementar durante la realización de cualquier programa de auditoría en seguridad de la información.
- **Objetivo:** ámbito que se está atacando, que se compone del activo y cualquier protección del activo pueda tener.
- **Operaciones:** son la falta de seguridad hay que tener para ser interactivo, útil, público, abierto, o disponible.
- **OSSTMM:** metodología creada por ISECOM, que busca establecer un método científico para el análisis de la seguridad.
- **PBX**: representa el Conmutador Telefónico, y es el servidor central que administra las líneas telefónicas en una organización.

- **Políticas:** toda intención y directriz expresada formalmente por una dirección ejecutiva.
- **Porosidad:** todos los puntos interactivos, operaciones, que se clasifican como visibilidad, acceso, o de confianza.
- **Preocupación:** falla que reduce los efectos de los controles de proceso.
- **Prueba de penetración:** proceso utilizado para realizar una evaluación o una auditoría de seguridad de alto nivel.
- **RAV:** El rav es una medición escala de una superficie de ataque, la cantidad de interacciones no controlados con un objetivo, que se calcula por el equilibrio cuantitativo entre porosidad, limitaciones y controles.
- **Red informática:** conjunto de enlaces de comunicaciones dispuestos de manera que es posible el envío de mensajes mediante su paso a través de muchos de aquéllos, con el fin de comunicar a un emisor y un receptor.
- **Seguridad perfecta:** balance exacto de la seguridad y los controles con operaciones y limitaciones.
- **Superficie de ataque:** falta de separaciones específicas y controles funcionales que existen para ese vector.
- **Sniffer**: también conocido como paquete analizador, analizador de red o analizador de protocolo. Software o hardware que puede interceptar y registrar el tráfico que pasa por una red digital.
- **UPS:** (Uninterruptible Power Supply), también conocido por sus siglas en español SAI (Sistema de Alimentación Ininterrumpida). Son dispositivos que tras un corte de suministro eléctrico proveen ésta a los equipos del sistema informático, además, proporciona seguridad ante subidas y bajadas de tensión en la red.
- **Usuario**: conjunto de permisos dispositivos o recursos a los cuales se tiene acceso. Un usuario puede ser tanto una persona como una máquina, un programa, etc.
- **Vector:** dirección de una interacción.
- **Vector de ataque:** sub-meta de un vector creado con el fin de acercarse a las pruebas de seguridad de un ámbito complejo de una manera organizada. Se basa en el divide y vencerás paradigma de diseño algoritmo que consiste en descomponer recursivamente un problema en dos o más sub-problemas de la misma (o afines) tipo, hasta que éstos se vuelven lo suficientemente simple como para ser resuelto directamente.
- **Visibilidad:** representa a los objetivos observables dentro del alcance.

- **VPN:** *(Virtual Private Network)* Red Privada Virtual, se utiliza para interconectar varias redes locales utilizando una red de área extensa como Internet. Viene de la existencia de una comunicación virtual entre las redes que conecta. Esto quiere decir que no existe realmente una conexión directa entre ellas, sino que está simulada.

ACRÓNIMOS

- **ANSI:** *(American National Standards Institute)* Instituto Nacional Estadounidense de Estándares
- **AP:** *(Access Point)* Punto de Acceso
- **ARP**: *(Address Resolution Protocol)* Protocolo de Resolución de Direcciones
- **BGP**: *(Border Gateway Protocol)* Protocolo de Gateway de Frontera
- **CD**: *(Compact Disc)* Disco Compacto
- **CCMP:** *(Counter Mode with Cipher Block Chaining Message Authentication Code Protocol)*
- **COIP**: Código Orgánico Integral Penal
- **COBIT:** *(Control Objectives for Information Systems and related Technology)* Objetivos de Control para la Información y Tecnologías Relacionadas.
- **CPU:** *(Central Processing Unit)* Unidad Central de Procesamiento
- **DHCP:** *(Dynamic Host Configuration Protocol)* Protocolo de Configuración Dinámica de Host.
- **DMZ: (***demilitarized zone***)** Zona Desmilitarizada
- **DNS:** *(Domain Name System)* Sistema de Nombres de Dominio
- **DoS:** *(Denial of Service)* Denegación de Servicio
- **DVD:** *(*Digital Versatile Disc) Disco Versátil Digital
- **DVR:** *(Digital Video Recorder)* Grabador de Video Digital
- **EIA:** *(Energy Information Administration)* Administración de Información Energética de Estados Unidos
- **FTP:** *(File Transfer Protocol)* Protocolo de Transferencia de Archivos
- **FRS:** Funcionalidad, Seguridad y Rapidez
- **GADM:** Gobierno Autónomo Descentralizado Municipal
- **HTTP:** *(Hypertext Transfer Protocol)* Protocolo de Transferencia de Hipertexto
- **HTTPS:** *(Hypertext Transfer Protocol Secure)* Protocolo Seguro de Transferencia de Hipertexto
- **ICMP:** *(Internet Control Message Protocol)* Protocolo de Mensajes de Control de Internet
- **IEEE:** *(Institute of Electrical and Electronics Engineers)* Instituto de Ingeniería Eléctrica y Electrónica
- **IP:** (*Internet Protocol)* Protocolo de Internet

- **ISF:** (*Information Security Forum)* Foro de Seguridad de la Información
- **ISACA:** *(Information Systems Audit and Control Association)* Asociación de Auditoría y Control de Sistemas de Información
- **ISDN:** *(Integrated Services Digital Network)* Red Digital de Servicios Integrados
- **ISECOM:** *(Institute for Security and Open Methodologies)* Instituto para la Seguridad y Metodologías Abiertas
- **ISO:** *(International Organization for Standardization)* Organización Internacional de Normalización
- **ITIL:** (*Information Technology Infrastructure Library)* Biblioteca de Infraestructura de Tecnologías de Información
- **LAN:** *(Local Area Network)* Red de Área Local
- **MAC:** *(Media Access Control)* Control de Acceso al Medio
- **MPLS:** *(Multiprotocol Label Switching)* Conmutación Multi-Protocolo mediante Etiquetas
- **NFS:** *(Network File System)* Sistema de Archivos de Red
- **NIST:** (*National Institute of Standards and Technology)* Instituto Nacional de Estándares y Tecnología
- **NMAP:** *(Network Mapper)* Mapeador de Redes
- **OIE:** Organización Internacional para la Estandarización
- **OML:** *(Open Methodology License)* Metodología de Licencia Abierta
- **ONG:** Organizaciones No Gubernamentales
- **OSI:** *(Open System Interconnection)* Interconexión de Sistemas Abiertos
- **OSPF:** *(Open Shortest Path First)* Camino más Corto Primero
- **OSSTMM:** *(Open Source Security Testing Manual Methodology)* Manual de la Metodología Abierta del Testeo de Seguridad.
- **PBX:** *(Private Branch Exchange)* Central Telefónica Privada
- **PKI:** *(Public Key Infrastructure)* Infraestructura de Clave Pública
- **RAID:** *(Redundant Array of Inexpensive Disks)* Conjunto Redundante de Discos Independientes
- **RFID:** *(Radio Frequency IDentification)* Identificación por Radiofrecuencia
- **RIP:** *(Routing Information Protocol)* Protocolo de Información de Encaminamiento
- **SNMP:** *(Simple Network Management Protocol)* Protocolo Simple de Administración de Redes

- **SQL:** (*Structured Query Language*) Lenguaje de Consulta Estructurado
- **SSID:** *(Service Set Identifier)* Nombre de la Red Inalámbrica
- **STAR:** *(Security Test Auditing Report)* Informe de Auditoria de Pruebas de Seguridad
- **TCP:** (*Transmission Control Protocol*) Protocolo de Control de Transmisión
- **TIA:** *(Telecommunications Industry Association)* Asociación de Industrias de Telecomunicaciones
- **TIC:** Tecnologías de la Información y Comunicación
- **TKIP:** *(Temporal Key Integrity Protocol)* Protocolo de Integridad de Clave Temporal
- **UDP:** (*User Datagram Protocol*) Protocolo de Datagrama de Usuario
- **UPS:** *(Uninterruptible Power Supply)* Sistema de Alimentación Ininterrumpida
- **UR:** Unidades de Rack
- **USB:** *(Universal Serial Bus)* Bus Universal en Serie
- **UTP:** *(Unshielded Twisted Pair)* Par Trenzados Sin blindar
- **VoIP:** *(Voice over Internet Protocol)* Voz sobre el Protocolo de Internet
- **VPN:** *(Virtual Private Network)* Red Privada Virtual
- **WEP:** *(Wired Equivalent Privacy)* Privacidad Equivalente a Cableado
- **Wi-Fi:** *(Wireless Fidelity)* Fidelidad Inalámbrica
- **WPA:** *(Wi-Fi Protected Access)* Acceso Wi-Fi Protegido
- **XSS:** *(Cross Site Scripting*) Secuencias de Órdenes en Sitios Cruzados

ANEXOS

Anexo 1. - Datasheet Del Switch De Core (tl-sg1024D)

TP-LINK

Datasheet

8/16/24-Port Gigabit Switch

TL-SG1008 / TL-SG1016D / TL-SG1024D

Overview

The TL-SG1008/TL-SG1016D/TL-SG1024D Gigabit Ethernet Switch provides you with a high-performance, low-cost, easy-to-use, seamless and standard upgrade to improve old network to 1000Mbps network. All 8/16/24 ports support auto MDI/MDIX, no need to worry about the cable type, simply plug and play. Moreover, with the innovative energy-efficient technology, the TL-SG1008/TL-SG1016D/TL-SG1024D can save up to 75%/40%/40%* of the power consumption and 80% of the packaging material can be recycled, making it an eco-friendly solution for your business network.

www.tp-link.com

TP-LINK

Datasheet

Green Technology

- Saving power 75%/40%/40%
- Recyclable packaging materia

High Performance

- IEEE 802.3x flow control
- Non-blocking switching architecture
- 16/32/48 Gbps Switching Capacity
- Store and forward
- Auto-MDI/MDIX
- Auto-negotiation
- MAC address auto-learning and auto-aging
- 10KB Jumbo frame

Easy to use

- Plug and Play design
- Quiet/Fanless design

24/7 Global technical support

- Details:http://www.tp-link.com/support/Localesupport.asp
- German/Austrian/Swiss users are not included

8/16/24-Port Gigabit Switch

TL-SG1008 / TL-SG1016D / TL-SG1024D

TP-LINK Green Technology

This new generation TL-SG1008/TL-SG1016D/TL-SG1024D Gigabit Switch features the latest innovative energy-efficient technologies that can greatly expand your network capacity with much less power. It automatically adjusts power consumption according to the link status and cable length to limit the carbon footprint of your network. It also complies with the EU'S RoHS, prohibiting the use of certain hazardous materials. Besides, 80% of the packaging material can be recycled.

High Performance

All 8/16/24 ports are Gigabit RJ-45 ports which can provide large file transferring and also be compatible with 10Mbps and 100Mbps Ethernet devices. Featuring non-blocking switching architecture, TL-SG1008/TL-SG1016D/TL-SG1024D forwards and filters packets at full wire-speed for maximum throughput. With 10KB Jumbo frame, the performance of large files transfers is improved significantly. And IEEE 802.3x flow control for Full Duplex mode and backpressure for Half Duplex mode alleviate the traffic congestion and make The TL-SG1008/TL-SG1016D/TL-SG1024D work reliably. It's a perfect choice to update your network to Gigabit while protecting your previous investment properly.

Easy to Use

The auto features of this gigabit switch make installation plug and play and hassle-free. No configuring is required. Auto MDI/MDIX eliminates the need for crossover cables. Auto-negotiation on each port senses the link speed of a network device (10, 100, or 1000 Mbps) and intelligently adjusts for compatibility and optimal performance.

TP-LINK®

Datasheet

Specifications:

Product Picture			
Model	TL-SG1008	TL-SG1016D	TL-SG1024D
Standards	IEEE 802.3, IEEE 802.3u, IEEE 802.3x	IEEE 802.3, IEEE 802.3u, IEEE 802.3x	IEEE 802.3, IEEE 802.3u, IEEE 802.3x
Network Ports	8*10/100/1000Mbps RJ45 ports	16*10/100/1000Mbps RJ45 ports	24*10/100/1000Mbps RJ45 ports
Auto Negotiation	YES	YES	YES
Auto MDI/MDIX	YES	YES	YES
Systems	Windows 2000/XP/Vista/7 Linux/MAC OS	Windows 2000/XP/Vista/7 Linux/MAC OS	Windows 2000/XP/Vista/7 Linux/MAC OS
Forwarding Mode	Store and Forward	Store and Forward	Store and Forward
Switch Capacity	16 Gbps	32 Gbps	48 Gbps
MAC Address Table	8 K	8 K	8 K
Jumbo Frame	10 KB	10 KB	10 KB
Flow Conrol	YES	YES	YES
Fanless	YES	YES	YES
Green Technology	YES	YES	YES
Power Saving	Up to 75%	Up to 40%	Up to 40%
LED	Power、1000Mbps、Link/Act	Power、1000Mbps、Link/Act	Power、1000Mbps、Link/Act
Dimensions	294*180*44 mm	294*180*44 mm	294*180*44 mm
Operating Temperature	0°C~40°C (32°F~104°F)	0°C~40°C (32°F~104°F)	0°C~40°C (32°F~104°F)
Storage Temperature	-40°C~70°C (-40°F~158°F)	-40°C~70°C (-40°F~158°F)	-40°C~70°C (-40°F~158°F)
Operating Humidity	10%~90% non-condensing	10%~90% non-condensing	10%~90% non-condensing
Storage Humidity	5%~90% non-condensing	5%~90% non-condensing	5%~90% non-condensing
Ordering Information	8-Port Gigabit switch	16-Port Gigabit switch	24-Port Gigabit switch

* Maximum power savings when compared to a TP-LINK conventional switch, the real saving rate may vary based on the usage condition.

Anexo 2.- Datasheet Del Switch De Distribución (d-link des-1016d)

D-Link

10/100Mbps Unmanaged Switch

DES-1016D

The DES-1016D switch provides 16 auto-sensing 10/100Mbps ports in a desktop box. The switch allows mix and match of Ethernet and Fast Ethernet in full- and half-duplex modes.

16-Port 10/100Mbps Switch for SOHO/Workgroup

The DES-1016D is an unmanaged 10/100Mbps switch designed to enhance workgroup performance while providing a high level of flexibility. Powerful yet easy to use, this device allows users to simply plug any port to either a 10Mbps or 100Mbps network to multiply bandwidths, boost response time and satisfy heavy load demands.

16 Auto-sensing 10/100Mbps Ports

The switch comes with 16 10/100Mbps ports, allowing a small workgroup to flexibly integrate to Ethernet and Fast Ethernet. These intelligent ports detect the network speed and auto-negotiate between 100BASE-TX and 10BASE-T, as well as between full and half-duplex.

Flow Control for Secure Transmission

All ports support flow control. This function minimizes dropped packets by sending out collision signals when the port's receiving buffer is full.

Auto-negotiation of MDI/MDIX Cross Over

All ports support auto-negotiation of MDI/MDIX cross over. This eliminates the need for cross over cables or uplink ports. Any port can simply plug to a server, a hub or aswitch, using the usual straight-through twisted-pair cable.

Plug-and-Play

With 16 plug-and-play ports, the switch is a perfect choice for workgroups to upgrade performance in a client/server environment. The ports can be connected to servers in full-duplex, or hubs in half-duplex.

Direct Connection to Workstations

With low-cost connection per-port, the switch can be set up for direct connection from the PCs. This relieves data bottleneck by giving each workstation a dedicated bandwidth on the network.

Features

- *16 10/100Mbps ports*
- *Auto MDI/MDIX for each port*
- *Full/half-duplex support for each port*
- *Flow control for protection against data loss for each port*
- *Uto-learning of network configuration*
- *Secure store-and-forward switching scheme*
- *Per-port auto-correction of reverse twisted-pair polarity*
- *Compact desktop size*

DES-1016D

Technical Specifications

10/100Mbps Unmanaged Switch

General

Standards
- IEEE 802.3 10BASE-T Ethernet
- IEEE 802.3u 100BASE-TX Fast Ethernet
- ANSI/IEEE 802.3 NWay auto-negotiation

Protocol
CSMA/CD

Data Transfer Rates
- Ethernet:
  10Mbps (half-duplex)
  20Mbps (full-duplex)
- Fast Ethernet:
  100Mbps (half-duplex)
  200Mbps (full-duplex)

Topology
Star

Network Cables
- 10BASE-T:
  UTP Cat. 3, 4, 5 (100 m)
  EIA/TIA-568 100-ohm STP (100 m)
- 100BASE-TX:
  UTP Cat. 5 (100 m)
  EIA/TIA-568B 100-ohm STP (100 m)

Number of Ports
10/100Mbps port x 16

Media Interface Exchange
Auto MDI-II/MDI-X for each port

Twisted-pair Rx Reverse Polarity
Auto-correction for each port

Diagnostic LEDs
Per device:
- Power
Per port:
- Link/Activity
- Full-duplex/Collision
- 100Mbps speed

Performance

Transmission Method
Store-and-forward

Filtering Address Table
8K entries per device

MAC Address Learning
Automatic update

Packet Filtering Rates
- 10BASE-T: 14,880 pps per port (half-duplex)
- 100BASE-TX: 148,810 pps per port (half-duplex)

Packet Forwarding Rates
- 10BASE-T: 14,880 pps per port (half-duplex)
- 100BASE-TX: 148,810 pps per port (half-duplex)

RAM Buffer
4MBits per device

Physical & Environmental

Power Supply
100 - 240 VAC, 50/60 Hz 0.3A
Internal universal power supply

Power Consumption
6 watts (max.)

Ventilation
no DC fan required

Operating Temperature
0° - 40°C

Storage Temperature
-10° - 70°C

Humidity
5% - 90%

Dimensions
280 (W) x 180 (D) x 44 (H) mm

Weight
2.8 kg

Emission (EMI)
- FCC Class A
- CE Class A
- VCCI Class A

Safety
- CUL
- CB

Ordering Information

Ethernet/Fast Ethernet Switch	
DES-1016D	16 10/100Mbps ports

D-Link®

U.S.A.	TEL: 1-949-788-0805	FAX: 1-949-753-7033
Canada	TEL: 1-905-829-5033	FAX: 1-905-829-5095
Europe	TEL: 44-20-8731-5555	FAX: 44-20-8731-5511
U.K.	TEL: 44-20-8731-5555	FAX: 44-20-8731-5511
Germany	TEL: 49-61-96779903	FAX: 49-61-96779930
France	TEL: 33-1-30238688	FAX: 33-1-30238689
Italy	TEL: 39-02-2900-0676	FAX: 39-02-2900-1723
Iberia	TEL: 34-93-4090770	FAX: 34-93-4910795
Sweden	TEL: 46-(8)-564-61900	FAX: 46-(8)-564-61901
Norway	TEL: 47-22-991990	FAX: 47-22-207038
Denmark	TEL: 45-43-969040	FAX: 45-43-424347
Finland	TEL: 358-9-2707-5080	FAX: 358-9-2707-5081
Singapore	TEL: 65-6774-6233	FAX: 65-6774-6322
Australia	TEL: 61-2-9417-7100	FAX: 61-2-9417-1077
Japan	TEL: 81-3-5434-9678	FAX: 81-3-5434-9868
China	TEL: 86-010-8518-2533	FAX: 86-010-8518-2250
India	TEL: 91-22-652-6696	FAX: 91-22-652-8914
Middle East	TEL: 202-2456176	FAX: 202-2456192
South America	TEL: 56-2-232-3185	FAX: 56-2-232-0923
Brazil	TEL: 55-11-3094-2910	FAX: 55-11-3094-2921
South Africa	TEL: 27(0)126652165	FAX: 27(0)126652186
Russia	TEL: 7-095-737-3389	FAX: 7-095-737-3390
Taiwan	TEL: 886-2-2910-2626	FAX: 886-2-2910-1515
D-Link Corp.	TEL: 886-2-2916-1600	FAX: 886-2-2914-6299

RECYCLABLE
Rev. 03 (Aug. 2002)
Printed in Taiwan

Anexo 3. - Datasheet Del Switch De Acceso (d-link des-1008A)

D-Link
Building Networks for People

Product Highlights

High-speed Wired Connection

Connect up to eight Ethernet devices to enjoy a high-speed network connection

Plug and Play

Auto MDI/MDIX simplifies cable connections, allowing for immediate usage and operation

Compact Design

Stylish, compact design can be placed anywhere

DES-1008A

8-Port 10/100 Switch

Features

Connectivity

- Eight Fast Ethernet LAN ports for high-speed wired connections
- IEEE802.3az EEE Power-saving compliance
- D-Link Green Technology features power-saving by link status and by cable length
- Auto-sensing ports automatically detect network connections and adjust accordingly

The DES-1008A 8-Port 10/100 Switch is is an 8-port 10/100 Mbps Fast Ethernet switch that allows you to quickly set up a wired network. Connect the DES-1008A to multiple computers together to share files and folders, or connect it to a router to share an Internet connection.

Auto-sensing 10/100 Ports

The D-Link DES-1008A 8-Port 10/100 Switch uses auto-sensing 10/100 Mbps ports, allowing a small workgroup to flexibly connect to Ethernet and Fast Ethernet devices to create an integrated network. These ports detect the network speed and auto-negotiate between 10BASE-T and 100BASE-TX, as well as between full and half-duplex, allowing you to get the maximum speed possible for each device connected to your network.

Auto MDI/MDIX CrossOver

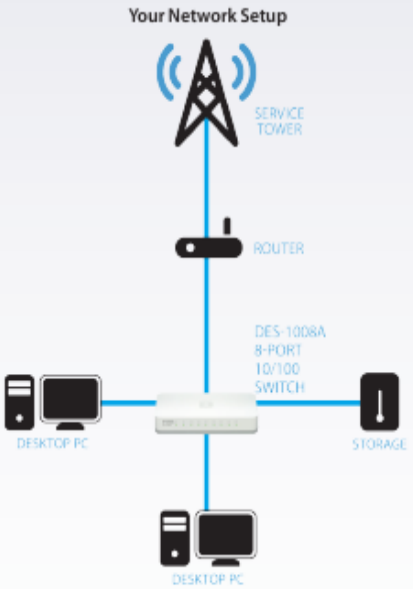
All ports support automatic MDI/MDIX crossover, eliminating the need for crossover cables or uplink ports. Each port can be plugged directly to a server, hub, router, or switch using regular straight-through twisted-pair Ethernet cables.

Flow Control for Secure Transmission

802.3x flow control on each port minimizes dropped packets when the port's receiving buffer is full. This gives you a more reliable connection for all of your connected devices, ensuring smooth and uninterrupted network connection.

D-Link
Building Networks for People

DES-1008A 8-Port 10/100 Switch



Technical Specifications		
General		
Device Interfaces	• Eight 10/100 Fast Ethernet LAN ports	
Functionality		
Advanced Features	• Green Ethernet • 1.6 Gbps switching fabric • Auto MDI/MDIX crossover for all ports • Secure store-and-forward switching scheme • Compliance with IEEE802.3az EEE power saving	• Full/half-duplex for Ethernet/Fast Ethernet speeds • IEEE 802.3x Flow Control • Plug-and-play installation • RoHS compliant • Supports 2048-byte Jumbo Frames
Protocol	• CSMA/CD	

Data Transfer Rates	• Ethernet:
	  • 10 Mbps (half duplex)
	  • 20 Mbps (full duplex)
		• Fast Ethernet:
		  • 100 Mbps (half duplex)
		  • 200 Mbps (full duplex)

Transmission Method	• Store-and-forward	
MAC Address Table	• 2K	
MAC Address Learning	• Automatic Update	
Packet Filtering/Forwarding Rates	• Ethernet: 14,880 pps per port	• Fast Ethernet: 148,800 pps per port
RAM Buffer	• 96 KB per device	
Physical		
LED Indicators	• Per port: Link/Activity	• Per device: Power

DES-1008A 8-Port 10/100 Switch

Media Interface Exchange	• Auto MDI/MDIX adjustment for all ports	
Dimensions	• 141.5 x 78.5 x 23.8 mm (5.57 x 3.09 x 0.94 inches)	
Power	• 5 V/0.55 A Power Adapter	
Heat Dissipation	• Power On (Standby): AC input:2.0472 Btu/h	• Maximum: AC input:7.47228 Btu/h
Power Consumption	• Power On (Standby): DC input: 0.36 watts, AC input: 0.6 watts	• Maximum: DC input: 1.78 watts, AC input: 2.19 watts • Link Up: EEE mode: DC input: 0.75 watts AC input: 1.1. watts
Temperature	• Operating: 0 to 40 °C (32 to 104 °F)	• Storage: -10 to 70 °C (14 to 158 °F)
Humidity	• Operating: 10% to 90% non-condensing	• Storage: 5% to 90% non-condensing
MTBF	• 2,137,319 hours	
Certifications	• CE Class B • FCC Class B • cUL	• CB • VCCI Class B

Order Information

Part Number	*Description*
DES-1008A	8-Port 10/100 Switch

Updated 2013/05/20

D-Link®
Building Networks for People

Anexo 4.- Datasheet De La Central Telefónica (Panasonic kx-tem824)

La mejor solución

para su necesidad de comunicación

El Teléfono es su principal fuente de comunicación - contacte a sus distribuidores, clientes, amigos, miembros de su oficina y sobre todo a sus familiares. Los Sistemas Híbridos Avanzados, KX-TES824 y KX-TEM824 son sistemas telefónicos que pueden manejar sus negocios y necesidades personales.
La KX-TES824 acepta 3 líneas CO y 8 extensiones.
La KX-TEM824 acepta 6 líneas CO y 16 extensiones.
Con tarjetas opcionales, puede fácilmente expandir la capacidad de su sistema hasta 8 líneas CO y 24 extensiones* dependiendo como sus necesidades aumenten. Ambos sistemas proveen las funciones que satisfacen la demanda de los usuarios más sofisticados y conscientes de los costos. Puede conectar una variedad de equipos de comunicación, como teléfonos inalámbricos, máquinas contestadoras, modems, verificadores de tarjetas de crédito, máquinas de fax, y cualquier otro equipo que trabaje con líneas telefónicas convencionales.
Las Centrales Panasonic KX-TES824 y KX-TEM824 son ideales para negocios pequeños u oficinas en casa que requieren un sistema flexible con un alto grado de sofisticación.

* 8 de las extensiones son puertos para teléfonos sencillos.

Funciones útiles y eficientes

Recepción automática de tres niveles con guía de voz

El sistema ofrece la función DISA (Acceso del Sistema de Ingreso Directo) que permite que los que llaman de afuera tengan un acceso directo a cualquier extensión sin pasar por la recepcionista. La recepcionista o gerente puede grabar un mensaje automático de bienvenida (3 niveles) pasando la llamada a una sección apropiada. "Para el Departamento de Ventas, pulse 1." (Nivel 1) " Para el grupo PBX, pulse 2." (Nivel 2) "Para Marcos, pulse 3 (Nivel 3). La persona que llama también puede marcar el destino deseado, no sólo a una extensión, también para la Llamada a un Grupo* o incluso a líneas externas.
Cuando el sistema recibe una señal de transmisión de facsímil por DISA, se conecta automáticamente a la extensión de facsímil especificada. Las llamadas de facsímil pueden recibirse de día o de noche sin participación de una recepcionista y no es necesario tener una línea telefónica especial para el facsímil.

* Todos los teléfonos en el grupo sonarán simultáneamente, para que cualquiera del grupo conteste la llamada.

Mensaje de voz integrado (BV)*

Ahora puede disfrutar de la eficiencia y facilidad de uso de los mensajes de voz sin agregar un sistema de buzones de voz independiente. La Tarjeta de Mensajes de Voz opcional evita que pueda perder una llamada o mensaje importante de un cliente o colega. Personalice su buzón grabando sus propios mensajes de bienvenida directamente en su buzón personal, para que reciba información privada sin tener que descifrar notas y anotaciones manuscritas. Los Centros de Llamadas de Clientes y los Grupos de Trabajo pueden utilizar el área de mensajes comunes para grabar mensajes de las personas que llaman para reproducirlas posteriormente por una recepcionista o miembro del grupo. Si necesita mensajes de voz más avanzados, un Sistema de Procesamiento de Voz (VPS) le da una flexibilidad y control más profesionales.

* Una Tarjeta de Mensajes de Voz opcional es requerida.

Indicador de ID de llamada en SLT y APT*

- Reconocimiento de Llamada
- Mejor Gestión de Llamadas

El sistema es compatible con el ID de llamada que permite al usuario ver la información de llamada en las pantallas de los Teléfonos Sencillos (SLT) con indicador de ID de llamada y los Teléfonos Propietarios Análogos (APT). Los teléfonos con pantalla propietarios pueden contener el registro de ID de llamada de las 20 llamadas más recientes (Registro de llamadas). Y el sistema tiene 300 registros comunes. Las llamadas recibidas registradas pueden llamarse fácilmente.

* Una tarjeta opcional es requerida.
Llame a su tienda o empresa telefónica para confirmar si el servicio de ID de llamada existe en su región.

Ruta de SMS flexible*

Los mensajes SMS (Servicios de Mensajes Cortos) son una forma barata y cada vez más popular de enviar mensajes de texto entre teléfonos de línea fija y teléfonos móviles. Puede personalizar el sistema para que los transmisores de mensajes SMS dirijan sus mensajes directamente al SLT (Teléfono de Una Línea) de un usuario específico para que sus mensajes se reciban rápidamente y en privado por el usuario deseado.

* Una tarjeta de ID de llamada opcional y un teléfono compatible con SMS para enviar y recibir mensajes SMS son requeridos. Hable con su tienda o empresa telefónica para confirmar que el Servicio de Mensajes Cortos existe en su región.

Sistema Híbrido

Flexible y Simple Expansión

Panasonic le ofrece flexibilidad y simple expansión jamás vista mediante tarjetas opcionales.
Adicionando tarjetas opcionales, puede expandir el sistema desde 3 COs/ 8 extensiones hasta 8 COs/ 24 extensiones para conseguir los cambios que usted necesita.
No se requiere programación adicional ni costos de recableado.

Manejo Eficiente de Llamadas

UCD (Distribución Uniforme de Llamadas) con mensaje

- Mejora la imagen de la compañía.
- No se perderán importantes llamadas de negocios.
- Se comparte la carga de la recepcionista.

Esta función permite que las llamadas entrantes sean distribuidas uniformemente en un grupo de extensiones. Esto es esencial para el manejo eficiente y rápido de muchas llamadas. Si todas las extensiones del grupo UCD (Distribución Uniforme de Llamadas) están ocupadas, el sistema dará un mensaje al que llama – actuando como una recepcionista. Si el grupo de UCD se mantiene ocupado, la llamada puede ser atendida por el sistema secundario DISA (OGM2). Esto es especialmente útil para una oficina donde muchas llamadas llegan al grupo y sólo hay una persona para contestar las llamadas (función de cola).

Desvío de Llamada (Ocupado / Sin Respuesta / Sígueme / hacia Afuera)

- No se perderán importantes llamadas de negocios.

Llamadas entrantes, internas y transferidas pueden ser dirigidas a su extensión u otro destino cuando usted esté en el teléfono o se encuentre lejos de su escritorio. Las llamadas pueden ser dirigidas a un número preprogramado, como su buzón de correo, otro teléfono, o también fuera del edificio de su oficina, mejorando la eficiencia y sobretodo el servicio al cliente. La programación "Sígueme" le permite a usted fijar remotamente la transferencia de llamada desde otro teléfono dentro de su oficina (ej. Sala de Reuniones), así las llamadas a su extensión le llegarán mientras usted este lejos de su escritorio.

Modo Diurno / Nocturno / Almuerzo

El sistema provee las funciones de modo "Diurno/ Nocturno" y "Almuerzo" los cuales pueden ser usados para cambiar la operación del sistema de acuerdo a la hora del día. Por ejemplo, usted puede especificar cuales teléfonos sonarán para las llamadas entrantes después de horas, o prevenir llamadas externas en la noche.

Teléfono Portero, Abridores de Puerta y Timbres de Puerta*

Hasta 4 porteros eléctricos pueden conectarse al sistema. Si un visitante presiona un botón de un teléfono portero. La extensión preasignada sonará y el usuario puede responder la llamada para hablar con el visitante. También puede conectar timbres de puerta estándar al sistema para indicar las llamadas de portero eléctrico con el familiar sonido de campana. Las llamadas de portero eléctrico pueden indicarse por llamada, por timbre o ambos. Si se conectó un abridor de puerta opcional, el usuario de la extensión puede incluso abrir la puerta y dejar entrar al visitante.

* Una tarjeta opcional es requerida.

Mensaje en Espera*

Permite a un usuario desde una extensión notificar a la extensión llamada de un mensaje en espera cuando la extension llamada se encuentra ocupada o no contesta la llamada. Presionando el botón iluminado de Mensaje en Espera del teléfono propietario se puede regresar automáticamente la llamada a la extensión que dejó el mensaje en espera cuando esta se encuentra ocupada o no se contesta la llamada. Presionando la luz en el botón de Mensaje en Espera del teléfono propietario puede retornar la llamada a la extensión que dejó el mensaje.

* Sólo Teléfono Propietario Analógo.

Administración Económica de Costos

Reportes de Actividad de Llamadas (SMDR : Registro Detallado de las Llamadas en el Sistema)

El sistema puede registrar o imprimir la información de llamadas como la fecha, hora, número de extensión, número marcado, duración, etc. La información de SMDR puede ayudar a manejar los costos de llamadas de larga distancia, productividad de los empleados y uso del sistema telefónico.

Introducción de Código de Cuenta (Opcional / Forzado / Verificado)

Los códigos de cuenta puede ser utilizados para identificar las llamadas externas salientes con propósitos de contabilidad y facturación. Las actividades de llamadas hechas con códigos de identificación pueden ser impresas (SMDR). Un "Código de Verificación de Cuenta" es muy útil para controlar los costos de llamadas, porque un usuario que marca un número de larga distancia debe introducir temporalmente un código de cuenta válido para ignorar la restricción de llamada. Códigos de cuenta pueden ser utilizados para administrar los gastos de teléfono más eficientemente.

Restricción de Llamada

El sistema puede ser programado para prohibir llamadas de larga distancia restringiendo a ciertas extensiones de accesar Código de área específicos, determinados prefijos, etc

Bloqueo Electrónico de Extensiones

Previene a personal no autorizado hacer llamadas desde un teléfono "bloqueando" las líneas externas e internas y es requerido un código de seguridad de 4 dígitos antes de hacer llamadas. El operador y administrador son los que dan los privilegios de Bloqueo Electrónico de Extensiones en cualquier extensión usando la consola DSS (Botonera). Por ejemplo, esta función es muy útil para hoteles pequeños cuando los húespedes han efectuado su salida del mismo.

Duración de la Llamada Limitada

El sistema desconectará las llamadas externas salientes cuando el tiempo preprogramado expire. Un tono de alarma será enviado hacia ambas partes 15 segundos antes del límite de tiempo asignado.

Llamadas de Emergencia

Es posible asignar cinco números los cuales pueden ignorar la restricción de llamadas. De esta forma usted podrá hacer llamadas de emergencia a la policía, bomberos, ambulancia, etc.

Conferencia de 5 participantes

Esta función permite a 5 participantes tener una conversación telefónica al mismo tiempo.
Hasta dos líneas externas pueden integrarse a una llamada de conferencia.

Monitoreo de Habitación

Un teléfono propietario o teléfono de puerta puede ser utilizado como un Monitoreo de Habitación. Esta función es muy útil para el monitoreo de infantes o para propósitos de seguridad.

Grupo de Extensiones

El sistema soporta 8 grupos de extensiones. En un grupo de extensiones, las siguientes funciones pueden ser activadas.

Grupo de Contestación de Llamada : Cualquier miembro de un grupo de extensiones puede contestar una llamada dirigida a otro miembro del grupo.

Grupo de Voceo : Cualquier miembro de un grupo de extensiones puede hacer un anuncio de voceo a un miembro de otro grupo.
Un grupo de caza, un grupo de timbrado DISA (Acceso Directo al Sistema) o un grupo UCD (Distribución Uniforme de llamadas) es un grupo específico de extensiones.

Selección de Patrones de Timbrado

Un patrón de timbrado puede ser selecionado dependiendo del tipo de llamada, ya sea una llamada externa, llamada interna o llamada del Teléfono Portero. Usted puede distinguir llamadas privadas de llamadas de negocios.

Fácil Mantenimiento

Personalización y Mantenimiento Intuitivo

La personalización y mantenimiento del sistema es más fácil, gracias al software de Consola de Mantenimiento KX-TE de Panasonic. Simplemente conecte un PC al sistema por la interface USB o en serie (RS-232C) y la interface gráfica intuitiva del software le ayudará con el resto. El Administrador del Sistema puede incluso programar y mantener el sistema fuera del sitio, conectado remotamente a través del modem integrado. Y, por supuesto, también cuenta con la interface de Programación de Teléfono Propietario de Panasonic, para que pueda programar el sistema utilizando un Teléfono Propietario.

Interfase de Respaldo de Batería (Incorporado)

El sistema es fabricado con un interfase de batería incorporado el cual provee una operación completa del sistema en el caso de que falle la energía eléctrica.

Lista de Funciones

- Capacidad de Mensaje en Ausencia
- Introducción de Código de Cuenta (Opcional / Forzado / Verificado)
- Tipo de llamada – Timbre / Voz
- Llamada de vuelta automática cuando Ocupado
- Configuración automática para el tipo de línea externa (CO)
- Transferencia Automática de Fax*
- Interfase de Respaldo de Batería (Incorporado)
- Mensaje de voz integrado (BV)*1
- Señalización de Extensión Ocupada (BSS)
- Desvío de Llamada
  - Todas
  - Ocupada / Sin Respuesta
  - Sígueme
  - Hacia afuera
- Indicacion de Identificador de Llamada en SLT y APT*1*3
- Detección de Señal de Control de Llamada (CPC)*2
- Llamada estacionada
- Captura de Llamada
- Ruta de llamada para SMS de línea fija
- Separación de Llamadas
- Transferencia de Llamadas (hacia extensiones o líneas externas)
- Llamada en espera
- Conferencia (3 Personas / 5 Personas)
- Conferencia, Desatendida (3 Personas)
- Seguridad en Línea de Datos
- Línea de Entrada Directa (DIL)
- DISA (Acceso Directo al Sistema Interno) con mensaje (3 niveles, 1 canal, 180 segundos)
- Tono Distintivo de Llamada
- No Molestar (DND)
- Ignorar No Molestar
- Abridor de Puerta*1
- Llamada al Teléfono de puerta (portero)*1
- Consola DSS (Botonera) (Selección Directa de Interno)
- Llamada de Emergencia
- Acceso a llamada en curso (Extensiones / Línea externa)
- Negar acceso a llamada en curso
- Grupo de Extensiones
- Contraseña de Extensiones / Contraseña del Sistema
- Acceso a Funciones Externas
- Respuesta con Manos Libres
- Retención de Llamada
- Interrupción de Ruta
- Llamada Interna
- Duración de Llamada Limitada (1-32 minutos)
- Ingreso / Salida de Sistema
- Música durante la retención de Llamada (BGM)
- Discado de un toque
- Llamada de Operador
- Mensaje de Bienvenida (OGM)*
- Voceo
  - Todas las extensiones
  - Grupo
  - Externa
- Voceo Denegado
- Conexión de Teléfono en Paralelo
- Discado Automático (Línea Caliente)
- Detección de Polaridad Inversa*2
- Transferencia en Caso de Falla Eléctrica
- Asignación de línea de preferencia (Entrante / Saliente)
- Programación (vía teléfono propietario/ PC)
- Conversión de Pulso a Tono
- Rediscado (Automática / Último Número / Número Memorizado / Identificador de llamada registrado*1)
- Selección de Patrón de Timbrado
- Monitoreo de Habitación (Teléfono Propietario Análogo / Teléfono Portero)
- Discado Secreto
- Discado Rápido
  - Sistema
  - Personal
- Cancelación de Funciones de Interno
- Búsqueda de Extensión
- Bloqueo de Extensión
- Bloqueo de Extensión, mediante teclas de Línea Remota.
- SMDR (Registro en Detalle de las Llamadas del Sistema)
- Servicio de Horario (Diurno / Nocturno / Almuerzo)
- Alarma recordatoria
- Alarma recordatoria, mediante teclas de Línea Remota
- Restricción de Llamada
- Ignorar Restricción de Llamada
- UCD (Distribución Uniforme de Llamada) con mensaje*
- Integración con el correo de voz (APT / DTMF)
- Clase de Servicio (Trasladable)
- Numeración Flexible de Extensión

*1 Una tarjeta opcional es requerida.
*2 La Detección de Polaridad Inversa está sujeta a la Compañía de Teléfonos de su país.
*3 Llame a su tienda o empresa telefónica para confirmar que el servicio de Identificador de llamada existe en su región.
* Abridor de Puerta #1 y Abridor de Puerta #2 no pueden ser usados al mismo tiempo.
Abridor de Puerta #3 y Abridor de Puerta #4 no pueden ser usados al mismo tiempo.
APT: Teléfono Propietario Análogo
SLT: Teléfono Sencillo

Interfases

RS-232C
USB (1.1)
Interfase de Batería
Teléfono Portero / Abridor de Puerta
Fuente de Música Externa
Voceo Externo

Especificaciones

Configuración

Configuración Básica	KX-TE82480 2COs / 8 SLTs	KX-TE82483 3COs / 8 Híbridas	KX-TE82474 8 SLTs
KX-TES824 Línea externa : 3 Extensión : 8	5 16	6 16	3 16
		6 16	6 24
	5 16	8 24	
KX-TEM824 Línea externa : 8 Extensión : 16	8 24		6 24

Capacidad del Sistema

Elemento	KX-TES/TEM824
Operador	1
Discado Rápido del Sistema	100
Discado Rápido Personal	10 / Ext.
Discado de un toque	Max. 24 / Extensiones
Grupos de Extensiones	8
Grupo de UCD	1
Niveles de Restricción de Llamada	5
Códigos de Cuenta (Verificados)	50
Llamada Estacionada	10
Registro de llamada (Identificador de llamada)*3	20 (Personal) 300 (Común)
Mensaje en Ausencia	6
Mensaje en Espera	8 / Extensiones
Códigos de Emergencia	5
Fuente de Música Externa	1
Voceo Externo	1
Teléfono Portero	4
Abridores de Puerta	4
Consolas DSS	2
Mensaje de Salida (DISA)	360 seg.
Mensaje de bienvenida (BV)	125 mensajes o 60 min. (1 canal)

Especificaciones

Elemento	KX-TES824	KX-TEM824
Capacidad Máxima	8 CO y 24 Extensiones 16 Híbridas, 8 Sencillas	8 CO y 24 Extensiones 16 Híbridas, 8 Sencillas
Vías Internas	4	4
Método de Discado	Externo: Tono/Pulso (10pps, 20pps) Interno: Tono/Pulso (10pps, 20pps)	
Conversión de Discado	Pulso a Tono	
Conexiones	Líneas CO: Jack Modular RJ-11 Internos: Jack Modular (4 hilos) Voceo: Jack Conductor Música Externa: Jack Conductor SMDR: Interfase RS-232C Puerto (9 pines D-SUB) Programación: RS-232C/USB/modem remoto	
SMDR	Detalle de Grabación : Fecha, Hora, Número de Extensión, Número de Troncal, Números Marcados, Duración de la Llamada y Código de Cuenta, Identificador de llamada*3	
Detección de Polaridad Inversa*2	Sí	Sí
Puertos para Correo de Voz	2 puertos (APT o DTMF)	4 puertos (APT o DTMF)
Receptores DTMF	2	4
Generadores DTMF	1	1
Rutas de Transferencia CO-CO	2	2
Puertos de Transferencia de Falla Eléctrica	1	2
Conexión Directa a la Batería Externa	Sí	Sí
Fuente de Poder	AC 110 – 240 Voltios, 50/60Hz	
Requerimientos de Energía (max.)	45W	58W
Dimensiones	368mm x 284mm x 102mm	368mm x 284mm x 102mm
Peso (cuando tiene todos los accesorios)	Aprox. 3.5Kg	

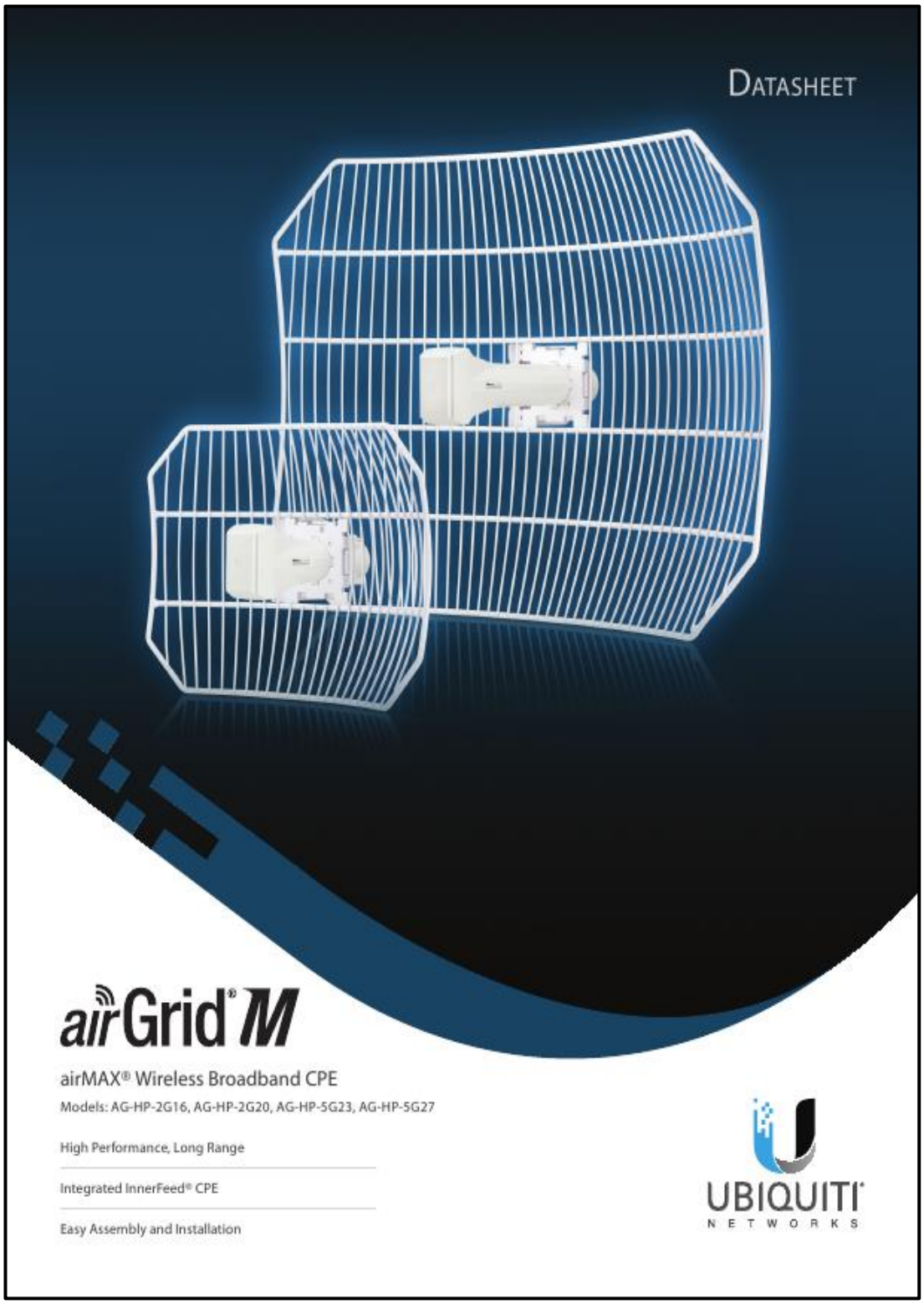
Opciones

Opción	Descripción	KX-TES824	KX-TEM824
KX-TE82461	Tarjeta de Teléfono Portero / Abridor de Puerta de 4 puertos	Max. 1	Max. 1
KX-TE82474	Tarjeta de 8 puertos de extensión para teléfono sencillo	Max. 1	Max. 1
KX-TE82480	Tarjeta de 2 puertos de línea CO análoga y 8 puertos de extensión sencilla	Max. 1	Max. 1
KX-TE82483	Tarjeta de 3 puertos de línea CO análoga y 8 puertos de extensión híbrida.	Max. 1	
KX-TE82491	Tarjeta de expansion de Mensaje de Salida (OGM) en DISA / UCD	Max. 1	Max. 1
KX-TE82492	Tarjeta de Correo de Voz de 2 canales	Max. 1	Max. 1
KX-TE82493	Tarjeta de Identificación de llamada de 3 puertos	Max. 3	Max. 3
KX-T30865	Teléfono de Puerta	Max. 4	Max. 4
KX-A227	Cable de la Batería de Respaldo		

www.telepana.com

Panasonic
TELEFONIA SOPORTE Y SERVICIO PA

Anexo 5. - Datasheet airGrid AG-HP-5G27

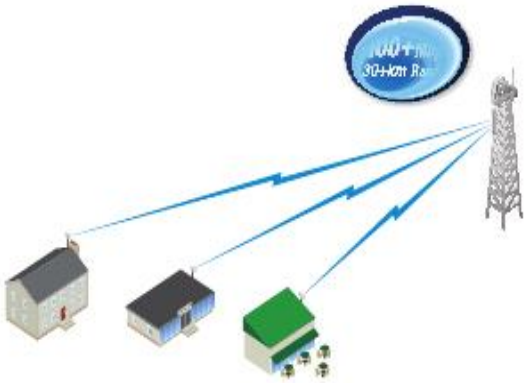


airGrid M

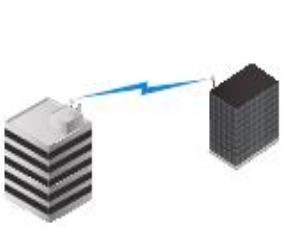
Utilizing InnerFeed technology, the new airGrid® M HP Series from Ubiquiti Networks represents the latest evolution of outdoor wireless broadband devices. The revolutionary InnerFeed technology integrates the entire radio system into the feedhorn of the antenna. airGrid M combines Ubiquiti's InnerFeed and airMAX® (TDMA protocol) technologies to create a simple, yet extremely powerful and robust wireless CPE (Customer Premises Equipment).

Complete antenna and radio system integration provides affordable cost/performance solutions to the wireless broadband industry. airGrid M operates in the worldwide, license-free frequency range of either 2 GHz or 5 GHz, and features breakthrough performance of up to 100+ Mbps in real outdoor throughput and incredible range of up to 30+ km.

The low-cost, high-performance, robust "all-in-one" design and light weight of airGrid M make it versatile and ideal in several different applications.



airGrid M as a cost-effective CPE in an airMAX Point-to-Multi-Point network.



Use an airGrid M on each side of a Point-to-Point link to create a reliable connection.

airGrid M as a powerful wireless client.

Integrated airMAX Technology

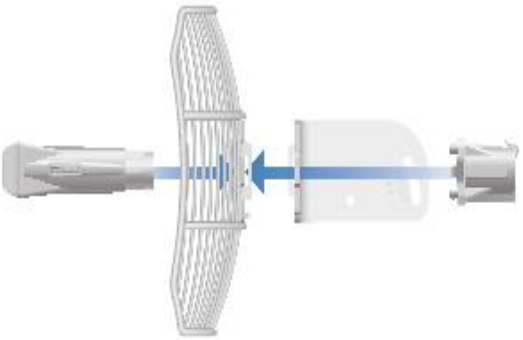
Unlike standard Wi-Fi protocol, the exclusive Ubiquiti Networks® airMAX Time Division Multiple Access (TDMA) protocol allows each client to send and receive data using pre-designated time slots managed by an intelligent AP controller. This "time slot" method eliminates hidden node collisions and maximizes airtime efficiency.

Compared to other systems in its class, the airGrid M delivers superior performance in reduced latency, throughput, and scalability.

- **Intelligent QoS** Priority is given to voice/video for seamless access.
- **Scalability** High capacity and scalability.
- **Long Distance** Capable of high-speed, 30+ km links.

Easy, No-Tool Assembly

With its updated mechanical design, assembling and disassembling the airGrid M is literally a snap. No tools are required.



You simply snap the feed, antenna, mounting bracket and rear housing together for a secure, solid assembly.

Specifications

System Information	
Processor Specs	Atheros MIPS 74Kc, 560 MHz
Memory Information	64 MB DDR2, 8 MB Flash
Networking Interface	(1) 10/100 Ethernet Port

Regulatory / Compliance Information	
Wireless Approvals	FCC Part 15.247, IC RS210, CE
RoHS Compliance	Yes

Physical / Electrical / Environmental	
Enclosure Characteristics	Outdoor UV Stabilized Plastic
Mounting Kit	Pole Mounting Kit (Included)
Max. Power Consumption	3W
Power Supply	24V, 0.5A PoE Adapter (Included)
Power Method	Passive Power over Ethernet (Pairs 4, 5+; 7, 8 Return)
Operating Temperature	-30 to 75° C (-22 to 167° F)
Operating Humidity	5 to 95% Condensing
Shock and Vibration	ETSI300-019-1.4
ETSI Specification	EN 302 326 DN2

AG-HP-2G20

AG-HP-2G16

AG-HP-5G27

AG-HP-5G23

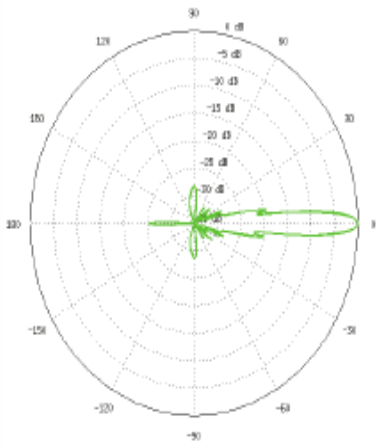
Specifications

AG-HP-5G27	
Dimensions (Mount Included)	620 x 460 x 360 mm (24.41 x 18.11 x 14.17")
Weight (Mount Included)	2585 g (5.699 lb)
Wind Survivability	200 km/h (125 mph)
Wind Loading	102 N @ 200 km/h (23 lbf @ 125 mph)
Operating Frequency	Worldwide: 5170 – 5875 MHz USA: 5725 – 5850 MHz
Max. VSWR	1.5:1
Gain	27 dBi

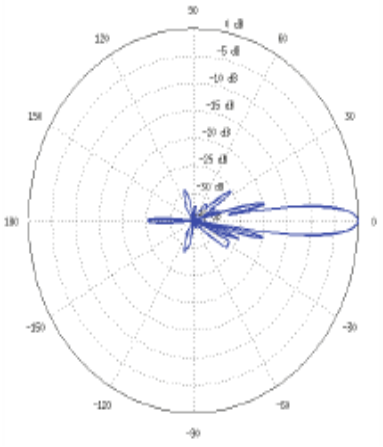
AG-HP-5G27 Output Power: 25 dBm							
TX Power Specifications				**RX Power Specifications**			
Modulation	Data Rate	Avg. TX	Tolerance	Modulation	Data Rate	Sensitivity	Tolerance
11a	1 - 24 Mbps	25 dBm	± 2 dB	11a	1 - 24 Mbps	-97 dBm min.	± 2 dB
	36 Mbps	24 dBm	± 2 dB		36 Mbps	-90 dBm	± 2 dB
	48 Mbps	22 dBm	± 2 dB		48 Mbps	-86 dBm	± 2 dB
	54 Mbps	21 dBm	± 2 dB		54 Mbps	-84 dBm	± 2 dB
11n / airMAX	MCS0	25 dBm	± 2 dB	11n / airMAX	MCS0	-97 dBm	± 2 dB
	MCS1	25 dBm	± 2 dB		MCS1	-96 dBm	± 2 dB
	MCS2	25 dBm	± 2 dB		MCS2	-93 dBm	± 2 dB
	MCS3	24 dBm	± 2 dB		MCS3	-91 dBm	± 2 dB
	MCS4	23 dBm	± 2 dB		MCS4	-87 dBm	± 2 dB
	MCS5	22 dBm	± 2 dB		MCS5	-84 dBm	± 2 dB
	MCS6	21 dBm	± 2 dB		MCS6	-78 dBm	± 2 dB
	MCS7	19 dBm	± 2 dB		MCS7	-75 dBm	± 2 dB

Antenna Polar Plots

Azimuth



Elevation



www.ubnt.com

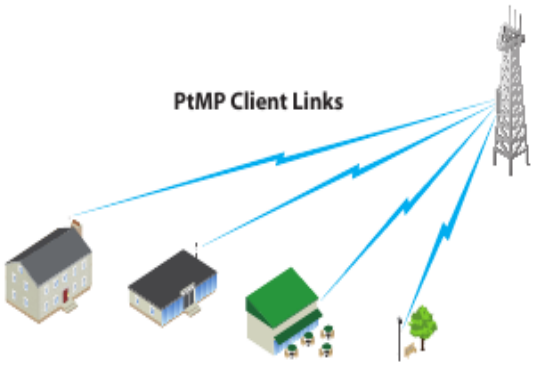
Anexo 6. - Datasheet Ubiquiti locoM5 NanoStation

Overview

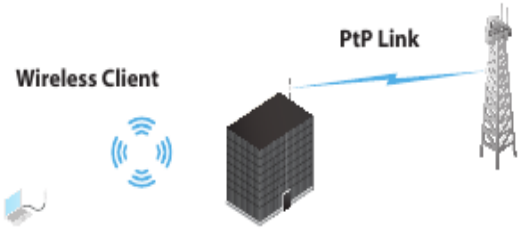
Leading-Edge Industrial Design

Ubiquiti Networks sets the bar for the world's first low-cost and efficient broadband Customer Premises Equipment (CPE) with the original NanoStation®. The NanoStationM and NanoStationlocoM take the same concept to the future with sleek and elegant form factors, along with integrated airMAX® (MIMO TDMA protocol) technology.

The low cost, high performance, and small form factor of NanoStationM and NanoStationlocoM make them extremely versatile and economical to deploy.



NanoStationM used as powerful clients in an airMAX PtMP (Point-to-Multi-Point) network setup.



NanoStationM as a powerful wireless client.

Use two NanoStationM to create a PtP link.

Utilize airMAX Technology

Unlike standard Wi-Fi protocol, Ubiquiti's Time Division Multiple Access (TDMA) airMAX protocol allows each client to send and receive data using pre-designated time slots scheduled by an intelligent AP controller.

This "time slot" method eliminates hidden node collisions and maximizes airtime efficiency. It provides many magnitudes of performance improvements in latency, throughput, and scalability compared to all other outdoor systems in its class.

Intelligent QoS Priority is given to voice/video for seamless streaming.

Scalability High capacity and scalability.

Long Distance Capable of high-speed, carrier-class links.

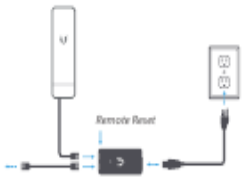
Latency Multiple features dramatically reduce noise.

Dual Ethernet Connectivity[1]

The NanoStationM provides a secondary Ethernet port with software-enabled PoE output for seamless IP video integration.

Intelligent PoE[2]

The remote hardware reset circuitry of the NanoStationM allows the device to be remotely reset from the power supply location.



The NanoStationM may also be powered by the Ubiquiti Networks® EdgeSwitch™. In addition, any NanoStationM can easily become 48V, 802.3af compliant through use of the Ubiquiti® Instant 802.3af Adapter (sold separately).

[1] *Only NanoStationM models*

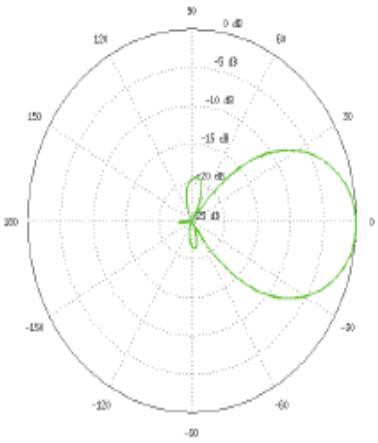
[2] *Remote reset is an option that is sold separately as the POE-24. The NanoStationM includes a 24V PoE adapter without remote reset.*

Specifications

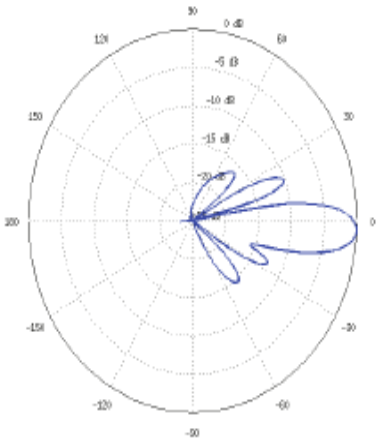
NSM5			
Dimensions	294 x 31 x 80 mm (11.57 x 1.22 x 3.15")		
Weight	400 g (14.11 oz)		
Power Supply (PoE)	24V, 0.5A		
Max. Power Consumption	8W		
Power Method	Passive PoE (Pairs 4, 5+; 7, 8 Return)		
Operating Frequency	Worldwide	USA	USA DFS
	5170-5875 MHz	5725-5850 MHz	5250-5850 MHz
Gain	14.6-16.1 dBi		
Networking Interface	(2) 10/100 Ethernet Ports		
Processor Specs	Atheros MIPS 74Kc, 560 MHz		
Memory	64 MB DDR2, 8 MB Flash		
Frequency	5 GHz		
Cross-pol Isolation	22 dB Minimum		
Max. VSWR	1.6:1		
Beamwidth	43° (H-pol) / 41° (V-pol) / 15° (Elevation)		
Polarization	Dual Linear		
Enclosure	Outdoor UV Stabilized Plastic		
Mounting	Pole-Mount (Kit Included)		
Operating Temperature	-30 to 75° C (-22 to 167° F)		
Operating Humidity	5 to 95% Noncondensing		
Wireless Approvals	FCC Part 15.247, IC RS210, CE		
RoHS Compliance	Yes		
Shock & Vibration	ETSI300-019-1.4		

Output Power: 27 dBm							
5 GHz TX Power Specifications				5 GHz RX Power Specifications			
Modulation	Data Rate/MCS	Avg. TX	Tolerance	Modulation	Data Rate/MCS	Sensitivity	Tolerance
11a	6-24 Mbps	27 dBm	± 2 dB	11a	6-24 Mbps	-94 dBm	± 2 dB
	36 Mbps	25 dBm	± 2 dB		36 Mbps	-80 dBm	± 2 dB
	48 Mbps	23 dBm	± 2 dB		48 Mbps	-77 dBm	± 2 dB
	54 Mbps	22 dBm	± 2 dB		54 Mbps	-75 dBm	± 2 dB
11n/airMAX	MCS0	27 dBm	± 2 dB	11n/airMAX	MCS0	-96 dBm	± 2 dB
	MCS1	27 dBm	± 2 dB		MCS1	-95 dBm	± 2 dB
	MCS2	27 dBm	± 2 dB		MCS2	-92 dBm	± 2 dB
	MCS3	27 dBm	± 2 dB		MCS3	-90 dBm	± 2 dB
	MCS4	26 dBm	± 2 dB		MCS4	-86 dBm	± 2 dB
	MCS5	24 dBm	± 2 dB		MCS5	-83 dBm	± 2 dB
	MCS6	22 dBm	± 2 dB		MCS6	-77 dBm	± 2 dB
	MCS7	21 dBm	± 2 dB		MCS7	-74 dBm	± 2 dB
	MCS8	27 dBm	± 2 dB		MCS8	-95 dBm	± 2 dB
	MCS9	27 dBm	± 2 dB		MCS9	-93 dBm	± 2 dB
	MCS10	27 dBm	± 2 dB		MCS10	-90 dBm	± 2 dB
	MCS11	27 dBm	± 2 dB		MCS11	-87 dBm	± 2 dB
	MCS12	26 dBm	± 2 dB		MCS12	-84 dBm	± 2 dB
	MCS13	24 dBm	± 2 dB		MCS13	-79 dBm	± 2 dB
	MCS14	22 dBm	± 2 dB		MCS14	-78 dBm	± 2 dB
	MCS15	21 dBm	± 2 dB		MCS15	-75 dBm	± 2 dB

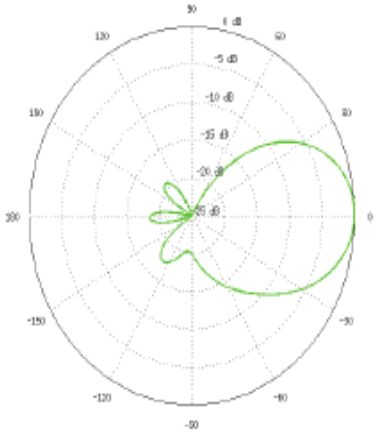
Vertical Azimuth



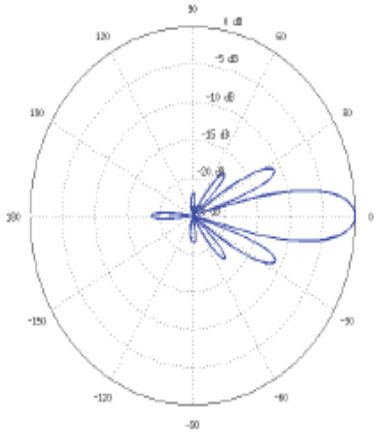
Vertical Elevation



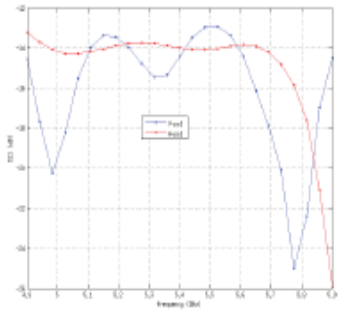
Horizontal Azimuth



Horizontal Elevation



Return Loss



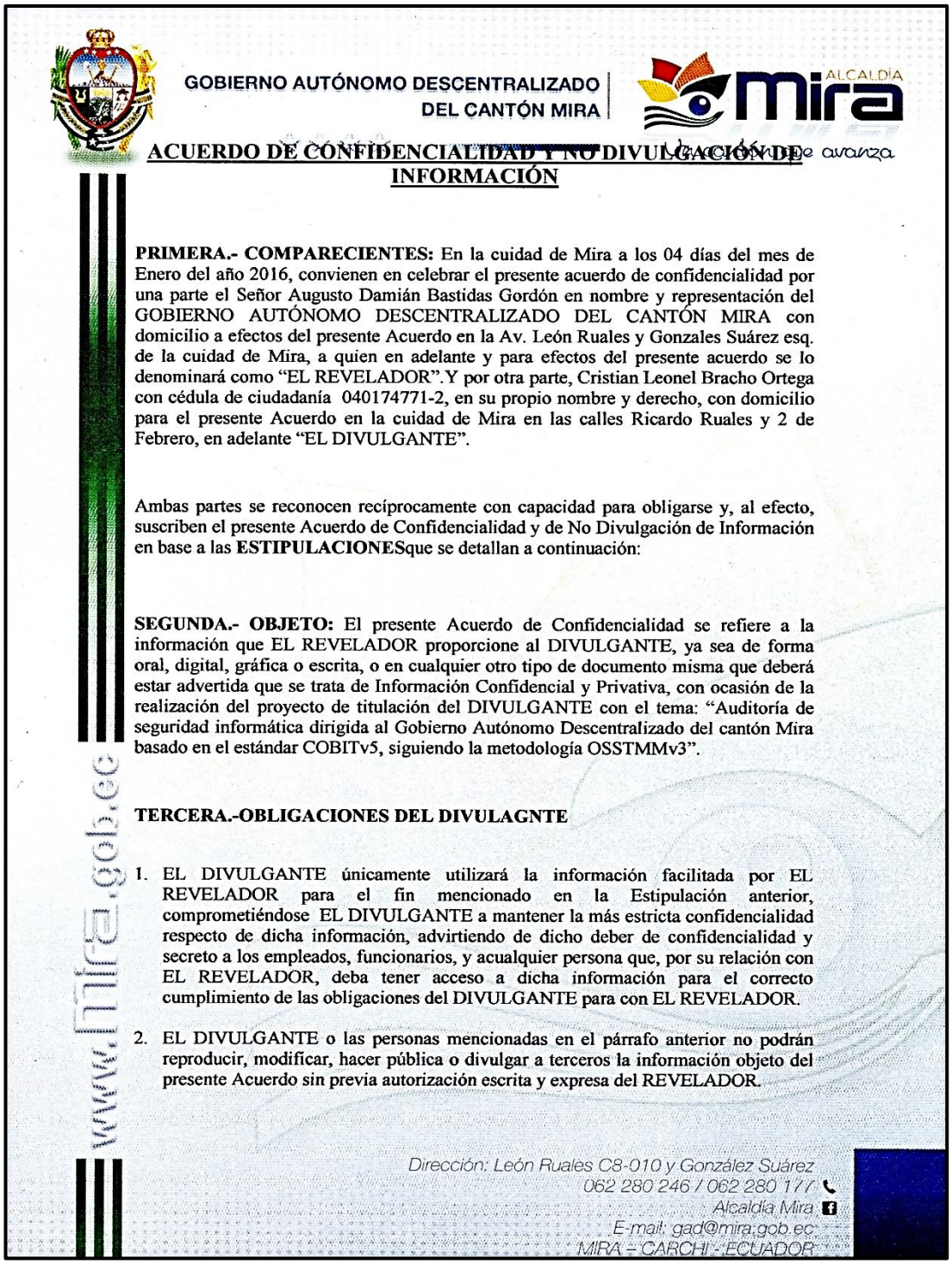
Specifications are subject to change. Ubiquiti products are sold with a limited warranty described at: www.ubnt.com/support/warranty

www.ubnt.com

NanoStation M NanoStation loco M | DATASHEET

AJUL092016

Anexo 7.- Acuerdo De Confidencialidad Y No Divulgación De Información



GOBIERNO AUTÓNOMO DESCENTRALIZADO
DEL CANTÓN MIRA

ALCALDÍA Mira

la acción de avanza

ACUERDO DE CONFIDENCIALIDAD Y NO DIVULGACIÓN DE INFORMACIÓN

PRIMERA.- COMPARECIENTES: En la cuidad de Mira a los 04 días del mes de Enero del año 2016, convienen en celebrar el presente acuerdo de confidencialidad por una parte el Señor Augusto Damián Bastidas Gordón en nombre y representación del GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN MIRA con domicilio a efectos del presente Acuerdo en la Av. León Ruales y Gonzales Suárez esq. de la cuidad de Mira, a quien en adelante y para efectos del presente acuerdo se lo denominará como "EL REVELADOR".Y por otra parte, Cristian Leonel Bracho Ortega con cédula de ciudadanía 040174771-2, en su propio nombre y derecho, con domicilio para el presente Acuerdo en la cuidad de Mira en las calles Ricardo Ruales y 2 de Febrero, en adelante "EL DIVULGANTE".

Ambas partes se reconocen recíprocamente con capacidad para obligarse y, al efecto, suscriben el presente Acuerdo de Confidencialidad y de No Divulgación de Información en base a las **ESTIPULACIONES**que se detallan a continuación:

SEGUNDA.- OBJETO: El presente Acuerdo de Confidencialidad se refiere a la información que EL REVELADOR proporcione al DIVULGANTE, ya sea de forma oral, digital, gráfica o escrita, o en cualquier otro tipo de documento misma que deberá estar advertida que se trata de Información Confidencial y Privativa, con ocasión de la realización del proyecto de titulación del DIVULGANTE con el tema: "Auditoría de seguridad informática dirigida al Gobierno Autónomo Descentralizado del cantón Mira basado en el estándar COBITv5, siguiendo la metodología OSSTMMv3".

TERCERA.-OBLIGACIONES DEL DIVULAGNTE

1. EL DIVULGANTE únicamente utilizará la información facilitada por EL REVELADOR para el fin mencionado en la Estipulación anterior, comprometiéndose EL DIVULGANTE a mantener la más estricta confidencialidad respecto de dicha información, advirtiendo de dicho deber de confidencialidad y secreto a los empleados, funcionarios, y acualquier persona que, por su relación con EL REVELADOR, deba tener acceso a dicha información para el correcto cumplimiento de las obligaciones del DIVULGANTE para con EL REVELADOR.
2. EL DIVULGANTE o las personas mencionadas en el párrafo anterior no podrán reproducir, modificar, hacer pública o divulgar a terceros la información objeto del presente Acuerdo sin previa autorización escrita y expresa del REVELADOR.

www.mira.gob.ec

Dirección: León Ruales C8-010 y González Suárez
062 280 246 / 062 280 177
Alcaldía Mira
E-mail: gad@mira.gob.ec
MIRA - CARCHI - ECUADOR

3. De igual forma, EL REVELADOR adoptará respecto de la información objeto de este Acuerdo las mismas medidas de seguridad que adoptaría normalmente respecto a la información confidencial de su propia Institución a la que representa, evitando en la medida de lo posible su pérdida, robo o sustracción.

CUARTA.-EXCEPCIONES A LA CONFIDENCIALIDAD: Sin perjuicio de lo estipulado en el presente Acuerdo, ambas partes aceptan que la obligación de confidencialidad no se aplicará en los siguientes casos:

a) Cuando EL REVELADOR autorice, por escrito, al DIVULGANTE para que revele la información sin restricción alguna.

b) Cuando la información se encontrara en el dominio público en el momento de su suministro al DIVULGANTE o, una vez suministrada la información, ésta acceda al dominio público sin infracción de ninguna de las Estipulaciones del presente Acuerdo.

c) Cuando la información ya estuviera en el conocimiento del DIVULGANTE con anterioridad a la firma del presente Acuerdo y sin obligación de guardar confidencialidad.

d) Cuando la legislación vigente o un mandato judicial exija su divulgación. En ese caso, EL DIVULGANTE notificará al REVELADOR tal eventualidad y hará todo lo posible por garantizar que se dé un tratamiento confidencial a la información.

e) En caso de que EL DIVULGANTE pueda probar que la información fue desarrollada o recibida legítimamente de terceros, de forma totalmente independiente a su relación con EL REVELADOR.

QUINTA.- PROPIEDAD: Los derechos de propiedad intelectual de la información objeto de este Acuerdo pertenecen al REVELADOR y el hecho de revelarla al DIVULGANTE para el fin mencionado en la Estipulación Primera no cambiará tal situación.

En caso de que la información resulte revelada o divulgada o utilizada por EL DIVULGANTE de cualquier forma distinta al objeto de este Acuerdo, ya sea de forma dolosa o por mera negligencia, habrá de indemnizar al REVELADOR los daños y perjuicios ocasionados, sin perjuicio de las acciones civiles o penales que puedan corresponder a este último.

SEXTA.- OBLIGACIONES ANTE EL CESE DEL ACUERDO: Las partes se obligan a devolver cualquier documentación, antecedente facilitado en cualquier tipo de

Dirección: León Ruales C8-010 y González Suárez
062 280 246 / 062 280 177
Alcaldía Mira
E-mail: gad@mira.gob.ec
MIRA – CARCHI - ECUADOR

soporte y, en su caso, las copias obtenidas de los mismos, que constituyan información amparada por el deber de confidencialidad objeto del presente Acuerdo en el supuesto de que cese la relación entre las partes por cualquier motivo.

SEPTIMA.-PLAZO: El presente Acuerdo entrará en vigor en el momento de la firma del mismo por ambas partes, extendiéndose su vigencia hasta un plazo de dos años después de finalizada la relación entre las partes o, en su caso, la prestación del servicio.

OCTAVA.-JURISDICCIÓN: En caso de cualquier conflicto o discrepancia que pueda surgir en relación con la interpretación y/o cumplimiento del presente Acuerdo, las partes se someten expresamente a los Juzgados y Tribunales de la Provincia del Carchi, con renuncia a su fuero propio, aplicándose la legislación del Ecuador vigente.

Y en señal de expresa conformidad y aceptación de los términos recogidos en el presente Acuerdo, lo firman las partes por duplicado ejemplar y a un solo efecto en el lugar y fecha indicados en la Cláusula Primera.

POR EL REVELADOR,
Augusto Damián Bastidas Gordón

GOBIERNO AUTÓNOMO DESCENTRALIZADO DE MIRA
MIRA - CARCHI
INFORMÁTICA

POR EL DIVULGANTE,
Cristian Leonel Bracho Ortega

Anexo 8.- Cronograma de la auditoría

Mira, 12 de Septiembre del 2016

Señor
Damián Bastidas
RESPONSABLE DEL ÁREA DE SISTEMAS DEL GADM MIRA
Presente

Yo, Cristian Leonel Bracho Ortega, portador del número de cédula de ciudadanía 040174771-2 y estudiante de la Carrera de Ingeniería de Electrónica y Redes de Comunicación de la Universidad Técnica del Norte, por motivo de encontrarme desarrollando mi trabajo de grado con el tema: "AUDITORÍA DE SEGURIDAD INFORMÁTICA DIRIGIDA AL GOBIERNO AUTÓNOMO DESCENTRALIZADO DEL CANTÓN MIRA BASADO EN EL ESTÁNDAR COBITv5, SIGUIENDO LA METODOLOGÍA OSSTMMv3", por medio de la presente solicito muy comedidamente se me brinde la apertura necesaria a tan prestigiosa entidad, y a la información que sea permitida acceder, para poder llevar a cabo las actividades requeridas para el proceso de la auditoría.

Para ello se adjunta el cronograma al que se acogerá dicho proceso, en el que constan los cinco puntos que se auditarán dentro del GADM.

De antemano le agradezco su atención y consideración hacia mi solicitud.

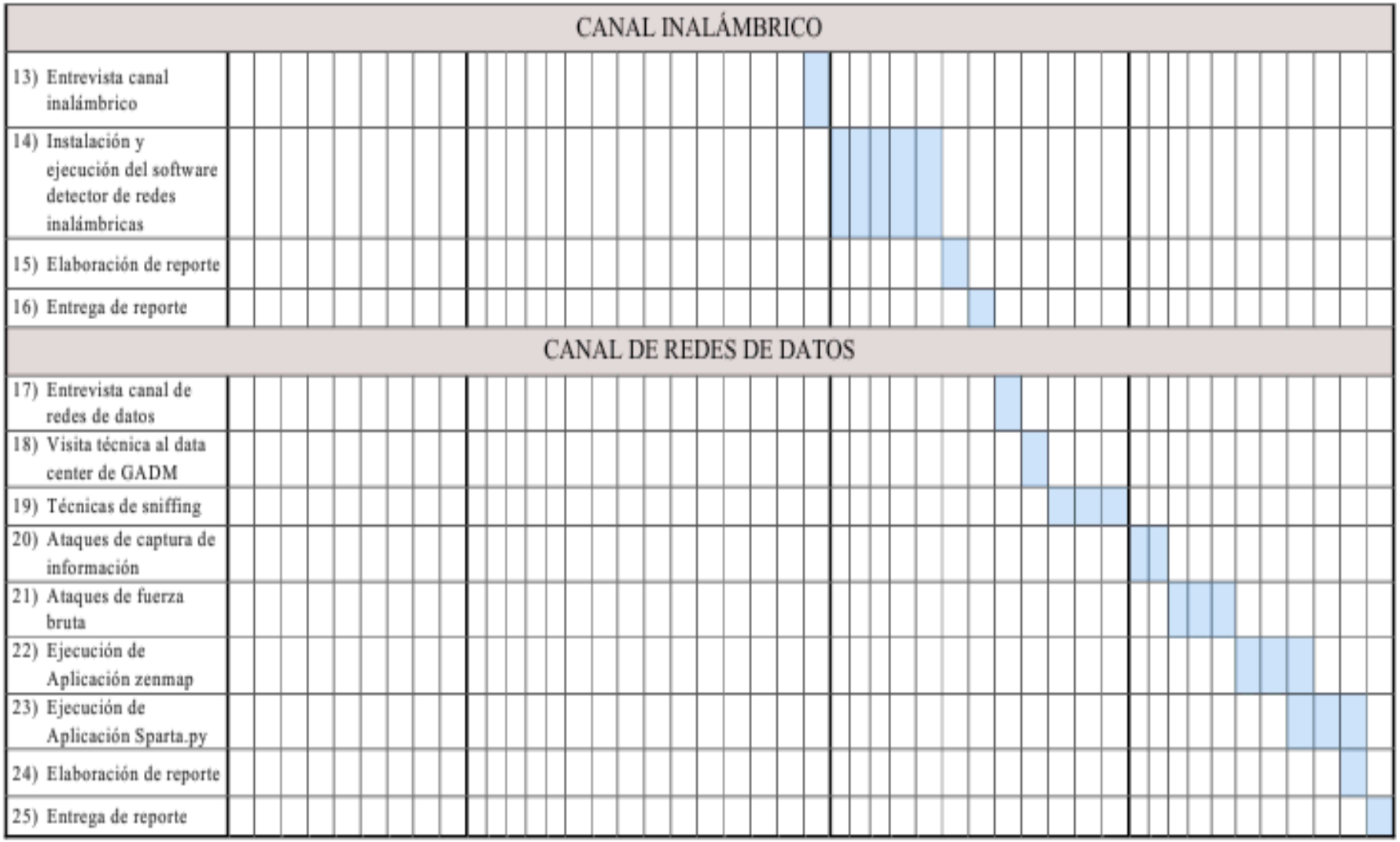
Atentamente:

Cristian Leonel Bracho Ortega

RECIBIDO 12/SEPTIEMBRE/2016
GOBIERNO AUTONOMO DESCENTRALIZADO DE MIRA
MIRA - CARCHI
INFORMÁTICA

CRONOGRAMA DE ACTIVIDADES

Actividad \ Fecha	Septiembre									Octubre											Noviembre										Diciembre											
	15	17	20	21	23	26	28	29	30	3	4	5	6	7	10	11	12	13	14	19	25	26	27	28	7	8	9	10	11	17	18	21	23	25	28	30	1	2	6	7	8	9	12	13	14	15	16
CANAL HUMANO																																													
1) Encuestas a 10 empleados del GADM																																													
2) Tabulación de encuestas																																													
3) Técnicas de Observación y Persuasión																																													
4) Técnica de la llamada telefónica falsa																																													
5) Recolección de información para reporte																																													
6) Redacción del reporte																																													
7) Entrega del reporte																																													
CANAL FÍSICO																																													
8) Técnicas de observación directa																																													
9) Checklist Responsable del Área de Sistemas																																													
10) Comparación con datos reales																																													
11) Elaboración del reporte																																													
12) Entrega de reporte																																													


CANAL INALÁMBRICO
13) Entrevista canal inalámbrico
14) Instalación y ejecución del software detector de redes inalámbricas
15) Elaboración de reporte
16) Entrega de reporte
CANAL DE REDES DE DATOS
17) Entrevista canal de redes de datos
18) Visita técnica al data center de GADM
19) Técnicas de sniffing
20) Ataques de captura de información
21) Ataques de fuerza bruta
22) Ejecución de Aplicación zenmap
23) Ejecución de Aplicación Sparta.py
24) Elaboración de reporte
25) Entrega de reporte

Anexo 9.- Directorio completo del personal de planta del GADM del Cantón Mira

Art. 7 de la Ley Orgánica de Transparencia y Acceso a la Información Pública - LOTAIP

Literal b1) El directorio completo de la institución

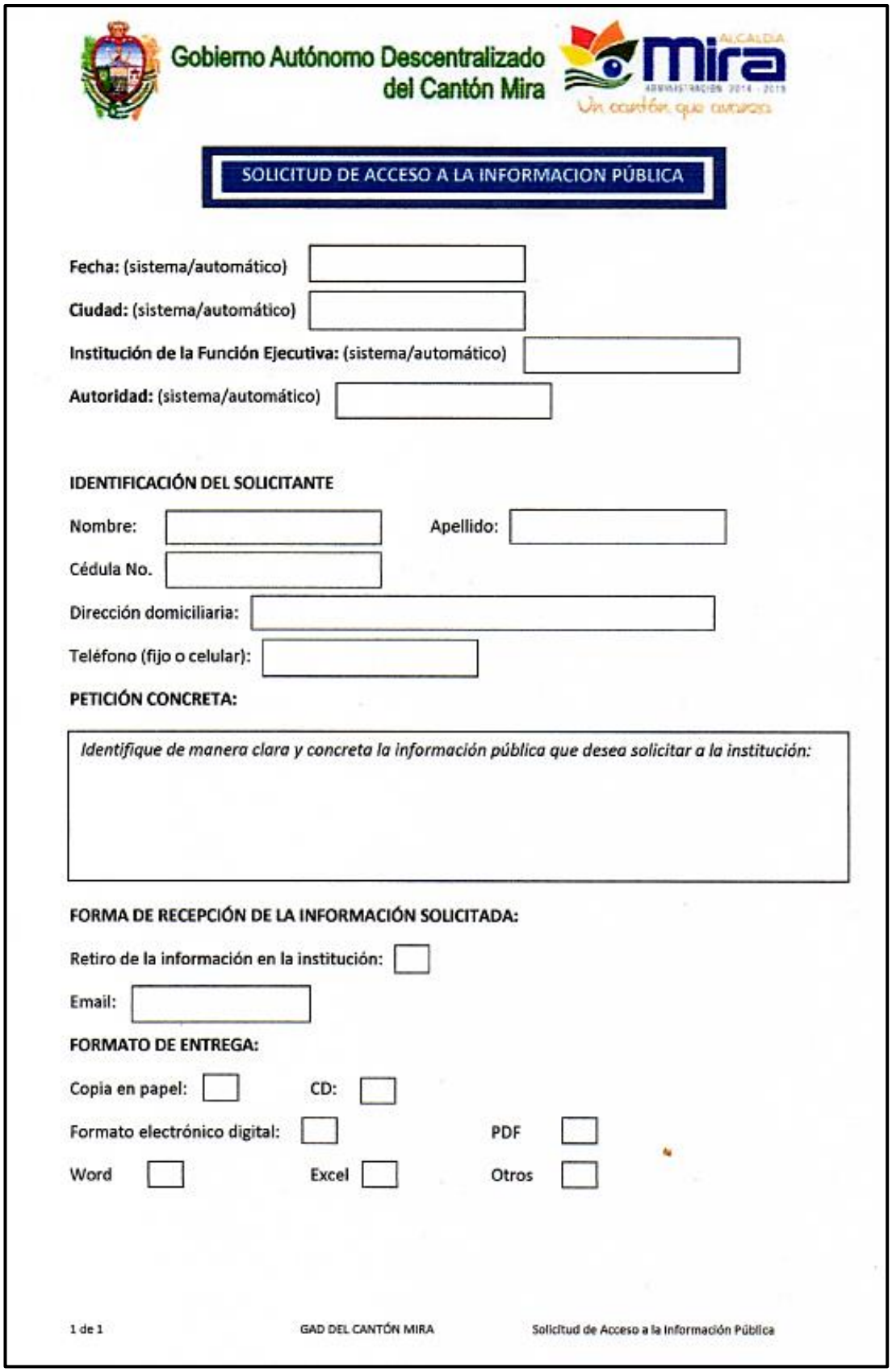
No.	Apellidos y Nombres de los servidores y servidoras	Puesto Institucional	Unidad a la que pertenece	Dirección institucional	Ciudad en la que labora	Teléfono institucional	Extensión telefónica	Correo Electrónico institucional
1	VILLEGAS GUARDADO WALTER DE JESUS	ALCALDE	ADMINISTRACION GENERAL	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	102	wvillegas@mira.gob.ec
2	LOPEZ CARRERA EDISSON MAURICIO	ASESOR DE ALCALDIA	ADMINISTRACION GENERAL	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	103	mlopez@mira.gob.ec
3	ENRIQUEZ AYALA CARLOS ANDRES	SECRETARIA GENERAL	ADMINISTRACION GENERAL	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	103	aenriquez@mira.gob.ec
4	PAREDES BRACHO ZOILA IRENE	ASISTENTE ADMINISTRATIVO	ADMINISTRACION GENERAL	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	103	zparedes@mira.gob.ec
5	SALAZAR LARA JULIO CESAR	PROCURADOR SINDICO	ADMINISTRACION GENERAL	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	111	csalazar@mira.gob.ec
6	RUIZ MUÑOZ NANCY ARGENTINA	ASISTENTE ADMINISTRATIVO	ADMINISTRACION GENERAL	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	111	nruiz@mira.gob.ec
7	BOLAÑOS RUALES NANCY DEL CONSUELO	CONCEJAL	ADMINISTRACION GENERAL	Eloy Alfaro y Simón Bolivar, esquina	Mira	2280452	S/E	nbolaños@mira.gob.ec
8	VILLOTA PALMA LUIS GERMAN	CONCEJAL	ADMINISTRACION GENERAL	Eloy Alfaro y Simón Bolivar, esquina	Mira	2280452	S/E	gvillota@mira.gob.ec
9	CADENA ENRIQUEZ ARMANDO VINICIO	CONCEJAL	ADMINISTRACION GENERAL	Eloy Alfaro y Simón Bolivar, esquina	Mira	2280452	S/E	acadena@mira.gob.ec
10	LARA BORJA BYRON IVAN	CONCEJAL	ADMINISTRACION GENERAL	Eloy Alfaro y Simón Bolivar, esquina	Mira	2280452	S/E	ilara@mira.gob.ec
11	LARA CALDERON MARIA BARBARITA	CONCEJAL	ADMINISTRACION GENERAL	Eloy Alfaro y Simón Bolivar, esquina	Mira	2280452	S/E	blara@mira.gob.ec
12	TOBAR LOPEZ HAROL VINICIO	DIRECTOR FINANCIERO	ADMINISTRACION FINANCIERA	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	106	htobar@mira.gob.ec
13	GAON MONTENEGRO ADRIANA VANESSA	CONTADOR GENERAL	ADMINISTRACION FINANCIERA	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	109	agaon@mira.gob.ec
14	URRESTA ONOFRE VIRGINIA MARIOLA	JEFE DE PRESUPUESTO(E)	ADMINISTRACION FINANCIERA	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	109	vurresta@mira.gob.ec
15	MAFLA CLAVIJO CECILIA DEL CARMEN	TECNICO CONTADOR	ADMINISTRACION FINANCIERA	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	109	cmafla@mira.gob.ec
16	REINA PALMA MARIO ANDRES	TESORERÍA MUNICIPAL	ADMINISTRACION FINANCIERA	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	108	areina@mira.gob.ec
17	REYES ORQUERA YOLANDA TERESA	RECAUDADOR FISCAL	ADMINISTRACION FINANCIERA	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	S/E	treyes@mira.gob.ec
18	PUENTESTAR PALMA SONIA NARCISA	ASISTENTE ADMINISTRATIVO	ADMINISTRACION FINANCIERA	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	S/E	spuentestar@mira.gob.ec
19	GARRIDO ROMERO LIGIA MARLENE	TECNICO EN RENTAS	ADMINISTRACION FINANCIERA	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	S/E	mgarrido@mira.gob.ec
20	PEREZ JOAQUIN CELIANO	DIRECTOR ADMINISTRATIVO	DIRECCION ADMINISTRATIVA	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	116	jperez@mira.gob.ec
21	LARA CHIRIBOGA ANDRES ERNESTO	COORD. DE TALENTO HUMANO	DIRECCION ADMINISTRATIVA	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	116	alara@mira.gob.ec
22	PORTILLA ORTIZ MARIA ELISA	TECNICO DE TALENTO H.	DIRECCION ADMINISTRATIVA	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	116	mportilla@mira.gob.ec
23	VALLEJO VALLEJO JESICA PAMELA	TECN. COMPRAS PUBLICAS	DIRECCION ADMINISTRATIVA	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	106	pvallejo@mira.gob.ec
24	MADERA PADILLA JOSE ELIAS	AYUDANTE BODEGA	DIRECCION ADMINISTRATIVA	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	105	jmadera@mira.gob.ec
25	VINUEZA LARA WILSON MARCELO	POLICIA MUNICIPAL 1	DIRECCION ADMINISTRATIVA	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	S/E	wvinueza@mira.gob.ec
26	QUITAMA CHILES LUIS OSWALDO	POLICIA MUNICIPAL	DIRECCION ADMINISTRATIVA	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	S/E	oquitama@mira.gob.ec
27	PORTILLA MUÑOZ ALONSO FRANCISCO	INSPECTOR DE MERCADO ENC	DIRECCION ADMINISTRATIVA	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177		
28	PULE RUIZ HECTOR VICENTE	ASISTENTE ADMINISTRATIVO	DIRECCION ADMINISTRATIVA	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177		
29	URRESTA CABEZAS JAVIER REMIJUNDO	TECNICO EN SERVICIOS MUNICIP	DIRECCION ADMINISTRATIVA	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177		
30	MERA GARRIDO VILMA INES	TECNICO DE LA NIÑEZ Y ADOL.	DIRECCION ADMINISTRATIVA	Eloy Alfaro y Simón Bolivar, esquina	Mira	2280452		
31	PRADO BERNAL LADY CAROLINA	TECNICO DE LA NIÑEZ Y ADOL.	DIRECCION ADMINISTRATIVA	Eloy Alfaro y Simón Bolivar, esquina	Mira	2280452		

32	CAICEDO ALVAREZ HUGO ERNESTO	TECNICO DE LA NIÑEZ Y ADOL.	DIRECCION ADMINISTRATIVA	Eloy Alfaro y Simón Bolivar, esquina	Mira	2280452	S/E	hcaicedo@mira.gob.ec
33	PULE PUENTESTAR SULEMA CECILIA	AUXILIAR ADMINISTRATIVO	DIRECCION ADMINISTRATIVA	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	S/E	psulema@mira.gob.ec
34	JIMENEZ BORJA CARLOS MICHAEL	DIRECTOR DE PLANIFICACION	DIRECCION PLANIFICACION	Eloy Alfaro y Simón Bolivar, esquina	Mira	2280452	S/E	mjimenez@mira.gob.ec
35	HERRERA ARBOLEDA ARSENIO PATRICIO	PROFESIONAL 1 AVALUOS Y CAT.	DIRECCION PLANIFICACION	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	107	pherrera@mira.gob.ec
36	CONGO SUAREZ FREDDY ESTEBAN	ANALISTA PART. CIUDADANA	DIRECCION PLANIFICACION	Eloy Alfaro y Simón Bolivar, esquina	Mira	2280452	S/E	fcongo@mira.gob.ec
37	BASTIDAS GORDON AUGUSTO DAMIAN	JEFE DE SISTEMAS INF.	DIRECCION PLANIFICACION	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	114	dbastidas@mira.gob.ec
38	MUÑOZ GUERRERO YOBANY FABRICIO	JEF.UNID. TRANSITO Y TRANS.	DIRECCION PLANIFICACION	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	110	ymuñoz@mira.gob.ec
39	TAPIA LOPEZ LAURA LIDIA	ASISTENTE ADMINISTRATIVO	DIRECCION PLANIFICACION	Eloy Alfaro y Simón Bolivar, esquina	Mira	2280246-2280177	S/E	ltapia@mira.gob.ec
40	REYES ORQUERA TEODORO DANIEL	DIRECTOR DE DESARROLLO SOCIAL	DESARROLLO SOCIAL	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	110	treyes@mira.gob.ec
41	CALAPI GRIJALVA MARIA LUCIA	ASISTENTE ADMINISTRATIVO	DESARROLLO SOCIAL	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	110	mcalapi@mira.gob.ec
42	CADENA MONCAYO WILSON JOAQUIN	TECNICO PROG. DE CULTURA	DESARROLLO SOCIAL	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	110	jcadena@mira.gob.ec
43	ORTEGA IMBAQUINGO PAOLA ELIZABETH	ESPECIALISTA PROMOCION SOCIAL	DESARROLLO SOCIAL	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	110	portega@mira.gob.ec
44	PINEDA PUETATE MARIA CUMANDA	ASISTENTE ADMINISTRATIVO	DESARROLLO SOCIAL	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	110	mpineda@mira.gob.ec
45	YEPEZ CAZAR FRANKLIN FERNANDO	MEDICO OCUPACIONAL DEL GAD MIRA	DESARROLLO SOCIAL	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	110	fyepez@mira.gob.ec
46	PADILLA MENDEZ DIEGO MAURICIO	DIR. DE OBRAS PUBLICAS E HIGIENE	DIRECCIÓN DE OBRAS PÚBLICAS	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	115	mpadilla@mira.gob.ec
47	BOLAÑOS VALLEJO LILIAN MERCEDES	ASISTENTE ADMINISTRATIVO	DIRECCIÓN DE OBRAS PÚBLICAS	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	104	lbolaños@mira.gob.ec
48	ANGULO SANAFRIA JOSE DANIEL	FISCALIZADOR DE OBRAS	DIRECCIÓN DE OBRAS PÚBLICAS	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	104	dangulo@mira.gob.ec
49	BASTIDAS MAFLA NELSON RENATO	TECNICO EN AGUA P.	DIRECCIÓN DE OBRAS PÚBLICAS	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	104	rbastidas@mira.gob.ec
50	MUÑOZ GUERRERO NELSON ORLANDO	ASISTENTE ADMINISTRATIVO	DIRECCIÓN DE OBRAS PÚBLICAS	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	104	omuñoz@mira.gob.ec
51	ESPAÑA MANOSALVAS EDWIN MIGUEL	DIRECTOR DE GESTION AMBIENTAL	GESTIÓN AMBIENTAL	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	110	eespaña@mira.gob.ec
52	ZAPATA MIÑO SULEMA DEL ROSARIO	AMBIENTE Y PRODUCTIVIDAD	GESTIÓN AMBIENTAL	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	110	szapata@mira.gob.ec
53	ULLOA URRESTA DANIEL SEBASTIAN	RESPONSABLE GESTION AMBIENTAL	GESTIÓN AMBIENTAL	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	110	sulloa@mira.gob.ec
54	MENDEZ VELEZ FRANKLIN MARCELO	TECNICO DE RIESGOS Y DESASTRES	GESTIÓN AMBIENTAL	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	110	mmendez@mira.gob.ec
55	GARRIDO TANICUCHI ANA LISETH	ASISTENTE ADMINISTRATIVO	DIRECCIÓN FINANCIERA	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	106	lgarrido@mira.gob.ec
56	BUITRON GOMEZ KATHERINE ELIZABETH	ASISTENTE ADMINISTRATIVO	DIRECCIÓN FINANCIERA	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	108	kbuitron@mira.gob.ec
57	ESPINOZA CHALA LENYN ALIRIO	COMISARIO MUNICIPAL	DIRECCION ADMINISTRATIVA	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	S/E	lespinoza@mira.gob.ec
58	VALLEJO CARRERA LENIN GABRIEL	GUARDARMACEN ENCARGADO	DIRECCION ADMINISTRATIVA	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	S/E	lvallejo@mira.gob.ec
59	ACOSTA PADILLA PATRICIA MERCEDES	ASISTENTE ADMINISTRATIVO	OTROS SERVICIOS COMUNALES	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	116	pacosta@mira.gob.ec
60	BRAVO MEJIA WILSON ALFREDO	TECNICO EN COACTIVAS	OTROS SERVICIOS COMUNALES	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	S/E	wbravo@mira.gob.ec
61	RAMIREZ CHICAIZA PABLO MARDOQUEO	AUXILIAR DE SERVICIOS MUNICIPALES	OTROS SERVICIOS COMUNALES	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177		
62	BASTIDAS RUIZ TULA GUADALUPE	AUX. SER. GENERALES	OTROS SERVICIOS COMUNALES	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177		
63	ORTEGA CAICEDO ANA CRISTINA	ASISTENTE ADMINIST	OTROS SERVICIOS COMUNALES	Eloy Alfaro y Simón Bolivar, esquina	Mira	2280246-2280177		
64	ESCOBAR GAON TANIA ALCIRA	COOR.PLAN.Y ORD. TERRIT	OTROS SERVICIOS COMUNALES	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177		
65	HERRERA ESPAÑA INDIRA YAJAIRA	ANALISTA DE PLANIFICACION	OTROS SERVICIOS COMUNALES	Eloy Alfaro y Simón Bolivar, esquina	Mira	2280452		

66	ANGULO PEREZ ALEXANDER	ASISTENTE DE SISTEMAS UTIC	OTROS SERVICIOS COMUNALES	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	114	aangulo@mira.gob.ec
67	LOPEZ JARAMILLO NELSON RAMIRO	TECNICO EN COMUNICACIÓN	OTROS SERVICIOS COMUNALES	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	S/E	nlopez@mira.gob.ec
68	VILLOTA CASANOVA ALEXANDER MAURICIO	JEFE DE COMUNICACIÓN	OTROS SERVICIOS COMUNALES	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	S/E	mvillota@gadmira.gob.ec
69	LOAIZA LARA DENISSE VERONICA	TECN. DE SEGUIMIENTO.Y EVALUACIÓN DE PROYECTOS	OTROS SERVICIOS COMUNALES	León Ruales y Gonzalez Suarez, esquina	Mira	2280452	S/E	dloaiza@gadmira.gob.ec
70	TOBAR RUIZ JORGE LUIS	TEC. EN MAN DEL SIST INF. GEOG.	OTROS SERVICIOS COMUNALES	León Ruales y Gonzalez Suarez, esquina	Mira	2280452	107	jtobar@gadmira.gob.ec
71	PALMA TANICUCHI WILMAN IGNACIO	TECNICO EN PROG. DEPORTIVA	OTROS SERVICIOS COMUNALES	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	110	wpalma@mira.gob.ec
72	RUALES MESA LUIS ENRIQUE	PROMOTOR DEPORTIVO	OTROS SERVICIOS COMUNALES	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	110	eruales@mira.gob.ec
73	MAFLA TOBAR CESAR FRANCISCO	TECNICO DE CULTURA	OTROS SERVICIOS COMUNALES	Caserío Santa Ana parroquia La Concepción)	Mira	2280246-2280177	S/E	cmafla@mira.gob.ec
74	ONOFRE YEPEZ SABINA ELIZABETH	TECNICO TUR. Y PATRIMONIO	OTROS SERVICIOS COMUNALES	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	110	sonofre@mira.gob.ec
75	CALDERON VALVERDE PABLO ISRAEL	TECNICO EDUCACION	OTROS SERVICIOS COMUNALES	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	110	pcalderon@mira.gob.ec
76	CHANDI CAMPOS HENRY RENATO	TECNICO DE TRASN,MTTO,MOV.	OTROS SERVICIOS COMUNALES	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	S/E	hchandi@mira.gob.ec
77	LAGUNA PEREZ EDWIN MARCELO	TOPOGRAFO	OTROS SERVICIOS COMUNALES	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	104	elaguna@mira.gob.ec
	PASTAZ POZO LUIS ANIBAL	AUXILIAR DE CONTROL D.P.D.R.AGUA P	OTROS SERVICIOS COMUNALES	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	S/E	apastaz@mira.gob.ec
	PINEDA CARANQUI SEGUNDO ATAHUALPA	POLICIA MUNICIPAL	OTROS SERVICIOS COMUNALES	León Ruales y Gonzalez Suarez, esquina	Mira	2280246-2280177	S/E	apineda@mira.gob.ec

RESPONSABLE DE LA UNIDAD POSEEDORA DE LA INFORMACIÓN DEL LITERAL b1):	ING. ANDRÉS LARA CHIRIBOGA
CORREO ELECTRÓNICO DEL O LA RESPONSABLE DE LA UNIDAD POSEEDORA DE LA INFORMACIÓN:	alara@mira.gob.ec
NÚMERO TELEFÓNICO DEL O LA RESPONSABLE DE LA UNIDAD POSEEDORA DE LA INFORMACIÓN:	(02) 280246-2280177 EXTENSIÓN 116 (Número de teléfono y extensión)

Anexo 10.- Solicitud de acceso a la información pública del GADM del Cantón Mira



Gobierno Autónomo Descentralizado del Cantón Mira

ALCALDÍA Mira ADMINISTRACIÓN 2014 - 2019 Un cantón que avanza

SOLICITUD DE ACCESO A LA INFORMACION PÚBLICA

Fecha: (sistema/automático)

Ciudad: (sistema/automático)

Institución de la Función Ejecutiva: (sistema/automático)

Autoridad: (sistema/automático)

IDENTIFICACIÓN DEL SOLICITANTE

Nombre: Apellido:

Cédula No.

Dirección domiciliaria:

Teléfono (fijo o celular):

PETICIÓN CONCRETA:

Identifique de manera clara y concreta la información pública que desea solicitar a la institución:

FORMA DE RECEPCIÓN DE LA INFORMACIÓN SOLICITADA:

Retiro de la información en la institución:

Email:

FORMATO DE ENTREGA:

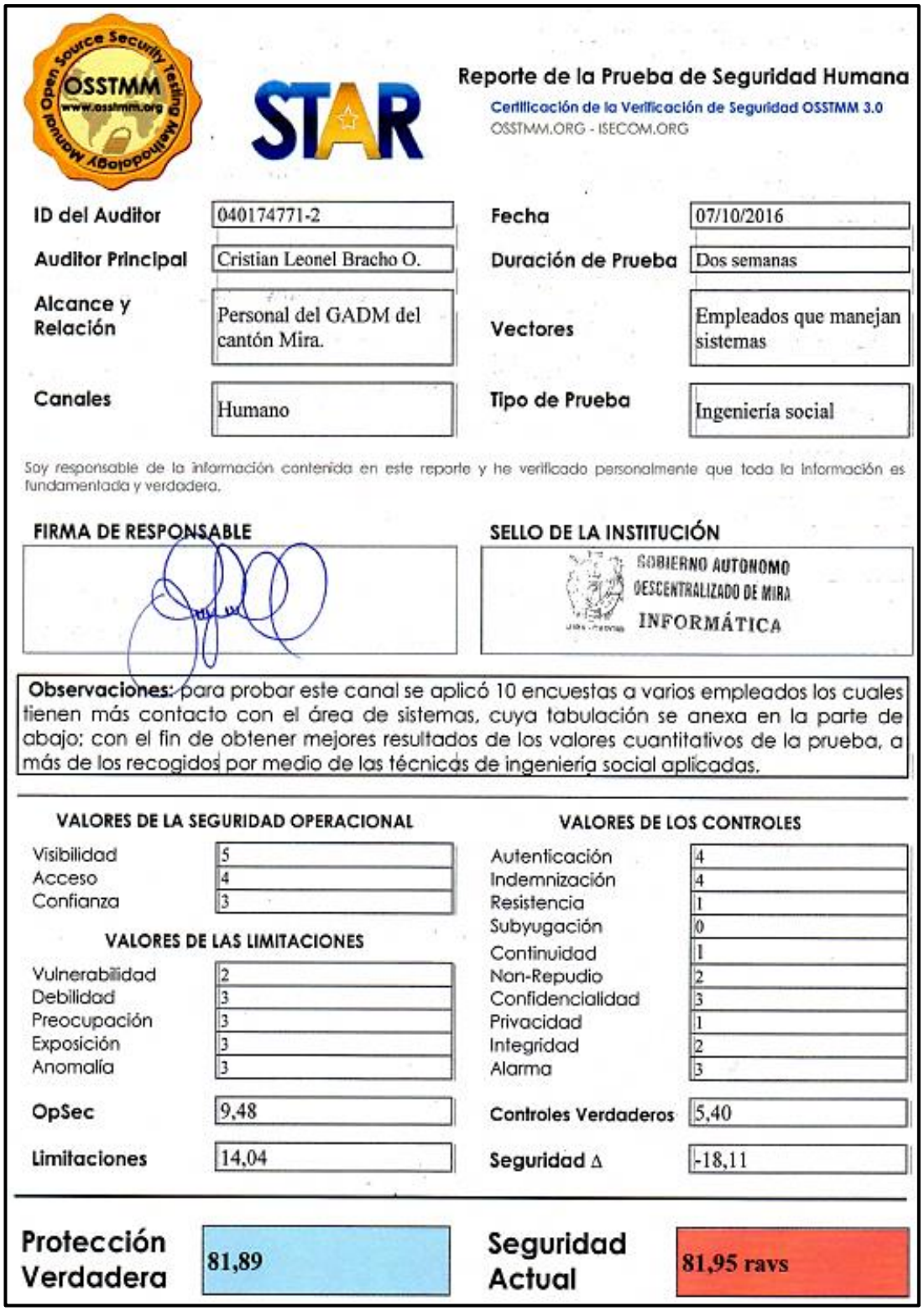
Copia en papel: CD:

Formato electrónico digital: PDF

Word Excel Otros

1 de 1 GAD DEL CANTÓN MIRA Solicitud de Acceso a la Información Pública

Anexo 11.- Reporte canal Humano del GADM del Cantón Mira



Reporte de la Prueba de Seguridad Humana

Certificación de la Verificación de Seguridad OSSTMM 3.0

OSSTMM.ORG - ISECOM.ORG

ID del Auditor	040174771-2	**Fecha**	07/10/2016
Auditor Principal	Cristian Leonel Bracho O.	**Duración de Prueba**	Dos semanas
Alcance y Relación	Personal del GADM del cantón Mira.	**Vectores**	Empleados que manejan sistemas
Canales	Humano	**Tipo de Prueba**	Ingeniería social

Soy responsable de la información contenida en este reporte y he verificado personalmente que toda la información es fundamentada y verdadera.

FIRMA DE RESPONSABLE

SELLO DE LA INSTITUCIÓN

GOBIERNO AUTONOMO DESCENTRALIZADO DE MIRA

INFORMÁTICA

Observaciones: para probar este canal se aplicó 10 encuestas a varios empleados los cuales tienen más contacto con el área de sistemas, cuya tabulación se anexa en la parte de abajo; con el fin de obtener mejores resultados de los valores cuantitativos de la prueba, a más de los recogidos por medio de las técnicas de ingeniería social aplicadas.

VALORES DE LA SEGURIDAD OPERACIONAL

Visibilidad	5
Acceso	4
Confianza	3

VALORES DE LAS LIMITACIONES

Vulnerabilidad	2
Debilidad	3
Preocupación	3
Exposición	3
Anomalía	3

VALORES DE LOS CONTROLES

Autenticación	4
Indemnización	4
Resistencia	1
Subyugación	0
Continuidad	1
Non-Repudio	2
Confidencialidad	3
Privacidad	1
Integridad	2
Alarma	3

OpSec	9,48	**Controles Verdaderos**	5,40
Limitaciones	14,04	**Seguridad Δ**	-18,11

Protección Verdadera	81,89	**Seguridad Actual**	81,95 ravs

UNIVERSIDAD TÉCNICA DEL NORTE

TABULACIÓN DE ENCUESTA SOBRE SEGURIDAD DE TECNOLOGÍAS DE LA INFORMACIÓN

La información obtenida en esta encuesta es estrictamente de uso estadístico para un estudiante de la Universidad Técnica del Norte que está realizando su trabajo de grado en el GAD Mira y no tendrá ninguna influencia en su aspecto laboral, por lo que se le pide de la manera más comedida que conteste con total honestidad.

Objetivo: La presente encuesta tiene como finalidad, realizar una prueba de seguridad de la información relacionada con el aspecto humano, a más de evaluar el grado de conocimiento sobre dichos temas por parte del personal de Gobierno Autónomo Descentralizado del Cantón Mira.

PREGUNTAS	RESPUESTAS		
	SÍ	NO	N/A
1. ¿Ha sufrido accidentalmente pérdida de información en su estación de trabajo?	6	4	0
2. ¿Conoce si alguna persona ha divulgado información personal o privada dentro o fuera de su estación de trabajo?	1	9	0
3. ¿Alguien diferente a usted ha insertado una **Flash Memory** en su ordenador o PC?	7	3	0
4. ¿Separa la información ya sea en forma digital o física, dependiendo de su grado de importancia?	10	0	0
5. ¿Existe un protocolo o procedimiento que le ayude al manejo de información privada o restringida?	3	7	0
6. ¿Alguna vez se le ha perdido algún dispositivo de almacenamiento con información de su trabajo?	4	6	0
7. ¿Ha escuchado alguna vez sobre el término "**encriptación**" de la información?	2	8	0
8. ¿En alguna ocasión se ha olvidado de cerrar la sesión en alguna aplicación que maneje en su ordenador o PC?	7	3	0
9. Cuando no se encuentra en su lugar de trabajo, ¿su ordenador permanece encendido?	7	3	0
10. ¿Alguna vez ha intentado ingresar a archivos o documentos para los cuales no tiene permiso?	1	9	0
11. Al finalizar sus labores diarias, ¿apaga su ordenador o PC?	10	0	0
12. ¿Comunica al departamento de sistemas por algún mensaje de error al ejecutar una aplicación?	10	0	0
13. ¿Existe algún método que le garantice que solo ud. tiene acceso a su estación de trabajo?	5	4	1
14. ¿Ha intentado ingresar a otras cuentas de usuario, a las que no tiene acceso?	0	10	0

15. ¿Cree usted que la información del GAD, incluyendo la suya, se encuentra totalmente segura?	3	7	0
16. ¿Comparte información con otros departamentos mediante una carpeta compartida?	3	7	0
17. ¿Realiza frecuentemente cambios de claves a su ordenador o PC y aplicaciones que utiliza regularmente?	2	8	0
18. ¿Realiza búsquedas de información en la Internet por medio de navegadores como Google en su ordenador?	10	0	0
19. ¿Realiza respaldos de información importante en dispositivos de almacenamiento como Flash Memory u otros?	7	3	0
20. Cuando comparte información con otro departamento, ¿está totalmente segur@ de que la información la recibió la persona a la que iba dirigida?	7	2	1
21. ¿Alguna vez ha notado que la información que ud. maneja en su estación de trabajo ha sido total o parcialmente modificada?	3	7	0
22. ¿Se realiza un mantenimiento oportuno de su ordenador de trabajo por parte del área de sistemas?	6	4	0
23. En los últimos 6 meses, ¿le han cambiado de ordenador por algún motivo?	0	10	0
24. ¿Su ordenador posee un antivirus actualizado?	7	3	0
25. ¿Alguna vez se le han mostrado alertas del antivirus en su ordenador?	10	0	0
26. ¿Cree usted que la información que maneja en su ordenador está completamente segura?	4	6	0
27. A parte de usted, ¿Alguna otra persona conoce su contraseña de acceso a su ordenador o aplicaciones?	3	7	0
28. En los últimos 6 meses, ¿ha recibido alguna capacitación para el mejor uso de las aplicaciones que posee en su ordenador?	0	10	0
29. ¿Ha guardado archivos o documentos importantes para llevarlos fuera del GAD como en CD, DVD, Flash Memory, u otros?	5	5	0
30. ¿Usa la misma clave para acceder a sus aplicaciones?	7	3	0
31. ¿En sus contraseñas incluye palabras como los nombres de sus hijos, el de su esposo, el suyo, direcciones de domicilio, o algo parecido?	5	5	0
32. ¿Comparte información de su trabajo por una cuenta de correo electrónico personal como Hotmail, Gmail, u otros?	8	2	0
33. ¿Posee acceso a la Internet desde su puesto de trabajo?	10	0	0
34. ¿Conoce cómo crear una contraseña segura para acceder a las aplicaciones?	3	7	0
35. ¿Hace uso de aplicaciones de mensajería instantánea como Whatsapp, Messenger, etc., para enviar información confidencial?	4	6	0
36. ¿Existe algún método de alarma que le informe cuando alguien ha tratado de acceder a su ordenador o aplicaciones?	0	10	0

37. ¿Guarda en su celular información personal como contraseñas, nombres de usuario, etc.?	**1**	**9**	**0**
38. ¿Comparte información importante con otros departamentos por medio de una llamada telefónica?	**5**	**5**	**0**
39. ¿En alguna ocasión se ha olvidado su celular en su estación de trabajo?	**5**	**5**	**5**
40. ¿Ha escuchado alguna vez sobre los términos "**cifrado de datos**"?	**1**	**9**	**0**
41. ¿Confía en el personal de seguridad del GAD?	**5**	**5**	**0**
42. ¿El personal de seguridad del GAD prohíbe el acceso a personas desconocidas a áreas restringidas dentro del GAD?	**5**	**5**	**0**
43. ¿Conoce si existe algún tipo de acción legal para las personas que intentaron robar su información personal para fines delictivos?	**0**	**10**	**0**
44. ¿Asume la responsabilidad por la pérdida de información importante para GAD por parte suya?	**3**	**7**	**0**
45. ¿Confía en el personal del área de sistemas?	**9**	**1**	**0**
46. ¿Conoce si se maneja un inventario de los activos del GAD a los que usted tiene acceso?	**3**	**7**	**0**
47. ¿Sabe si su ordenador puede ser manipulado de manera remota, es decir que no exista la necesidad de que una persona este físicamente en el sitio donde se encuentra el mismo?	**3**	**7**	**0**
48. Por cualquier motivo, ¿su estación de trabajo ha sido temporalmente sustituida por otra persona ajena al GAD?	**1**	**9**	**0**
49. ¿En su ordenador existe algún tipo de carpeta a la cual no tiene acceso?	**0**	**10**	**0**
50. ¿Maneja alguna cuenta de correo electrónico empresarial?	**4**	**6**	**0**

LISTA DE VERIFICACIÓN

Dirigida a: Talento Humano del GADM del Cantón Mira

Ítem/s inspeccionado/s: Personal de planta central del GADM	Fecha: 20/09/2016
Tipo de prueba: Observación y Persuasión	Auditor: Cristian Leonel Bracho Ortega
Firma del representante: 	Sello de la institución: GOBIERNO AUTONOMO DESCENTRALIZADO DE MIRA INFORMÁTICA

1. Seguridad Operacional		
a)	El personal del Área de Sistemas está autorizado a acceder al Cuarto de Comunicaciones	☒ SI ☐ NO
b)	El personal del Área de Comunicación está autorizado a acceder al Cuarto de Comunicaciones	☐ SI ☒ NO
c)	El personal de la Dirección de Planificación está autorizado a acceder al Cuarto de Comunicaciones	☐ SI ☒ NO
d)	El personal de la Secretaría General está autorizado a acceder al Cuarto de Comunicaciones	☐ SI ☒ NO
e)	El personal del Área Financiera está autorizado a acceder al Cuarto de Comunicaciones	☐ SI ☒ NO
f)	El personal de seguridad (guardianía) puede acceder al Cuarto de Comunicaciones	☒ SI ☐ NO

2. Controles		
a)	El personal de recepción lleva un registro de acceso en la entrada principal	☐ SI ☒ NO
b)	Para interactuar con el personal de recepción se necesita registrarse por medio del biométrico	☒ SI ☐ NO
c)	El Director del Área de Sistemas accede a los activos del Cuarto de comunicaciones del GADM	☒ SI ☐ NO
d)	La ausencia de los Directores Departamentales genera conflictos dentro del GADM	☒ SI ☐ NO
e)	El personal de recepción de la planta central del GADM genera registros de acceso	☐ SI ☒ NO
f)	Las comunicaciones a través de líneas seguras son eficientes	☒ SI ☐ NO
g)	Las comunicaciones a través de documentos físicos son eficientes	☐ SI ☒ NO
h)	Las propiedades transportadas utilizando firmas individuales dentro del GADM es eficiente	☐ SI ☒ NO
i)	Los activos informáticos del GADM transportados por un canal mediante procesos documentados es eficiente	☐ SI ☒ NO
j)	El servicio de antivirus genera alarmas en los ordenadores del GADM	☒ SI ☐ NO
k)	Se utilizan sistemas de advertencia y registros dentro de la planta central del GADM	☐ SI ☒ NO

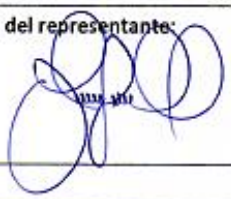
3. Limitaciones		
a)	Se puede obtener información privada del personal del GADM a través de la Ley de acceso a la información pública	☒ SI ☐ NO
b)	El personal que se integra a nuevos cargos entrega información de uso interno del GADM	☒ SI ☐ NO

c)	El personal permite que terceras personas inserten dispositivos de almacenamiento externo en sus ordenadores	☒ SI ☐ NO
d)	El personal cierra las sesiones en sus ordenadores cuando no se encuentran en sus estaciones de trabajo	☐ SI ☒ NO
e)	Se entrega información sobre el personal que se ausenta del GADM por cualquier motivo	☒ SI ☐ NO
f)	Los directores departamentales extraen documentos fuera del GADM	☒ SI ☐ NO
g)	El personal ha perdido información de su estación de trabajo accidentalmente	☒ SI ☐ NO
h)	El personal se incomoda con la presencia del auditor dentro del GADM	☒ SI ☐ NO

Observaciones

LISTA DE VERIFICACIÓN

Dirigida a: Talento Humano del GADM del Cantón Mira

Ítem/s inspeccionado/s: Personal de planta central del GADM	Fecha: 23/09/2016
Tipo de prueba: Observación y Persuasión	Auditor: Cristian Leonel Bracho Ortega
Firma del representante: 	Sello de la institución: GOBIERNO AUTONOMO DESCENTRALIZADO DE MIRA INFORMÁTICA

1. Seguridad Operacional		
a)	El personal del Área de Sistemas está autorizado a acceder al Cuarto de Comunicaciones	[X] SI [ ] NO
b)	El personal del Área de Comunicación está autorizado a acceder al Cuarto de Comunicaciones	[X] SI [ ] NO
c)	El personal de la Dirección de Planificación está autorizado a acceder al Cuarto de Comunicaciones	[X] SI [ ] NO
d)	El personal de la Secretaría General está autorizado a acceder al Cuarto de Comunicaciones	[X] SI [ ] NO
e)	El personal del Área Financiera está autorizado a acceder al Cuarto de Comunicaciones	[X] SI [ ] NO
f)	El personal de seguridad (guardianía) puede acceder al Cuarto de Comunicaciones	[X] SI [ ] NO

2. Controles		
a)	El personal de recepción lleva un registro de acceso para las oficinas de servicio a la ciudadanía	[ ] SI [X] NO
b)	Para interactuar con el personal de recepción se necesita manejar algún tipo de sistema o aplicación del GADM	[X] SI [ ] NO
c)	El personal de Seguridad accede a los activos del Cuarto de comunicaciones del GADM	[ ] SI [X] NO
d)	La ausencia de las Secretarias genera conflictos dentro del GADM	[ ] SI [X] NO
e)	El personal de recepción del Ex Patronato Municipal genera registros de acceso	[ ] SI [X] NO
f)	Las comunicaciones que utilizan encriptación son eficientes	[X] SI [ ] NO
g)	Las comunicaciones a través de los servicios de mensajería instantánea son eficientes	[ ] SI [X] NO
h)	Las propiedades transportadas utilizando identificaciones personales dentro del GADM es eficiente	[ ] SI [X] NO
i)	Los activos informáticos del GADM transportados por un canal haciendo uso del cifrado de datos es eficiente	[ ] SI [X] NO
j)	El servicio de antivirus genera alarmas en los ordenadores del GADM	[X] SI [ ] NO
k)	Se utilizan sistemas de advertencia y registros dentro de la planta central del GADM	[ ] SI [X] NO

3. Limitaciones	
a) Se puede obtener información privada del personal del GADM a través de la Ley de acceso a la información pública	☒ SI ☐ NO
b) El personal que se integra a nuevos cargos entrega información de uso interno del GADM	☐ SI ☒ NO
c) El personal permite que terceras personas inserten dispositivos de almacenamiento externo en sus ordenadores	☐ SI ☒ NO
d) El personal cierra las sesiones en sus ordenadores cuando no se encuentran en sus estaciones de trabajo	☒ SI ☐ NO
e) Se entrega información sobre el personal que se ausenta del GADM por cualquier motivo	☒ SI ☐ NO
f) Los directores departamentales extraen documentos fuera del GADM	☒ SI ☐ NO
g) El personal ha perdido información de su estación de trabajo accidentalmente	☐ SI ☒ NO
h) El personal se incomoda con la presencia del auditor dentro del GADM	☐ SI ☒ NO

Observaciones

LISTA DE VERIFICACIÓN

Dirigida a: Talento Humano del GADM del Cantón Mira

Ítem/s inspeccionado/s: Personal de planta central del GADM	Fecha: 26/09/2016
Tipo de prueba: Observación y Persuasión	Auditor: Cristian Leonel Bracho Ortega
Firma del representante: 	Sello de la institución: GOBIERNO AUTONOMO DESCENTRALIZADO DE MIRA INFORMÁTICA

1. Seguridad Operacional		
a)	El personal del Área de Sistemas está autorizado a acceder al Cuarto de Comunicaciones	☒ SI ☐ NO
b)	El personal del Área de Comunicación está autorizado a acceder al Cuarto de Comunicaciones	☒ SI ☐ NO
c)	El personal de la Dirección de Planificación está autorizado a acceder al Cuarto de Comunicaciones	☒ SI ☐ NO
d)	El personal de la Secretaría General está autorizado a acceder al Cuarto de Comunicaciones	☐ SI ☒ NO
e)	El personal del Área Financiera está autorizado a acceder al Cuarto de Comunicaciones	☒ SI ☐ NO
f)	El personal de seguridad (guardianía) puede acceder al Cuarto de Comunicaciones	☒ SI ☐ NO

2. Controles		
a)	El personal de recepción lleva un registro de acceso para las bodegas del GADM	☐ SI ☒ NO
b)	Para interactuar con el personal de recepción se necesita tener un oficio dirigido hacia el Sr. Alcalde	☒ SI ☐ NO
c)	El personal de la Secretaría General accede a los activos del Cuarto de comunicaciones del GADM	☐ SI ☒ NO
d)	La ausencia de los Guardias genera conflictos dentro del GADM	☐ SI ☒ NO
e)	El personal de recepción de los Garajes del GADM llevan registros de acceso	☐ SI ☒ NO
f)	Las comunicaciones que se llevan a cabo a través del correo electrónico institucional son eficientes	☒ SI ☐ NO
g)	Las propiedades transportadas a través de interacciones personales dentro del GADM es método eficiente	☒ SI ☐ NO
h)	Los activos informáticos del GADM transportados por un canal haciendo uso de la encriptación de datos es eficiente	☒ SI ☐ NO
i)	El servicio de antivirus genera alarmas en los ordenadores del GADM	☒ SI ☐ NO
j)	Se utilizan sistemas de advertencia y registros dentro de la planta central del GADM	☐ SI ☒ NO

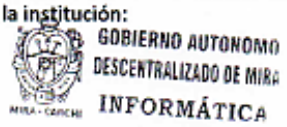
3. Limitaciones		
a)	Se puede obtener información privada del personal del GADM a través de la Ley de acceso a la información pública	☒ SI ☐ NO

b)	El personal que se integra a nuevos cargos entrega información de uso interno del GADM	☒ SI ☐ NO
c)	El personal permite que terceras personas inserten dispositivos de almacenamiento externo en sus ordenadores	☒ SI ☐ NO
d)	El personal cierra las sesiones en sus ordenadores cuando no se encuentran en sus estaciones de trabajo	☐ SI ☒ NO
e)	Se entrega información sobre el personal que se ausenta del GADM por cualquier motivo	☒ SI ☐ NO
f)	Los directores departamentales extraen documentos fuera del GADM	☒ SI ☐ NO
g)	El personal ha perdido información de su estación de trabajo accidentalmente	☒ SI ☐ NO
h)	El personal se incomoda con la presencia del auditor dentro del GADM	☒ SI ☐ NO

Observaciones

LISTA DE VERIFICACIÓN

Dirigida a: Talento Humano del GADM del Cantón Mira

Ítem/s inspeccionado/s: Personal de planta central del GADM	Fecha: 28/09/2016
Tipo de prueba: Observación y Persuasión	Auditor: Cristian Leonel Bracho Ortega
Firma del representante: 	Sello de la institución: 

1. Seguridad Operacional	
a) El personal del Área de Sistemas está autorizado a acceder al Cuarto de Comunicaciones	☒ SI ☐ NO
b) El personal del Área de Comunicación está autorizado a acceder al Cuarto de Comunicaciones	☒ SI ☐ NO
c) El personal de la Dirección de Planificación está autorizado a acceder al Cuarto de Comunicaciones	☒ SI ☐ NO
d) El personal de la Secretaría General está autorizado a acceder al Cuarto de Comunicaciones	☐ SI ☒ NO
e) El personal del Área Financiera está autorizado a acceder al Cuarto de Comunicaciones	☒ SI ☐ NO
f) El personal de seguridad (guardianía) puede acceder al Cuarto de Comunicaciones	☒ SI ☐ NO

2. Controles	
a) El personal de recepción lleva un registro de acceso para las áreas restringidas del GADM	☐ SI ☒ NO
b) Para interactuar con el personal de recepción se necesita registrarse por medio del biométrico	☒ SI ☐ NO
c) Para interactuar con el personal de recepción se necesita manejar algún tipo de sistema o aplicación del GADM	☒ SI ☐ NO
d) Para interactuar con el personal de recepción se necesita tener un oficio dirigido hacia el Sr. Alcalde	☒ SI ☐ NO
e) El personal de la Secretaría Financiera accede a los activos del Cuarto de comunicaciones del GADM	☐ SI ☒ NO
f) La ausencia del Personal de apoyo genera conflictos dentro del GADM	☐ SI ☒ NO
g) El personal de recepción del Centro Gerontológico llevan registros de acceso	☒ SI ☐ NO
h) Las comunicaciones que se llevan a cabo a través del susurro son eficientes	☐ SI ☒ NO
i) Las comunicaciones que se llevan a cabo a través de la comunicación verbal directa son eficientes	☐ SI ☒ NO
j) Las propiedades transportadas a través de interacciones personales dentro del GADM es método eficiente	☒ SI ☐ NO
k) Los activos informáticos del GADM transportados por un canal haciendo uso de firmas es eficiente	☐ SI ☒ NO
l) El servicio de antivirus genera alarmas en los ordenadores del GADM	☒ SI ☐ NO
m) Se utilizan sistemas de advertencia y registros dentro de la planta central del GADM	☐ SI ☒ NO

n)	Se utiliza un sistema de alarma sonora dentro de la planta central del GADM	☒ SI ☐ NO
o)	Se hace uso de un sistema de alarma basada en el envío de mensajes personales	☒ SI ☐ NO
p)	Para interactuar con el personal de recepción se necesita acceder por las oficinas externas del GADM	☐ SI ☒ NO
q)	Para interactuar con el personal de recepción se necesita hacer uso de claves de acceso para las aplicaciones	☐ SI ☒ NO

3. Limitaciones		
a)	Se puede obtener información privada del personal del GADM a través de la Ley de acceso a la información pública	☒ SI ☐ NO
b)	El personal que se integra a nuevos cargos entrega información de uso interno del GADM	☒ SI ☐ NO
c)	El personal permite que terceras personas inserten dispositivos de almacenamiento externo en sus ordenadores	☒ SI ☐ NO
d)	El personal cierra las sesiones en sus ordenadores cuando no se encuentran en sus estaciones de trabajo	☐ SI ☒ NO
e)	Se entrega información sobre el personal que se ausenta del GADM por cualquier motivo	☒ SI ☐ NO
f)	Los directores departamentales extraen documentos fuera del GADM	☒ SI ☐ NO
g)	El personal ha perdido información de su estación de trabajo accidentalmente	☒ SI ☐ NO
h)	El personal se incomoda con la presencia del auditor dentro del GADM	☒ SI ☐ NO

Observaciones

LISTA DE VERIFICACIÓN

Dirigida a: Talento Humano del GADM del Cantón Mira

Ítem/s inspeccionado/s: Personal de planta central del GADM	Fecha: 30/09/2016
Tipo de prueba: Observación y Persuasión	Auditor: Cristian Leonel Bracho Ortega
Firma del representante: 	Sello de la institución: GOBIERNO AUTONOMO DESCENTRALIZADO DE MIRA INFORMÁTICA

1. Seguridad Operacional		
a)	El personal del Área de Sistemas está autorizado a acceder al Cuarto de Comunicaciones	☒ SI ☐ NO
b)	El personal del Área de Comunicación está autorizado a acceder al Cuarto de Comunicaciones	☒ SI ☐ NO
c)	El personal de la Dirección de Planificación está autorizado a acceder al Cuarto de Comunicaciones	☒ SI ☐ NO
d)	El personal de la Secretaría General está autorizado a acceder al Cuarto de Comunicaciones	☒ SI ☐ NO
e)	El personal del Área Financiera está autorizado a acceder al Cuarto de Comunicaciones	☒ SI ☐ NO
f)	El personal de seguridad (guardianía) puede acceder al Cuarto de Comunicaciones	☒ SI ☐ NO

2. Controles		
a)	El personal de recepción lleva un registro de acceso en la entrada principal	☐ SI ☒ NO
b)	El personal de recepción lleva un registro de acceso para las oficinas de servicio a la ciudadanía	☐ SI ☒ NO
c)	El personal de recepción lleva un registro de acceso para las bodegas	☐ SI ☒ NO
d)	El personal de recepción lleva un registro de acceso para las áreas restringidas	☐ SI ☒ NO
e)	Para interactuar con el personal de recepción se necesita registrarse por medio del biométrico	☒ SI ☐ NO
f)	Para interactuar con el personal de recepción se necesita manejar algún tipo de sistema o aplicación del GADM	☒ SI ☐ NO
g)	Para interactuar con el personal de recepción se necesita tener un oficio dirigido hacia el Sr. Alcalde	☒ SI ☐ NO
h)	El personal del Área de Comunicación accede a los activos del Cuarto de comunicaciones del GADM	☐ SI ☒ NO
i)	La ausencia de los Directores Departamentales genera conflictos dentro del GADM	☒ SI ☐ NO
j)	La ausencia de las Secretarias genera conflictos dentro del GADM	☐ SI ☒ NO
k)	La ausencia de los Guardias genera conflictos dentro del GADM	☐ SI ☒ NO
l)	La ausencia del Personal de apoyo genera conflictos dentro del GADM	☐ SI ☒ NO
m)	El personal de recepción del Complejo Deportivo del GADM genera registros de acceso	☒ SI ☐ NO

n)	Se utiliza un sistema de alarma sonora dentro de la planta central del GADM	☒ SI ☐ NO
o)	Se hace uso de un sistema de alarma basada en el envío de mensajes personales	☒ SI ☐ NO
p)	Para interactuar con el personal de recepción se necesita hacer uso de claves de acceso para las aplicaciones	☐ SI ☒ NO
q)	Para interactuar con el personal de recepción se necesita acceder por las oficinas externas del GADM	☐ SI ☒ NO
r)	Las comunicaciones a través de la central telefónica del GADM son eficientes	☐ SI ☒ NO
s)	Los activos informáticos del GADM transportados por un canal mediante sellos es eficiente	☒ SI ☐ NO
t)	El servicio de antivirus genera alarmas en los ordenadores del GADM	☒ SI ☐ NO
u)	Se utilizan sistemas de advertencia y registros dentro de la planta central del GADM	☐ SI ☒ NO

3. Limitaciones		
a)	Se puede obtener información privada del personal del GADM a través de la Ley de acceso a la información pública	☒ SI ☐ NO
b)	El personal que se integra a nuevos cargos entrega información de uso interno del GADM	☒ SI ☐ NO
c)	El personal permite que terceras personas inserten dispositivos de almacenamiento externo en sus ordenadores	☒ SI ☐ NO
d)	El personal cierra las sesiones en sus ordenadores cuando no se encuentran en sus estaciones de trabajo	☐ SI ☒ NO
e)	Se entrega información sobre el personal que se ausenta del GADM por cualquier motivo	☒ SI ☐ NO
f)	Los directores departamentales extraen documentos fuera del GADM	☒ SI ☐ NO
g)	El personal ha perdido información de su estación de trabajo accidentalmente	☒ SI ☐ NO
h)	El personal se incomoda con la presencia del auditor dentro del GADM	☒ SI ☐ NO

Observaciones

LISTA DE VERIFICACIÓN

Dirigida a: Talento Humano del GADM del Cantón Mira

Ítem/s inspeccionado/s: Personal de planta central del GADM	Fecha: 21/09/2016
Tipo de prueba: Llamada telefónica falsa	Auditor: Cristian Leonel Bracho Ortega
Firma del representante: 	Sello de la institución: GOBIERNO AUTONOMO DESCENTRALIZADO DE MIRA INFORMÁTICA

1. Seguridad Operacional	
a) El personal del Área de Sistemas necesita de una credencial para acceder a las Áreas restringidas del GADM	☒ SI ☐ NO
b) El personal del Área de Sistemas necesita de una credencial para acceder a las estaciones de trabajo de sus compañeros	☒ SI ☐ NO
c) El personal del Área de Sistemas necesita de una credencial para acceder a los archivos físicos del GADM	☒ SI ☐ NO

2. Controles	
a) El personal del GADM tiene que someterse a acuerdos de responsabilidad	☒ SI ☐ NO
b) El personal del GADM tiene que someterse a acuerdos de confidencialidad e integridad de la información	☒ SI ☐ NO
c) Existen instructivos físicos para el manejo de los equipos del GADM	☐ SI ☒ NO
d) Existen instructivos en forma digital para el manejo de los equipos del GADM	☐ SI ☒ NO

Observaciones
-2-a- El personal que tiene que someterse a los acuerdos de responsabilidad son los que manejan sistemas.

LISTA DE VERIFICACIÓN

Dirigida a: Talento Humano del GADM del Cantón Mira

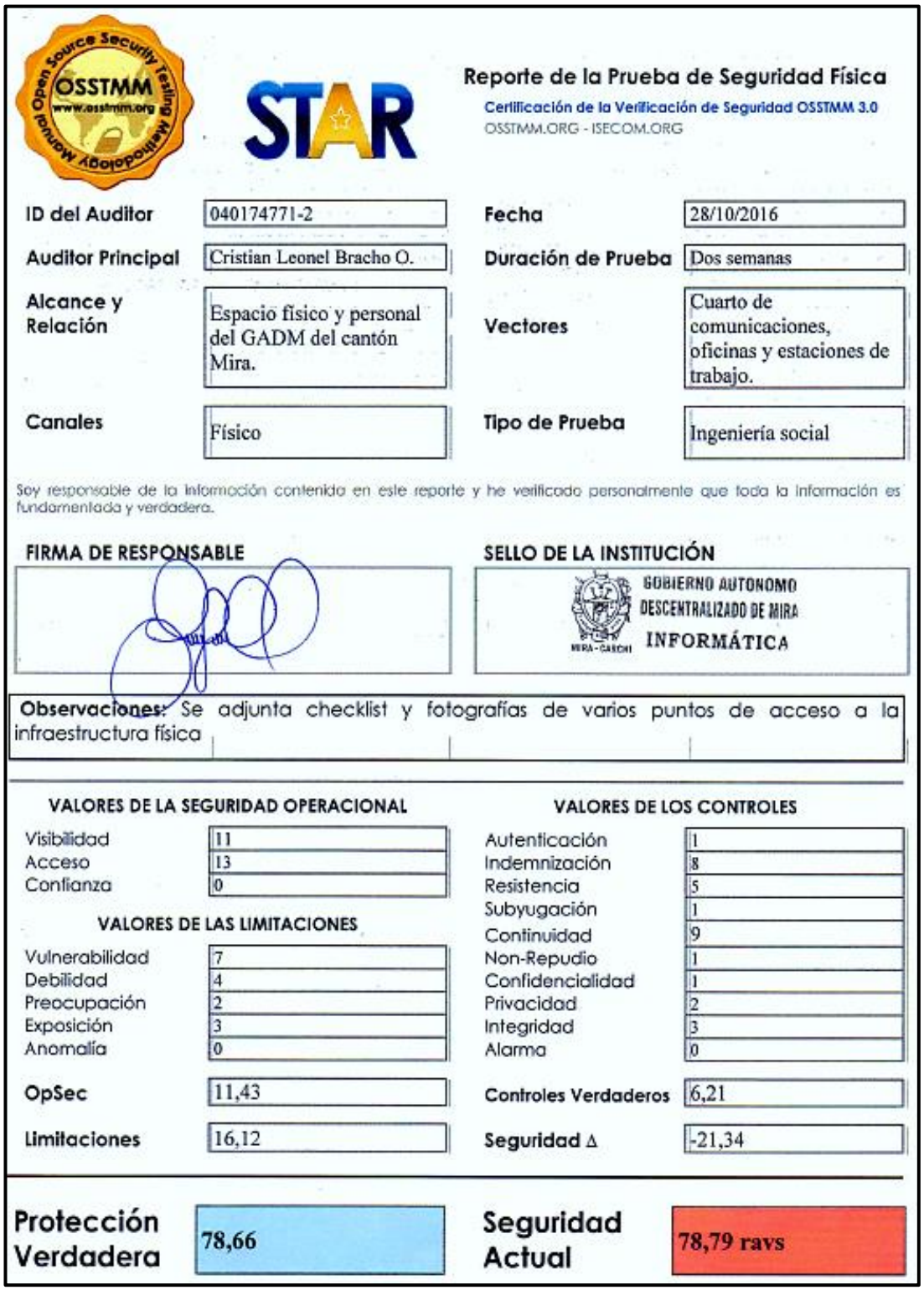
Ítem/s inspeccionado/s: Personal de planta central del GADM	Fecha: 29/09/2016
Tipo de prueba: Llamada telefónica falsa	Auditor: Cristian Leonel Bracho Ortega
Firma del representante: 	Sello de la institución: 

1. Seguridad Operacional		
a)	El personal de guardianía necesita de una credencial para acceder a las Áreas restringidas del GADM	☒ SI ☐ NO
b)	El personal de guardianía necesita de una credencial para acceder a las estaciones de trabajo de sus compañeros	☒ SI ☐ NO
c)	El personal de guardianía necesita de una credencial para acceder a los archivos físicos del GADM	☒ SI ☐ NO

2. Controles		
a)	El personal del GADM tiene que someterse a pólizas de seguros con empresas privadas	☒ SI ☐ NO
b)	El personal del GADM tiene que someterse a renuncias de usuario/uso	☒ SI ☐ NO
c)	Existen instructivos físicos para el manejo de los equipos del GADM	☐ SI ☒ NO
d)	Existen instructivos en forma digital para el manejo de los equipos del GADM	☐ SI ☒ NO

Observaciones

Anexo 12.- Reporte Canal Físico del GADM del Cantón Mira



Reporte de la Prueba de Seguridad Física

Certificación de la Verificación de Seguridad OSSTMM 3.0

OSSTMM.ORG - ISECOM.ORG

ID del Auditor	040174771-2	**Fecha**	28/10/2016
Auditor Principal	Cristian Leonel Bracho O.	**Duración de Prueba**	Dos semanas
Alcance y Relación	Espacio físico y personal del GADM del cantón Mira.	**Vectores**	Cuarto de comunicaciones, oficinas y estaciones de trabajo.
Canales	Físico	**Tipo de Prueba**	Ingeniería social

Soy responsable de la información contenida en este reporte y he verificado personalmente que toda la información es fundamentada y verdadera.

FIRMA DE RESPONSABLE

SELLO DE LA INSTITUCIÓN

GOBIERNO AUTONOMO DESCENTRALIZADO DE MIRA

MIRA - CARCHI

INFORMÁTICA

Observaciones: Se adjunta checklist y fotografías de varios puntos de acceso a la infraestructura física

VALORES DE LA SEGURIDAD OPERACIONAL

Visibilidad	11
Acceso	13
Confianza	0

VALORES DE LAS LIMITACIONES

Vulnerabilidad	7
Debilidad	4
Preocupación	2
Exposición	3
Anomalía	0

VALORES DE LOS CONTROLES

Autenticación	1
Indemnización	8
Resistencia	5
Subyugación	1
Continuidad	9
Non-Repudio	1
Confidencialidad	1
Privacidad	2
Integridad	3
Alarma	0

OpSec	11,43	**Controles Verdaderos**	6,21
Limitaciones	16,12	**Seguridad Δ**	-21,34

Protección Verdadera	78,66	**Seguridad Actual**	78,79 ravs

Las siguientes imágenes se muestran con el objetivo de exponer las debilidades en cuanto al acceso físico que existen en GADM-Mira. En la Imagen 1 se muestra una brecha que existe en la parte posterior de la planta central de la Institución por donde se puede acceder libremente, en la Imagen 2 se muestra la entrada anterior del GADM-Mira, en la Imagen 3 se muestra una de las entradas secundarias del GADM-Mira la cual permite el ingreso a ciertas áreas restringidas de la Institución y en la Imagen 4 se puede verificar que no existe ningún mecanismo de seguridad para el ingreso a las plantas superiores del GADM-Mira.

Imagen 1: Pared destruida por la que se puede acceder directamente al GADM

Imagen 2: Puerta de acceso Av. León Rúales

Imagen 3: Puerta de acceso calle Gonzáles Suárez

Imagen 4: Puerta de acceso a las plantas superiores del GADM

LISTA DE CHEQUEO

ACTIVOS FÍSICOS Y DE TELECOMUNICACIONES DEL GADM DEL CANTÓN MIRA

Ítem/s inspeccionado/s: Planta central y cuarto de comunicaciones del GADM	Fecha: 11/11/2016
Puntos chequeados: 1 ☒ 2 ☒ 3 ☒ 4 ☒	Auditor: Cristian Leonel Bracho Ortega
Firma del representante:	Sello de la institución: GOBIERNO AUTONOMO DESCENTRALIZADO DE MIRA INFORMÁTICA

1. Seguridad Operacional				
a)	Existen áreas de acceso público dentro de la planta central del GADM	☒ SI	☐ NO	☐ N/A
b)	Existen activos visibles fuera de la planta central del GADM	☒ SI	☐ NO	☐ N/A
c)	Existen normas de tráfico peatonal dentro del GADM	☒ SI	☐ NO	☐ N/A
d)	Existen dependencias fuera de la palnta central del GADM	☒ SI	☐ NO	☐ N/A
e)	Los directorios y direcciones del personal del GADM son de dominio público	☒ SI	☐ NO	☐ N/A
f)	El cuarto de comunicaciones del GADM se lo puede ubicar con facilidad	☐ SI	☒ NO	☐ N/A
g)	Existe un número aceptable de barreras físicas que protejan al cuarto de comunicaciones del GADM	☒ SI	☐ NO	☐ N/A
h)	Se tomo algún estándar de referencia para el diseño físico del cuarto de conumicaciones del GADM	☐ SI	☒ NO	☐ N/A
i)	Existe una sola vía de acceso para el cuarto de comunicaciones	☒ SI	☐ NO	☐ N/A
j)	De la siguiente lista, las barreras y obstáculos físicos del GADM permiten reducir:			
	• Calor	☒ SI	☐ NO	☐ N/A
	• Niveles altos de ruido	☒ SI	☐ NO	☐ N/A
	• Frío	☒ SI	☐ NO	☐ N/A
	• Humo	☒ SI	☐ NO	☐ N/A
	• Humedad	☒ SI	☐ NO	☐ N/A
	• Olores perjudiciales	☒ SI	☐ NO	☐ N/A
	• Campos magnéticos intensos	☐ SI	☒ NO	☐ N/A
	• Luz dañina	☒ SI	☐ NO	☐ N/A
	• Contaminantes	☐ SI	☒ NO	☐ N/A
k)	Para acceder a un área restringida del GADM se necesita de algún método de identificación	☐ SI	☒ NO	☐ N/A
l)	El personal de apoyo necesita algun tipo de credencial para tener acceso a los activos del GADM	☐ SI	☒ NO	☐ N/A

2. Controles				
a)	Existen privilegios para obtener acceso a los activos informáticos del GADM	☐ SI	☒ NO	☐ N/A
b)	Existe algún método de autenticación para los elementos que se pueden transportar dentro del GADM	☐ SI	☒ NO	☐ N/A
c)	Existe algún proceso de autenticación para objetos que van a ser extraídos fuera del GADM	☐ SI	☒ NO	☐ N/A
d)	Existen registros de los elementos que son introducidos y extraídos del GADM	☐ SI	☒ NO	☐ N/A

e)	De la siguiente lista, los empleados del GADM alguna vez han eludido:	
	• Políticas de los empleados _____	☒ SI ☐ NO ☐ N/A
	• Seguros obligatorios _____	☒ SI ☐ NO ☐ N/A
	• Acuerdos de no divulgación _____	☒ SI ☐ NO ☐ N/A
	• Contratos de responsabilidad _____	☒ SI ☐ NO ☐ N/A
	• Acuerdos de incompetencia _____	☐ SI ☐ NO ☒ N/A
	• Renuncias de uso/usuario	☐ SI ☐ NO ☒ N/A
f)	En la siguiente lista, dentro de la planta central del GADM se utilizan:	
	• Señales de advertencia de peligro _____	☒ SI ☐ NO ☐ N/A
	• Sistemas de vigilancia o alarmas _____	☒ SI ☐ NO ☐ N/A
	• Aviso de problemas de salud _____	☐ SI ☒ NO ☐ N/A
	• Avisos de entrada restringida	☒ SI ☐ NO ☐ N/A
g)	La inhabilitación o destrucción de los mecanismos de seguridad del GADM permiten el acceso oportuno a los activos procesos y operaciones	☒ SI ☐ NO ☐ N/A
h)	De la siguiente lista, la falta de qué elementos permiten el acceso directo a los activos u operaciones del GADM	
	• Combustible _____	☐ SI ☒ NO ☐ N/A
	• Energía eléctrica _____	☒ SI ☐ NO ☐ N/A
	• Alimentos _____	☒ SI ☐ NO ☐ N/A
	• Agua _____	☒ SI ☐ NO ☐ N/A
	• Comunicaciones	☐ SI ☒ NO ☐ N/A
i)	Existe algún plan de contingencia en caso de presentarse alguna amenaza catalogada como alta que permita que no se minimicen las medidas de seguridad operacional	☐ SI ☒ NO ☐ N/A
j)	Existen deficiencias en el acceso a los activos que no pueden ser monitoreados personalmente por el ente que genera el acceso, dentro del GADM	☒ SI ☐ NO ☐ N/A
k)	Existe personal de apoyo o algún medio automatizado que proporcione acceso en caso de alguna falla	☐ SI ☒ NO ☐ N/A
l)	El personal de recepción registra el acceso a los activos del GADM	☐ SI ☒ NO ☐ N/A
m)	La incapacidad para eliminar residuos y contaminantes dentro del GADM, detienen o impiden el acceso a los servicios, procesos y operaciones	☐ SI ☒ NO ☐ N/A
n)	De la siguiente lista, qué métodos se utilizan dentro del GADM para la asegurar el control de confidencialidad	
	• Códigos secretos _____	☐ SI ☒ NO ☐ N/A
	• Lenguaje indescifrable _____	☐ SI ☒ NO ☐ N/A
	• Interacciones personales a puerta cerrada	☒ SI ☐ NO ☐ N/A
o)	Se da algún tratamiento especial a los dispositivos de almacenamiento que sufren daños por causas naturales	☐ SI ☒ NO ☐ N/A
p)	Los dispositivos de almacenamiento de la información del GADM, tienen un lugar establecido para su archivación.	☐ SI ☒ NO ☐ N/A
q)	Dentro del GADM existe algún método que proteja los documentos en transporte para salvaguardar su integridad	☐ SI ☒ NO ☐ N/A
r)	Se considera el uso de una oficina para tratar asuntos importantes como un método le privacidad dentro del GADM	☒ SI ☐ NO ☐ N/A
s)	Existe algún sistema de alerta localizado en cada puerta de ingreso el cual envíe un mensaje en caso de alguna actividad sospechosa.	☐ SI ☒ NO ☐ N/A

3. Limitaciones	
a) La puerta de ingreso al cuarto de comunicaciones del GADM es de cristal	☐ SI ☒ NO ☐ N/A
b) Se maneja un control de plagas que permita proteger los equipos electrónicos	☐ SI ☒ NO ☐ N/A
c) Se utiliza un sistema biométrico para el ingreso al cuarto de comunicaciones del GADM	☐ SI ☒ NO ☐ N/A
d) Las cerraduras de las puertas son seguras de acceso al cuarto de comunicaciones es lo suficientemente segura	☒ SI ☐ NO ☐ N/A
e) El sistema de cableado estructurado ha cumplido con el ciclo de vida útil	☒ SI ☐ NO ☐ N/A
f) Los sistemas de redundancia se encuentran en condiciones de funcionamiento adecuadas	☒ SI ☐ NO ☐ N/A
g) Los jefes departamentales extraen documentos sin autorización	☒ SI ☐ NO ☐ N/A
h) Las ventanas de las oficinas del GADM permiten ver los activos que se encuentran dentro de las mismas	☒ SI ☐ NO ☐ N/A
i) Los documentos que no son de importancia se los almacenan o desechan adecuadamente	☐ SI ☒ NO ☐ N/A
j) Ha observado algún tipo de anomalía dentro del espacio físico del GADM	☒ SI ☐ NO ☐ N/A

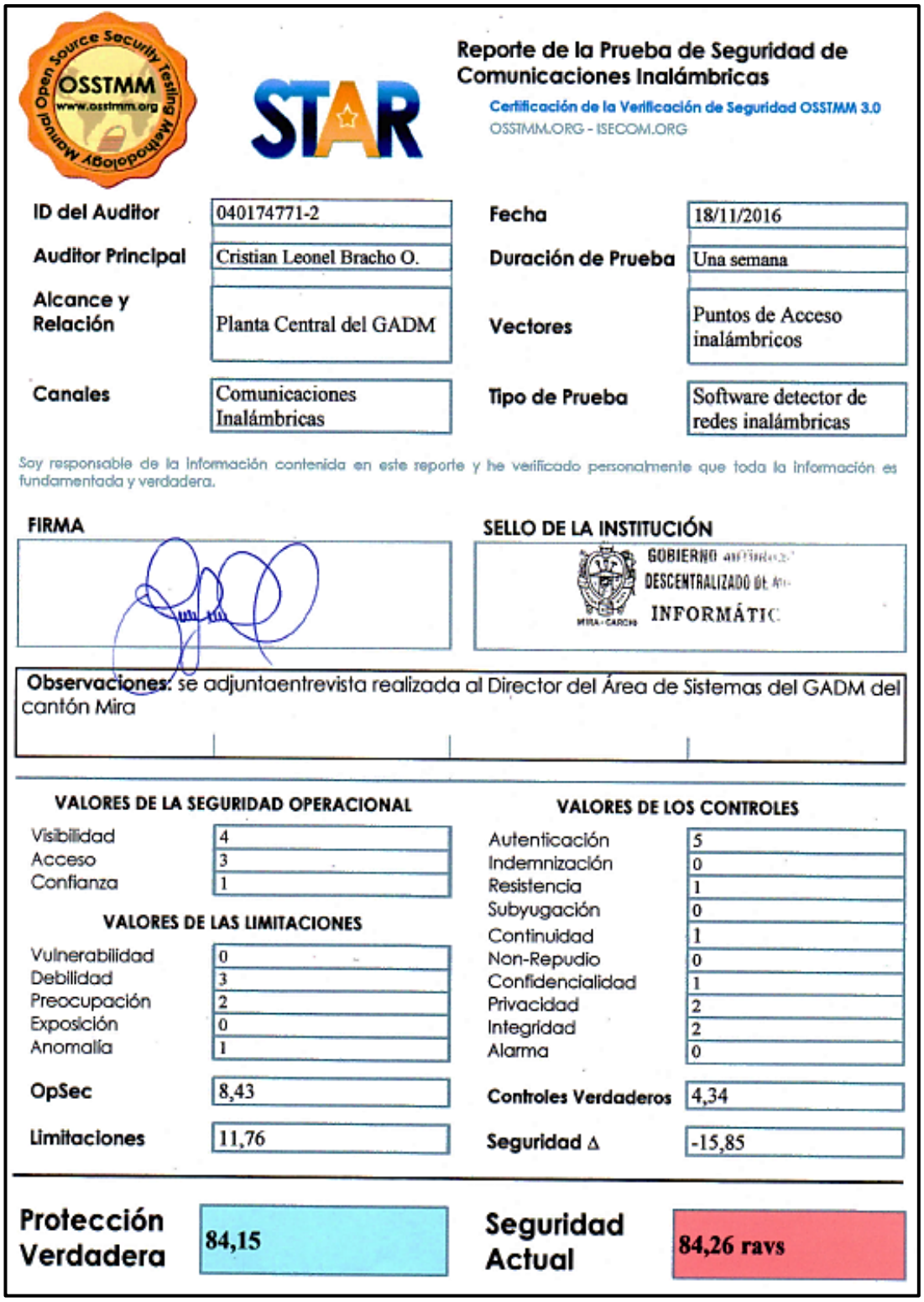
4. Equipos de telecomunicaciones	
a) Existe dentro del GADM un sistema de Voz sobre IP (VoIP)	☐ SI ☒ NO ☐ N/A
b) El GADM hace uso de una central telefónica analógica	☒ SI ☐ NO ☐ N/A
c) Existe dentro del GADM algún sistema de buzón de voz	☐ SI ☒ NO ☐ N/A
d) Existe dentro del GADM un sistema de fax	☒ SI ☐ NO ☐ N/A
e) Dentro del GADM se manejan sistemas de acceso remoto (RAS)	☐ SI ☒ NO ☐ N/A
f) En el GADM se utilizan las pruebas de líneas RDSI de respaldo	☐ SI ☒ NO ☐ N/A
g) El GADM hace uso de los sistemas de red X.25	☐ SI ☒ NO ☐ N/A

Nota: N/A= No aplicable

Observaciones

j) EL EDIFICIO NO CUENTA CON UNA INSTALACIÓN ELECTRICA ADECUADA, LO QUE OCACIONA PERMANENTES DAÑOS EN LOS EQUIPOS.

Anexo 13.- Reporte Canal de Comunicaciones Inalámbricas del GADM del Cantón Mira



Reporte de la Prueba de Seguridad de Comunicaciones Inalámbricas

Certificación de la Verificación de Seguridad OSSTMM 3.0

OSSTMM.ORG - ISECOM.ORG

ID del Auditor	040174771-2	**Fecha**	18/11/2016
Auditor Principal	Cristian Leonel Bracho O.	**Duración de Prueba**	Una semana
Alcance y Relación	Planta Central del GADM	**Vectores**	Puntos de Acceso inalámbricos
Canales	Comunicaciones Inalámbricas	**Tipo de Prueba**	Software detector de redes inalámbricas

Soy responsable de la información contenida en este reporte y he verificado personalmente que toda la información es fundamentada y verdadera.

FIRMA

SELLO DE LA INSTITUCIÓN

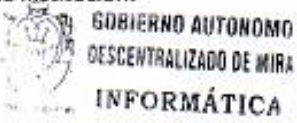
GOBIERNO [illegible]
DESCENTRALIZADO DE [illegible]
INFORMÁTIC

Observaciones: se adjuntaentrevista realizada al Director del Área de Sistemas del GADM del cantón Mira

VALORES DE LA SEGURIDAD OPERACIONAL		**VALORES DE LOS CONTROLES**	
Visibilidad	4	Autenticación	5
Acceso	3	Indemnización	0
Confianza	1	Resistencia	1
		Subyugación	0
VALORES DE LAS LIMITACIONES		Continuidad	1
Vulnerabilidad	0	Non-Repudio	0
Debilidad	3	Confidencialidad	1
Preocupación	2	Privacidad	2
Exposición	0	Integridad	2
Anomalía	1	Alarma	0
OpSec	8,43	**Controles Verdaderos**	4,34
Limitaciones	11,76	**Seguridad Δ**	-15,85

Protección Verdadera	84,15	**Seguridad Actual**	84,26 ravs

INFORME DE ENTREVISTA

Ítem investigado: Seguridad de las comunicaciones inalámbricas del GADM del cantón Mira	Fecha: 28/10/2016
Entrevistador: Cristian Leonel Bracho Ortega	Entrevistado: Ing. Damián Bastidas
Firma del representante: 	Sello de la institución: 

INTRODUCCIÓN

La presente entrevista se la realizó con motivo del desarrollo del proceso de auditoría de seguridad informática que se está ejecutando en el Gobierno Autónomo Descentralizado del Cantón Mira, y se utilizó este medio para obtener cierta información sobre la infraestructura de las conexiones inalámbricas que posee la institución en su planta central.

PREGUNTAS REALIZADAS

1) ¿Existe algún mecanismo de seguridad que regule el control de acceso para los equipos de comunicaciones inalámbricos, dentro de la planta central del GADM?
2) ¿Los radioenlaces que dispone el GADM desde su planta central se encuentran regularizados?
3) ¿Conoce que tipos de estándares soportan los equipos de comunicaciones inalámbricas del GADM?
4) ¿Dentro de la planta central del GADM se hace uso de algún tipo de sistema RFID (Radio Frecuencia), o algún otro tipo de sistema inalámbrico?
5) Actualmente, ¿cuántos Puntos de Acceso Inalámbricos (AP) dispone el GADM en su planta central?
6) ¿Se apagan los AP inalámbricos cuando no se hace uso de ellos?
7) ¿Se cambia regularmente el SSID de la red inalámbrica?
8) ¿Se hace uso de algún método de autenticación para conectarse a los AP inalámbricos de la planta central del GADM?
9) ¿Los equipos de comunicaciones inalámbricas se encuentran asegurados contra robo o daños?

10) ¿Se hace uso de algún tipo de acuerdo de responsabilidad por parte del personal que hace uso de los equipos inalámbricos del GADM?
11) ¿Cuál es el procedimiento a seguir cuando algún usuario incumple con un acuerdo legal?
12) Cuando se suscita algún tipo de daño o problema con los equipos inalámbricos de la planta central del GADM, ¿cuánto tiempo se tarda en resolverlo?
13) ¿Se hace uso de algún tipo de dispositivo o método que permita amortiguar las señales de los dispositivos inalámbricos de la planta central del GADM?
14) ¿Las transmisiones inalámbricas hacen uso de algún método de encripción?
15) ¿Se hace uso de algún sistema de alerta para evitar la ingeniería social dentro del GADM?
16) ¿La señal de un AP inalámbrico decae cerca de un horno microondas?

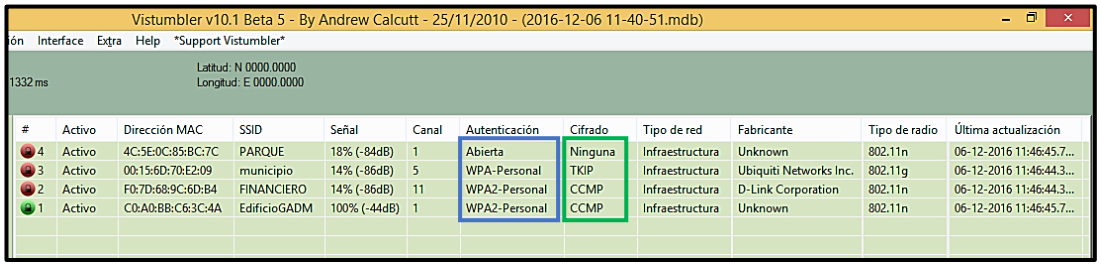
CONCLUSIONES

En base a las respuestas emitidas por el entrevistado, se llegó a las siguientes conclusiones:

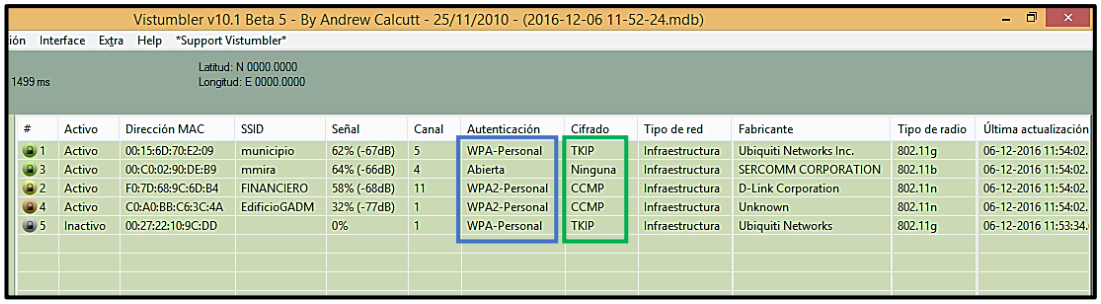
- Actualmente, no se hace uso de un sistema de control de acceso para los usuarios que acceden a las redes inalámbricas del GADM; pero sí se hace uso de un método de autenticación, el cual consiste en una contraseña diferente para cada punto de acceso inalámbrico.
- Los radioenlaces que ha implementado el GADM no se encuentran autorizados por un ente regulatorio.
- Actualmente existen 5 puntos de acceso en la planta central del GADM, que siempre permanecen encendidos independientemente de si se encuentren en uso o no, cuatro para uso interno y uno para uso público; dependiendo de la marca y de su ubicación dentro del GADM, se los configura de tal manera que no se interfieran, para ello se utilizan los estándares IEEE 802.11 b, g, n; en los canales 1,5 y 11.
- En el GADM no se hace uso de sistemas RFID o infrarrojos, u otros parecidos a estos; solo se utilizan las señales de Wi-Fi para la conexión a la Internet en los dispositivos móviles del personal.
- Una vez que se habilita el punto de acceso inalámbrico, se cambia su SSID y este no vuelve a ser cambiado; en algunos puntos de accesos se habilita la encripción de las contraseñas, pero no se habilita este servicio para las transmisiones.

- Los equipos de comunicaciones inalámbricas del GADM actualmente no se encuentran asegurados contra robos o daños, y no se firman acuerdos de responsabilidad por parte del personal; pero en caso de que una tercera persona incumpla con un acuerdo, el GADM recurre a las leyes vigentes en la región para aplicar una sanción.
- Al no existir un equipo de apoyo para el Área de sistemas, cuando se presenta un problema en alguna infraestructura externa del GADM, se puede tardar de uno a dos días en resolver el problema; pero en la planta central, se trata de resolverlo inmediatamente.
- Para amortiguar las señales que se emiten en la planta central del GADM, su hace uso de un método precario, que consiste en encerrar al punto de acceso en una caja metálica o de madera y de esta manera se limita la potencia de la señal. Nunca se ha notado que las señales de los equipos inalámbricos decaigan cerca de un horno microondas.
- El GADM ha implementado un sistema de video-vigilancia dentro de la planta central para asegurar el acceso físico a sus puntos de acceso inalámbricos, y para los equipos que se encuentran en una infraestructura externa se hace uso de cerraduras con llave, tanto para la puerta de acceso, como para los equipos; pero en caso de que alguna persona intente aplicar técnicas de ingeniería social para obtener información, no se hace uso de un sistema de alerta.

A continuación se muestran dos imágenes que corresponden a las capturas de pantalla generadas por el detector de redes inalámbricas Vistumbler, en la primera se muestran los Puntos de Acceso (AP) activos, luego de generar un escaneo fuera de las instalaciones del GADM-Mira; y la segunda muestra los Puntos de Acceso activos, luego de realizarse un escaneo dentro de las instalaciones de al Institución.

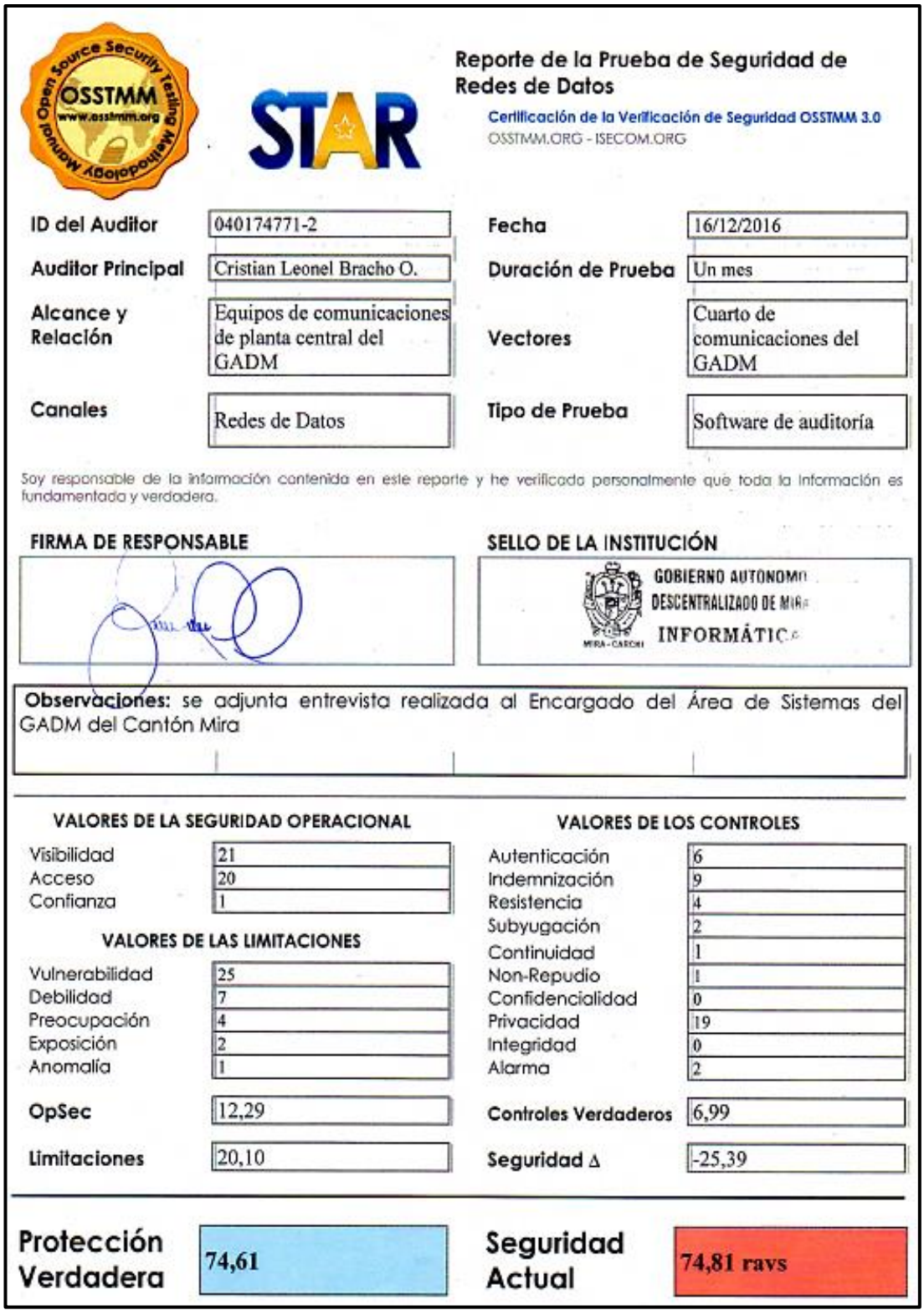


Captura de pantalla 1: Escaneo de redes inalámbricas fuera del GADM-Mira



Captura de pantalla 2: Escaneo de redes inalámbricas dentro del GADM-Mira

Anexo 14.- Reporte Canal de Redes de Datos del GADM del Cantón Mira



Reporte de la Prueba de Seguridad de Redes de Datos

Certificación de la Verificación de Seguridad OSSTMM 3.0

OSSTMM.ORG - ISECOM.ORG

ID del Auditor	040174771-2	**Fecha**	16/12/2016
Auditor Principal	Cristian Leonel Bracho O.	**Duración de Prueba**	Un mes
Alcance y Relación	Equipos de comunicaciones de planta central del GADM	**Vectores**	Cuarto de comunicaciones del GADM
Canales	Redes de Datos	**Tipo de Prueba**	Software de auditoría

Soy responsable de la información contenida en este reporte y he verificado personalmente que toda la información es fundamentada y verdadera.

FIRMA DE RESPONSABLE

SELLO DE LA INSTITUCIÓN

GOBIERNO AUTONOMO DESCENTRALIZADO DE MIRA

INFORMÁTICA

Observaciones: se adjunta entrevista realizada al Encargado del Área de Sistemas del GADM del Cantón Mira

VALORES DE LA SEGURIDAD OPERACIONAL

Visibilidad	21
Acceso	20
Confianza	1

VALORES DE LAS LIMITACIONES

Vulnerabilidad	25
Debilidad	7
Preocupación	4
Exposición	2
Anomalía	1

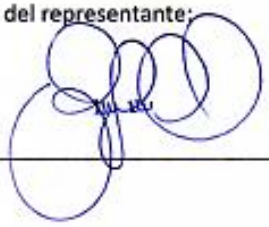
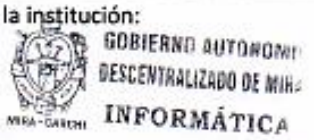
VALORES DE LOS CONTROLES

Autenticación	6
Indemnización	9
Resistencia	4
Subyugación	2
Continuidad	1
Non-Repudio	1
Confidencialidad	0
Privacidad	19
Integridad	0
Alarma	2

OpSec	12,29	**Controles Verdaderos**	6,99
Limitaciones	20,10	**Seguridad Δ**	-25,39

Protección Verdadera	74,61	**Seguridad Actual**	74,81 ravs

INFORME DE ENTREVISTA

Ítem investigado: Seguridad de las redes de datos del GADM del cantón Mira	Fecha: 21/11/2016
Entrevistador: Cristian Leonel Bracho Ortega	Entrevistado: Ing. Damián Bastidas
Firma del representante: 	Sello de la institución: 

INTRODUCCIÓN

La presente entrevista se la realizó con motivo del desarrollo del proceso de auditoría de seguridad informática que se está ejecutando en el Gobierno Autónomo Descentralizado del Cantón Mira, por lo que se utilizó este medio para poder tener un punto de partida en cuanto a detalles específicos de la red de datos de dicha entidad, y en base a la información obtenida, se podrá intervenir de mejor manera con un software de auditoría.

PREGUNTAS REALIZADAS

1) ¿Cuál es el proceso de autenticación a seguir para poder acceder a la red de datos del GADM?
2) ¿Qué equipos de comunicaciones se encuentran protegidos contra robo o daños?
3) ¿Qué tipos de usuarios se encuentran obligados a firmar un acuerdo de responsabilidad?
4) ¿Existen privilegios para los usuarios de la red de datos del GADM?
5) ¿Se obliga al personal del GADM a hacer uso de un tipo de protocolo o puerto en especial?
6) Aproximadamente, ¿Cuál es el tiempo de respuesta al presentarse algún tipo de daño en un equipo de comunicaciones del GADM?
7) ¿Existe algún tipo de mecanismo o sistema de detección de intrusos que permita verificar cuando alguien se ha conectado a la red de datos del GADM?
8) ¿Se hace uso de la encriptación de datos, como un mecanismo de seguridad?
9) ¿Se hace uso de algún método para la confidencialidad?
10) ¿Se limita en número de intentos de acceso a los servidores del GADM?
11) ¿En qué casos se hace uso del servicio de acceso remoto?
12) ¿Cuáles son los puntos más críticos de la red de datos del GADM?
13) ¿Qué impacto causa la caída de algún servidor en horas pico?
14) En caso de suscitarse algún tipo de fallo en la red, ¿se limitan los privilegios de acceso?

CONCLUSIONES

En base a las respuestas emitidas por el entrevistado, se llegó a las siguientes conclusiones:

- El procedimiento para autenticar a un usuario nuevo dentro de la red de datos consiste en la asignación de una dirección IP al equipo que vaya a utilizar dicho usuario, mismo que debe estar debidamente autorizado por el director del Área de sistemas del GADM.
- Actualmente, los dispositivos que se encuentran protegidos contra robos o daños son los equipos de computación de escritorio, las laptops y varios equipos de comunicaciones; pero el personal que hace uso de algún tipo de sistema debe someterse a un acuerdo de responsabilidad.
- No se manejan privilegios para los equipos de cómputo en general, pero para los servidores, el administrador asigna privilegios de lectura y escritura, solo lectura, y solo escritura a los usuarios; y en caso de que se presente algún tipo se fallo en la red, no se limitan los privilegios de acceso de los usuarios.
- No se obliga al personal del GADM a hacer uso de algún protocolo o puerto en especial, tampoco se hace uso de algún tipo de sistema de detección de intrusos en la red de datos, ni se utiliza la encriptación de la información reserva del GADM en la red.
- El tiempo de respuesta para resolver algún tipo de daño en la red depende del equipo, en caso de que se deba hacer una reposición, tarda hasta un mes; pero en caso de que se trate de un problema de configuración, se lo resuelve inmediatamente.
- No se utilizan métodos que permitan salvaguardar la confidencialidad de la información en proceso, ni se limitan los intentos de acceso a los servidores; y en caso de presentarse algún tipo de fallo en la red, no se limitan los privilegios de acceso.
- El servicio de acceso remoto se hace uso en los escritorios remotos del personal que necesite sacar respaldos del servidor de bases de datos, y para el servicio de NETBIOS del GADM.
- Los puntos más críticos de la red de datos del GADM son, por una parte su sistema de cableado estructurado, que prácticamente ha concluido con su tiempo de vida útil, y por otro lado la escalabilidad de la red, ya que se ha logrado cubrir el número de hosts disponibles con el pool de direcciones IP que dispone el GADM.
- Las caídas de servicios no solo de los servidores, sino también de los sistemas pueden causar pérdidas de información, molestias en la ciudadanía, entre otros tipos de impactos a la red como saturaciones en las respuestas a las peticiones que hace el personal, y que por ende desembocan en una mala imagen del GADM.

Anexo 15.- Informe Final de la Auditoría

INFORME FINAL DE AUDITORÍA DE SEGURIDAD INFORMÁTICA

1) ANTECEDENTES

El Gobierno Autónomo Descentralizado del Cantón Mira es una entidad pública que se encuentra al servicio de la ciudadanía mireña, fue fundado el 18 de Agosto de 1980; pero se comenzó a incursionar en el mundo de la Internet a mediados del año 2008, con alrededor de 19 puntos de red en su infraestructura de comunicaciones; y a medida que el desarrollo tecnológico ha ido evolucionando, también la escalabilidad con la que contaba en ese entonces la red fue decreciendo paulatinamente, hasta que en la actualidad prácticamente ha colapsado este recurso.

Al presente, la infraestructura de la red municipal del GAD tiene que enfrentarse a nuevos retos, ya que alrededor del mundo existen muchas personas mal intencionadas (hackers) que se dedican a encontrar las vulnerabilidades de las redes para provecho personal o con el simple fin de mostrar su superioridad, y con esto se puede llegar inclusive a crear un ambiente de temor para los usuarios que diariamente interactúan con el mundo exterior a través de las Internet. Es por ello que en el GADM se ha querido evaluar los mecanismos de seguridad que actualmente la red municipal posee, ya que en ciertas ocasiones el Administrador de la red ha notado un flujo exagerado de datos, para el número de usuarios disponibles, es por esta razón que la institución ha optado por llevar a cabo un proceso de auditoría de seguridad informática, mismo que se sustenta en un manual de metodologías de uso masificado, el OSSTMM (Open Source Security Testing Methodology Manual) versión 3.

2) FUNDAMENTO LEGAL Y NORMATIVA

El GADM del Cantón Mira, al no contar con una normativa legal interna, se recurrió a fundamentar el proceso de la auditoría como tal, en la Legislación Ecuatoriana vigente que regula todos los aspectos relacionados a la informática, entre ellos se encuentran:

- Ley orgánica de transparencia y acceso a la información pública
- Ley de comercio electrónico, firmas electrónicas y mensajes de datos
- Ley de propiedad intelectual
- Ley especial de telecomunicaciones

- Ley orgánica de garantías jurisdiccionales y control constitucional
- Código orgánico integral penal (COIP)

3) OBJETIVOS Y ALCANCE DE LA AUDITORÍA

El objetivo principal de la auditoría es:

Diagnosticar el estado de la red municipal del Gobierno Autónomo Descentralizado Municipal (GADM) del cantón Mira, mediante una auditoría de seguridad informática basada en la metodología OSSTMM versión 3, a fin de encontrar las posibles debilidades que ésta pueda tener y así proponer un plan de acción que ayude a corregirlas.

El alcance de la auditoría consiste en:

El proceso de la auditoría se lo desarrollara en cuatro fases:

(a) Fase de Inducción
(b) Fase de Interacción
(c) Fase de Indagación
(d) Fase de Intervención

Para la Fase de Inducción, es necesario hacer una revisión de los requisitos que serán necesarios para empezar con el proceso de la auditoría, tales como una autorización formal escita por el representante del GADM del Cantón Mira, quien velará para el proceso se lleve a cabo dentro de los márgenes permitidos por la ley, y que la información que se vaya a obtener de la auditoria sea utilizada únicamente para fines evaluativos, para ello es necesario también suscribir un acuerdo de confidencialidad y no divulgación de la información. También se realizará un breve análisis de la situación actual de la infraestructura de red del GADM, para seleccionar las posibles pruebas que se deben llevar a cabo.

Para la Fase de Interacción, se definirán los objetivos existentes para cada uno de los canales, y que se encuentren dentro del alcance, clasificándolos de tal manera que intervengan en el cálculo de cada una de las medidas que permiten evaluar la seguridad actual del canal auditado: Seguridad operacional o Porosidad, Controles y Limitaciones.

Para la Fase de Indagación, se aplicarán las técnicas escogidas para cada uno de los canales y se procederá a realizar las pruebas que permitan encontrar los valores numéricos

de cada uno de los ítems indicados para cada canal. Para el caso del canal humano y físico, para el canal de comunicaciones inalámbricas se aplicará en primer lugar una breve entrevista al Director del Área de Sistemas del GADM y se procederá a aplicar un software detector de redes inalámbricas, y para el canal de redes de datos se aplicara una breve entrevista al Director del Área de sistemas del GADM y se procederá a ejecutar varias aplicaciones del software de auditoría Kali-Linux.

Y para finalizar, en la Fase de Intervención se deberá determinar la efectividad de los canales auditados, para ello es necesario generar los informes para cada canal mediante el uso de la hoja de cálculos del RAV, la cual se encuentra disponible en el sitio web de ISECOM (http://www.isecom.org/research/ravs.html), en formato de una hoja de Excel. Para este proceso se debe insertar en los cuadros en blanco los valores numéricos obtenidos para cada ítem requerido y automáticamente se generaran los resultados que permiten emitir un juicio de criterio sobre la eficiencia de las medidas de seguridad adoptadas y dependiendo de los resultados obtenidos se deben recomendar las medidas correctivas necesarias.

4) PROCEDIMEINTOS RELEVANTES UTILIZADOS Y LIMITACIONES ENCONTRADAS

Entre los procedimientos utilizados a lo largo de las pruebas recomendadas para cada canal a probar se encuentran los siguientes: aplicación de varias técnicas de ingeniería social, para el canal humano y físico; hasta el uso de varios softwares, para el caso de comunicaciones inalámbricas, un software detector de redes inalámbricas (Vistumbler) y para el caso de las redes de datos, un software especializado para auditorías de seguridad de redes (Kali-Linux).

La limitación más predominante que se encontró en la red municipal fue que no se pudo probar el canal de telecomunicaciones, debido a que la metodología dictaba que se debían evaluar los siguientes vectores:

- Pruebas de PBX
- Pruebas de buzón de voz
- Encuesta, sondeo y pruebas de FAX y módem
- Pruebas de Servicio de Acceso Remoto (RAS)
- Pruebas de líneas RDSI de respaldo

- Pruebas de voz sobre IP
- Pruebas de conmutación de paquetes en redes X.25

Pero el Director del Área de Sistemas del GADM, quien se encarga de la administración de toda la infraestructura de red, aseguró por medio de un checklist que sólo existían dos de los vectores recomendados por la metodología; por lo tanto se procedió a reportar este canal como un objetivo no probado.

5) RESUMEN BREVE DE LOS RESULTADOS DE LA AUDITORÍA

El proceso de la auditoría arrojó los siguientes resultados:

Para el canal humano se obtuvo un valor para OpSec (Porosidad) de: 9,48; para los controles: 5,40; para las limitaciones: 14,03; para el Seguridad Δ, que es el valor que permite medir el equilibrio entre los tres valores anteriores -18,11. En base a estos valores se obtiene un valor para la protección verdadera de 81,89; y para la seguridad actual un valor de 81,95 ravs.

Para el canal físico se obtuvo un valor para OpSec (Porosidad) de: 11,43; para los controles: 6,21; para las limitaciones: 16,12; para el Seguridad Δ, que es el valor que permite medir el equilibrio entre los tres valores anteriores -21,34. En base a estos valores se obtiene un valor para la protección verdadera de 78,66; y para la seguridad actual un valor de 78,79 ravs.

Para el canal de comunicaciones inalámbricas se obtuvo un valor para OpSec (Porosidad) de: 8,43; para los controles: 4,34; para las limitaciones: 11,76; para el Seguridad Δ, que es el valor que permite medir el equilibrio entre los tres valores anteriores -15,85. En base a estos valores se obtiene un valor para la protección verdadera de 84,15; y para la seguridad actual un valor de 84,26 ravs.

Para el canal de redes de datos se obtuvo un valor para OpSec (Porosidad) de: 12,29; para los controles: 6,99; para las limitaciones: 20,10; para el Seguridad Δ, que es el valor que permite medir el equilibrio entre los tres valores anteriores -25,39. En base a estos valores se obtiene un valor para la protección verdadera de 74,61; y para la seguridad actual un valor de 74,81 ravs.

6) IDENTIFICACIÓN DE LOS HECHOS QUE DEBEN ORIGINAR RESPONSABILIDADES.

Los hechos que deben originar responsabilidades para el canal humano son: el GADM no maneja un Manual interno de Políticas de Seguridad de la Información, en el cual el personal pueda regir sus operaciones; tampoco se dictan regularmente capacitaciones al personal del GADM sobre temas de seguridad de la información; es por ello que este canal muestra una deficiencia en su efectividad de aproximadamente del 18%; lo que desencadena en que este canal es prácticamente vulnerable a la aplicación de técnicas de ingeniería social por parte de terceras personas.

Para el canal físico, los hechos que deben originar responsabilidades son: el manejo de normas de tráfico peatonal verificables dentro de la planta central del GADM, y el uso de mecanismos automatizados para el acceso a áreas restringidas; es por ello que este canal muestra una deficiencia de aproximadamente el 21%, a esto se suma el hecho de que el cuarto de comunicaciones no posee un diseño adecuado, ya que su implementación no se lo basó en algún tipo de estándar o norma.

Para el canal de comunicaciones inalámbricas, los hechos que deben originar responsabilidades son: el uso indiscriminado de los puntos de acceso inalámbricos que se encuentran en la planta central del GADM, ya que son equipos de gama baja y no están diseñados para permanecer encendidos todo el tiempo, por lo que se debería desarrollar un plan de uso de dichos equipos; si bien el uso de estos equipos por parte del personal del GADM es en mayor cantidad para uso de aplicaciones de mensajería instantánea que por lo general lo utilizan en sus dispositivos terminales móviles, se deberían aplicar las medidas de seguridad necesarias, ya que en ocasiones la información en curso puede contener datos de uso interno del GADM; es por ello que este canal muestra una deficiencia de aproximadamente del 16%.

Para el canal de redes de datos, los hechos que deben originar responsabilidades se deben analizar desde la base de su estructura que consiste en su sistema de cableado estructurado, ya que prácticamente ha cumplido con su tiempo de vida útil, a esto se le debe sumar que no se maneja una política de etiquetado de los equipos que forman parte de la infraestructura de la red. Por otra parte no se manejan equipos de uso particular del GADM y que sean administrables, en los que se puedan implementar los protocolos de

y como prácticamente la escalabilidad con la que contaba la red ha colapsado, se hace uso de un recurso muy precario que es la conexión en cascada de los equipos de conmutación.

Por otra parte se deben actualizar los equipos de cómputo que manejan ciertos empleados del GADM, ya que hacen uso de sistemas operativos para los que propietario ya no brinda soporte (Windows XP y Windows Vista); en cuanto a los servidores se debería implementar un firewall en el que el Administrador de la red pueda implementar sus propias reglas tanto para el tráfico de red de entrada como para el de salida. Es por ello y varios aspectos de seguridad más que este canal muestra una deficiencia aproximada del 25%.

7) COMENTARIOS DE LA ORGANIZACIÓN SOBRE LA ACEPTACIÓN DEL INFORME DE AUDITORÍA.

Observaciones

ENTREGADO POR	RECIBIDO POR	SELLO DE LA INSTITUCIÓN
Cristian Bracho Auditor	Sr. Damián Bastidas Responsable del Área de Sistemas del GADM Mira	GOBIERNO AUTONOMO DESCENTRALIZADO DE MIRA INFORMÁTICA

8) PROPUESTA DE MEJORAMIENTO

I. PORTADA

1. Título de la propuesta	Plan de mejoramiento del sistema de seguridad de la información del GADM del Cantón Mira
2. Objetivo general de la propuesta	Mejorar el sistema de seguridad de la información del GADM del Cantón Mira, respaldándose en las recomendaciones obtenidas luego de haber concluido el proceso de auditoría de seguridad informática en la Institución.
3. Nombre de la institución	Gobierno Autónomo Descentralizado Municipal del Cantón Mira
4. Domicilio	Av. León Rúales Nro. C8-010 y calle Gonzáles Suárez
5. Teléfonos, fax y correo electrónico	Fono.: 06 2280-246 Telefax: 06 2280-177 e-mail: gad@mira.gob.ec
6. Nombre del responsable técnico y datos de contacto	Sr. Damián Bastidas (Responsable del Área de Sistemas del GADM Mira) Cel.: 0997448787 e-mail: dbastidas@mira.gob.ec
7. Firma del representante técnico	GOBIERNO AUTONOMO DESCENTRALIZADO DE MIRA MIRA - CARCHI INFORMÁTICA
8. Ubicación del proyecto	Ecuador-Carchi-Mira
9. Tema de la convocatoria atendido por la propuesta	Auditoría de seguridad informática dirigida al Gobierno Autónomo Descentralizado del Cantón Mira basado en el estándar COBITv5, siguiendo la metodología OSSTMMv3
10. Presupuesto	Propio de la Entidad, o el que disponga el departamento
11. Fecha propuesta de inicio	La que disponga el departamento

II. RESUMEN DE LA PROPUESTA

Esta propuesta se crea con el fin de mejorar la eficiencia de los mecanismos de seguridad operacional adoptados actualmente por el GADM, ya que en el proceso de auditoría de seguridad informática aplicado a dicha entidad previamente, se obtuvo, en general que los mecanismos poseen una eficiencia de alrededor del 80%; es por esto que se propone ejecutar varias actividades de mejora en cada uno de los canales auditados (humano, físico, de comunicaciones inalámbricas y de redes de datos).

III. PROPUESTA TÉCNICA

1. Capacitación al personal

En primer lugar se debe contar con personal de apoyo para el Departamento; esto permitirá trabajar más fluidamente, ya que cada cual va a contar con tareas específicas.

Se debe crear un plan de capacitaciones continuas al personal del GADM en temas de seguridad de la información, de ser posible planificar una charla magistral por mes.

En la recepción se debe implementar un sistema de registro para las personas que vayan a acceder a las áreas restringidas del GADM

2. Normas de tráfico peatonal

Dentro de la planta central del GADM especificar las rutas de evacuación en caso de emergencias, puntos seguros, nombres de las diferentes estaciones de trabajo; y los lugares donde es permitido el acceso de terceras personas.

Ubicar y asignar epígrafes en las puertas de acceso a las áreas restringidas, como es el caso de las bodegas, cuarto de comunicaciones, oficinas de recaudación; y los que se consideren como tal; para el caso del cuarto de comunicaciones es importante implementar un sistema de acceso automatizado con un biométrico.

También se debe usar avisos de advertencia tales como de alto voltaje para las cajas térmicas, cámaras de vigilancia, puntos de acceso inalámbricos y extintores.

3. Comunicaciones Inalámbricas

Crear un plan de operación de los puntos de acceso inalámbricos, ya que es innecesario que estos permanezcan encendidos en jornadas en las cuales el personal no hace uso de ellos, tales como en las noches, fines de semana y días festivos.

Activar el cifrado de las transmisiones en los puntos de acceso inalámbricos que cuenten con este servicio.

Cambiar regularmente los SSID de las redes, así como las claves de acceso a los puntos de acceso, de ser posible se debe implementar un portal cautivo, para que de esta manera solo los usuarios autorizados puedan conectarse a la red de punto de acceso.

4. **Sistema de cableado estructurado**

Se debería considerar implementar un nuevo tendido del sistema de cableado estructurado tanto horizontal como vertical, tomando en cuenta las normas ANSI/EIA/TIA 569-C que trata sobre los espacios y canalizaciones para telecomunicaciones, ANSI/TIA/EIA-568-C, que trata sobre el cableado de telecomunicaciones para edificios comerciales y ANSI/TIA/EIA-607 que trata sobre las tierras y aterramientos para los sistemas de telecomunicaciones de los edificios comerciales ya que el sistema de cableado estructurado y el sistema de tendido eléctrico van de la mano; es preferible que para el nuevo tendido se cuente con un cable de mayor categoría con el que se cuenta actualmente, se podría considerar categoría 6 o 7.

El cuarto de comunicaciones debe ser diseñado de tal manera que cumpla con las especificaciones de TIER 1, o en caso de implementar las debidas redundancias tanto eléctricas, como para comunicaciones TIER 2, esto depende de la disponibilidad presupuestaría con la que cuente el Departamento, ya que este es el corazón de todo el sistema de comunicaciones del GADM.

Una vez que se concluya con el rediseño del cuarto de comunicaciones, se debe proceder a realizar un etiquetado de los equipos activos y pasivos que forman parte del sistema de comunicaciones.

Para los equipos de ruteo, por lo menos el router de núcleo debe ser administrable, y de propiedad del GADM; esto asegura que se puedan implementar los protocolos de enrutamiento que se acojan a las necesidades de la Institución y las reglas aplicables tanto al tráfico de entrada como de salida.

Para los equipos de conmutación, por lo menos el switch de acceso debe ser administrable, esto permite que se pueda segmentar la red y los acceso se los divida por áreas, dependiendo del número de usuarios que se permitan en cada área.

Implementar un equipo de firewall propio del GADM, para que el Administrador de la red pueda implementar las normas del tráfico de la red.

Se debe prescindir del uso de los ordenadores que ya hayan cumplido con su tiempo de vida útil, ya que eso hace más vulnerable a la red municipal.

IV. BENEFICIARIOS

Indirectamente, los beneficiarios inmediatos son la ciudadanía del Cantón Mira, ya que van a poder tener una confianza elevada hacia el GADM, porque su sistema de seguridad permitirá que la información que manejan de ellos sea lo más reservada posible.

Los beneficiarios directos son el personal del GADM, ya que van cuidar de mejor manera la información que generan diariamente en sus estaciones de trabajo, si bien los cambios en un inicio son un tanto incómodos, con el paso del tiempo se van verificando los incontables beneficios que estos generan, porque esto los hará más competitivos frente a otras entidades gubernamentales.

V. PROVEEDORES

Debido a que el financiamiento de esta propuesta dependerá del monto presupuestario que se le asigne a el área de Sistema des GADM, los proveedores obedecerán al método de financiamiento al que se acoja la entidad; por lo tanto se deberá planificar los costos aproximados que se invertirán en los cambios que se deben hacer en el sistema de seguridad informática y en la adquisición de equipos y materiales.

Anexo 16.- Manual de Políticas de Seguridad de la Información del GADM del Cantón Mira

GOBIERNO AUTÓNOMO DESCENTRALIZADO
DEL CANTÓN MIRA

ALCALDÍA Mira
Un cantón que avanza

ACTA DE ENTREGA RECEPCIÓN

Antecedentes.- El señor Cristian Leonel Bracho Ortega, estudiante de la carrera Electrónica y Redes de Comunicación de la Universidad Técnica del Norte, realizo el proyecto de Tesis "Auditoria de Seguridad Informática dirigida al Gobierno Autónomo Descentralizado del cantón Mira, basado en el estándar COBITv5, siguiendo la metodología OSSTMMv3".

Qué el Gobierno Autónomo Descentralizado del cantón Mira, brindo al estudiante todas las facilidades para que pueda realizar su proyecto dirigido a la Institución.

Acuerdan.-

El señor Cristian Leonel Bracho Ortega, estudiante de la carrera Electrónica y Redes de Comunicación de la Universidad Técnica del Norte, entregar el "Manual de Políticas de Seguridad de la Información del Gobierno Autónomo Descentralizado del cantón Mira", como producto de su proyecto de tesis.

El señor Damián Bastidas, responsable de la Unidad de Sistemas del Gobierno Autónomo Descentralizado del cantón Mira recibe el "Manual de Políticas de Seguridad de la Información del Gobierno Autónomo Descentralizado del cantón Mira".

Para dar fe de lo antes mencionado, se realiza la firma de la presente acta, a los 9 días del mes de febrero del 2017.

Cristian Leonel Bracho Ortega
ESTUDIANTE UTN
ENTREGUE CONFORME

Damián Bastidas
SISTEMAS GAD MIRA
RECIBI CONFORME

GOBIERNO AUTONOMO DESCENTRALIZADO DE MIRA
INFORMÁTICA

www.mira.gob.ec

Dirección: León Ruales C8-010 y González Suárez
062 280 246 / 062 280 177
Alcaldía Mira
E-mail: gad@mira.gob.ec
MIRA - CARCHI - ECUADOR

1. POLÍTICAS GENERALES DE SEGURIDAD DE LA INFORMACIÓN

Art. 1 Entiéndase por información al conjunto de datos sean estos de forma escrita, oral, gráfica, digital o en cualquier otra forma conocida; mismos que se generen por cualquier activo o difundan dentro del perímetro que comprende el espacio físico del Gobierno Autónomo Descentralizado Municipal del Cantón Mira, considerándose esta un recurso esencial para todo tipo de actividades que se desarrollen dentro del GADM desde el momento en que se la genera hasta el momento que es destruida, una vez que haya cumplido con su ciclo de validez.

Art. 2 El GADM del Cantón Mira deberá definir e implantar los controles necesarios para proteger la información contra los tres principios básicos de la misma: divulgación a usuarios no autorizados (confidencialidad), modificación inadecuada (integridad) y garantizar el acceso a los usuarios de los servicios que ofrece la Entidad cuando sea necesario (disponibilidad).

Art. 3 Todos los funcionarios y/o empleados serán responsables de proteger la información a la cual acceden y procesan, para evitar su pérdida, alteración, destrucción o uso indebido.

Art. 4 Los activos informáticos del GADM del Cantón Mira, serán identificados y clasificados para establecer los mecanismos de protección necesarios.

Art. 5 El GADM del Cantón Mira definirá e implantará los controles necesarios para proteger la información contra violaciones de autenticidad, accesos no autorizados, la pérdida de la integridad y que garanticen la disponibilidad requerida por los clientes y usuarios de los servicios ofrecidos por la Entidad.

Art. 6 Se deberán realizar auditorías y evaluaciones periódicas sobre un modelo de gestión de Seguridad Informática, dependiendo de la elección de las partes involucradas que actualizarán el manual y que se ajuste a las necesidades de la Institución.

Art. 7 Para los procesos dentro de la Institución que necesariamente hagan uso de algún tipo de programa, únicamente se permitirá el uso de un software autorizado que haya sido adquirido legalmente por la Institución.

Art. 8 Es responsabilidad de todos los funcionarios y empleados del GADM del Cantón Mira reportar los incidentes de Seguridad Informática, eventos sospechosos y el mal uso de los recursos que identifiquen.

Art. 9 Las violaciones a las Políticas y Controles de Seguridad Informática serán reportadas, registradas y monitoreadas constantemente por el personal pertinente.

Art. 10 El departamento que tenga dominio del manual de Políticas del GADM del Cantón Mira deberá sugerir la creación de un Plan de Continuidad del Servicio que garantice la estabilidad de los mecanismos de seguridad operacional, ante la ocurrencia de eventos no previstos o desastres naturales.

2. POLÍTICA DE CONTROL DE ACCESOS

2.1. POLÍTICAS DE SEGURIDAD A NIVEL DE ACCESO FÍSICO

Del acceso a áreas restringidas

Art. 11 Todas las áreas destinadas al procesamiento o almacenamiento de información sensibles para el GADM, así como aquellas en las que se encuentran los equipos y demás infraestructura de soporte para los sistemas de información y comunicaciones se consideran áreas de acceso restringido. En consecuencia, deben contar con medidas de control de acceso físico perimetral, de tal manera que permitan proteger la información, el software y el hardware de daños intencionales o accidentales.

Art. 12 El acceso del personal a las áreas restringidas del GADM se llevará a cabo de acuerdo a las normas y procedimientos que dicta el Departamento de Sistemas o en su defecto, el Departamento a cargo de dicha área.

Art. 13 Para el ingreso a las áreas restringidas después del horario normal de trabajo, fines de semana o feriados solo el personal que cuente con una autorización formal podrá acceder a dicha área.

Art. 14 En caso de ausencia del Jefe departamental que otorga la autorización, por motivos tales como vacaciones, calamidad doméstica, enfermedad o los contemplados en la ley; se deberá hacer una petición formal escrita al inmediato superior, explicando los motivos para acceder al área restringida.

Art. 15 En concordancia con la política de la institución y debido a la naturaleza de estas áreas es preciso llevar un registro permanente de acceso del personal, sin excepción alguna para así evitar el repudio.

Art. 16 El Departamento de Sistemas o su equivalente, deberá proveer la infraestructura de seguridad requerida para estas áreas, en base a las normas y estándares vigentes en la región, o hacer las debidas recomendaciones para las áreas que se encuentren fuera de su jurisdicción.

Art. 17 Las llaves para las puertas de acceso a estas áreas deben encontrase únicamente en poder del jefe departamental a cargo, o por una persona delegada por él.

Del acceso al data center cuarto o de comunicaciones

Art. 18 El acceso al cuarto de comunicaciones debe ser restringido y por lo tanto solo el personal autorizado por el Jefe departamental a cargo debe otorgar el debido acceso.

Art. 19 Queda totalmente prohibido realizar actos inadecuados dentro del data center tales como fumar, ingresar cualquier tipo de alimentos, ingresar líquidos inflamables, ingresar bebidas alcohólicas o cualquier acto que atente con el funcionamiento de los equipos que se encuentran dentro del data center.

Art. 20 El área informática debe estar vigilada las 24 horas del día, utilizando para ello hardware dedicado o personal de seguridad para evitar accesos no autorizados.

Art. 21 Durante los procedimientos de mantenimiento preventivo o correctivos de los equipos que se encuentran dentro del cuarto de comunicaciones, se deberá comprobar la credencial en caso de requerir personal ajeno al GADM, y deberá estar presente el jefe departamental o un supervisor delegado por esta área.

2.2. POLÍTICAS DE SEGURIDAD A NIVEL DE ACCESO LÓGICO

Del establecimiento, uso y protección de las claves de acceso

Art. 22 El Departamento de Sistemas o su equivalente deberá establecer procedimientos formales para controlar la definición de perfiles, id de usuarios, contraseñas o claves de acceso y la asignación de derechos de acceso de manera individual, previamente definidos por el ente responsable del procedimiento. Dichos procedimientos deben cubrir todas las etapas del ciclo de vida del usuario, desde su registro inicial hasta su eliminación o desactivación debido a que ya no necesita el acceso.

Art. 23 El jefe de sistemas debe brindar atención y dar seguimiento especial, donde se necesite un control de asignaciones de privilegios de acceso.

Art. 24 Cada usuario es responsable del mecanismo de control de acceso que le sea proporcionado, llámese este identificador de usuario y contraseña necesarios para acceder a la información y la infraestructura tecnológica de la organización, para lo cual se deberán mantener de forma confidencial.

Art. 25 Se debe concienciar y capacitar a los usuarios y el personal en general para que sigan buenas prácticas para el uso y protección de claves o contraseñas.

Art. 26 Los usuarios no deben proporcionar información al personal externo, de los mecanismos de control de acceso lógico para la infraestructura tecnológica del GADM, a menos que cuente con la autorización del jefe de sistemas.

Art. 27 Cualquier cambio en los roles y responsabilidades de los usuarios deberán ser notificados al departamento de sistemas, para el cambio de privilegios, previamente aprobados por el ente regulador a cargo.

Art. 28 En caso de que un usuario olvide, bloquee o extravíe su contraseña o clave de acceso, deberá acudir al departamento de sistemas, para la asignación de una nueva.

Art. 29 Queda totalmente prohibido que los usuarios expongan o revelen por cualquier medio y de manera legible sus claves o contraseñas de acceso.

Art. 30 Está prohibida la reutilización de las 5 últimas contraseñas, con el fin de utilizar las mismas contraseñas en intervalos regulares de tiempo.

Del control de acceso a la red de área local

Art. 31 El departamento de sistemas es responsable de establecer un procedimiento de autorización y controles para proporcionar a los usuarios el acceso y proteger los recursos de la red de área local del GADM.

Art. 32 Se debe asegurar que las redes inalámbricas del GADM cuenten con métodos de autenticación con el fin de evitar accesos no autorizados.

Art. 33 Se debe realizar una segmentación de las redes, separando los entornos de red con respecto a los usuarios y los servicios brindados por el GADM.

Art. 34 Queda totalmente prohibido realizar cualquier tipo de exploración inapropiada de los recursos informáticos conectados a la red de área local del GADM, con fines de búsqueda de vulnerabilidades y que atenten contra el buen funcionamiento de la red.

Art. 35 El acceso lógico a los equipos de red tales como: servidores, routers, switches administrables, puntos de acceso inalámbricos; conectados a la red de área local deben ser administrados únicamente por el personal competente.

Art. 36 Todo el equipo de cómputo que se encuentre conectado o pertenezca a la red, y que sea de propiedad del GADM, debe regirse a los procedimientos de acceso que dicte el departamento de sistemas.

De acceso a los sistemas informáticos

Art. 37 Solamente contarán con acceso a los sistemas informáticos el personal del GADM que tenga por obligación el manejo de dichos sistemas.

Art. 38 La información generada en los sistemas informáticos del GADM contiene información sensible de la ciudadanía, por medio de los servicios prestados por el GADM por lo que debe ser manejada con total responsabilidad y por ningún motivo, dicha información debe ser divulgada, salvo en casos donde la Ley así lo considere.

Art. 39 La instalación, actualización, mantenimiento y uso de los sistemas informáticos del GADM deben regirse por las normas o procedimientos establecidos por el departamento de sistemas o su equivalente.

Art. 40 El sistema informático debe contemplar la recuperación de información en caso de que en una transacción falle por error de programación, error de usuario o algún otro error.

Art. 41 En caso de necesitarse opciones con datos privados, el sistema debe contemplar la ejecución desde un determinado terminal o nivel de usuario.

Art. 42 La documentación de los sistemas informáticos debe contemplar las tablas a las que se tiene acceso, así como los diferentes permisos de lectura, escritura, inserción, actualización o eliminación.

Art. 43 Una vez que el usuario haya finalizado con su jornada de trabajo o deje en modo descanso el terminal donde éste se encuentra instalado, deberá cerrar su sesión de inicio.

Del acceso a la Internet

Art. 44 El acceso a Internet provisto a los usuarios del GADM es exclusivamente de uso para actividades relacionadas con las necesidades de la función desempeñada por el personal del GADM, por lo tanto se debe hacer uso de Firewall o proxies que permitan rechazar conexiones externas que busquen atentar a la red interna del GADM.

Art. 45 Se debe mantener actualizado el servicio de anti virus licenciado con el fin de evitar incidentes de software malintencionado hacia el recurso computacional del GADM.

Art. 46 No se permite el acceso a páginas relacionadas con pornografía, drogas, alcohol, hacking y cualquier tipo de páginas web que vayan en contra de la ética, la moral y las leyes vigentes en la región.

Art. 47 Se prohíbe el acceso o el uso de servicios interactivos o mensajería instantánea, cuyo objetivo sea el de crear comunidades para intercambiar información, o bien para fines diferentes a las actividades propias del GADM.

Art. 48 Se prohíbe la descarga, uso, intercambio o instalación de juegos, música, películas, información o productos que de alguna forma atenten a la propiedad intelectual de sus autores o que contengan herramientas que atenten contra la integridad, disponibilidad y confidencialidad de la infraestructura tecnológica del GADM.

Art. 49 En caso de ser necesario se debe crear niveles de acceso a la Internet, para que los usuarios en cada nivel conozcan las páginas que pueden ser visitadas, dependiendo al nivel que pertenezcan.

Acceso en caso de emergencia

Art. 50 Llámese emergencia a fenómenos causados por la naturaleza en donde el hombre no tiene influencia tales como: inundaciones, terremotos, sismos, lluvias torrenciales, deslaves; o las provocadas por influencia del hombre tales como incendios; para lo cual se debe crear un plan de contingencia dependiendo del nivel de afectación para el acceso a los activos del GADM, tomando en cuenta el peligro que conlleve este procedimiento.

Art. 51 Los centros de cómputo, cableado, espacios de infraestructura tecnológica y estaciones de trabajo deben contar con mecanismos que permitan garantizar el cumplimiento de los requerimientos ambientales, especificados por los fabricantes de los equipos a fin de que puedan responder de manera adecuada ante incidentes como incendios e inundaciones.

Art. 52 Se deben adoptar los controles necesarios para mantener a los equipos de comunicaciones alejados de sitios que puedan presentar riesgos potenciales como explosivos, agua, residuos, polvo, vibraciones, contaminantes e interferencias electromagnéticas a fin de asegurar su buen funcionamiento en caso de presentar alguna amenaza.

3. POLÍTICA DE SEGURIDAD DE LA INFROMACIÓN RELATIVA AL PERSONAL

Art. 53 El personal deben ser adecuadamente seleccionados antes de ser contratados, una vez contratado, debe ser fácilmente identificable mientras forme parte del GADM y su

acceso a los activos del GADM debe ser revocado oportunamente una vez que haya finalizado su contrato o haya sido transferido.

Art. 54 Los recursos tecnológicos y de software asignados a cada empleado o jefe departamental del GADM son manejados bajo su responsabilidad.

Art. 55 El personal debe estar consciente de sus responsabilidades y deberá tomar decisiones pertinentes en caso de presentarse algún incidente.

Art. 56 El personal es el activo más valioso del GADM, pero también es el más vulnerable, por lo que un gran número de problemas de seguridad informática con respecto a los activos de computo pueden generarse ya sea por negligencia o por desinformación, es por ello que se deben implementar procedimientos para manejar estos riesgos y ayudar al personal del GADM a generar un ambiente de trabajo seguro.

Art. 57 Se deben de tomar las medidas de precaución pertinentes cuando se contrata o se despide a un empleado, estableciendo los controles necesarios para comunicar los cambios de personal, ya que es crucial que estos cambios sean atendidos a tiempo.

Art. 58 Todo usuario de activos y recursos informáticos del GADM al ingresar como personal del mismo, acepta las condiciones de confidencialidad, acuerdos de responsabilidad y uso adecuado de los recursos informáticos y de información, así como el estricto apego en el Manual de Políticas de Seguridad de la Información vigente.

Art. 59 El Departamento de Talento Humano debe notificar al área de Sistemas, la contratación, despido o renuncia de los empleados; así como el inicio y fin de los períodos de vacaciones de los mismos, con el fin de revocar los privilegios asignados a dicho empleado.

Art. 60 Todo personal o usuario nuevo deberá contar con una debida inducción sobre el Manual de Políticas de Seguridad de la Información, en donde se deben dar a conocer tanto las obligaciones como las sanciones que se contemplan en dicho manual.

Art. 61 Es responsabilidad del área de sistemas promover constantemente la importancia de la seguridad informática a todo el personal del GADM, por medio de capacitaciones continuas, charlas; adicionalmente se pude emplear diversos métodos como afiches, mensajes u otros que permitan al personal recordar permanentemente el rol que cumple en el mantenimiento de la seguridad de la información.

Art. 62 Se consideran violaciones graves al presente manual el robo, daño, acceso no autorizado, divulgación de la información reservada o confidencial del GADM, renuncias a los acuerdos de responsabilidad; en cuyo caso se lo puede declarar al empleado que realice

alguna de las acciones antes descritas como culpable de un delito informático, por lo que deberá atenerse a las sanciones prescritas en la legislación regional vigente.

4. POLÍTICAS DE SEGURIDAD FÍSICA Y AMBIENTAL

Art. 63 Los equipos de procesamiento de datos y el cuarto de comunicaciones, así como los mecanismos de control de acceso físico, tanto para el personal como para personas particulares a áreas restringidas del GADM del Cantón Mira, deben encontrarse en ambientes físicamente protegidos a fin de garantizar el acceso no autorizado, daños o interferencias y deben apegarse a las normas y estándares vigentes en la región.

Del resguardo y protección de la información

Art. 64 El personal deberá reportar de forma inmediata al departamento de Sistemas o su equivalente, si llegará a detectar que existen riesgos reales o potenciales para los equipos de cómputo o comunicaciones, tales como fugas de agua, humedad, incendios, plagas no controladas, descargas eléctricas u otros que atentaren con el buen funcionamiento de los mismos.

Art. 65 El personal tiene la obligación de proteger las unidades de almacenamiento que encuentren bajo su cargo, aun cuando no se encuentren en uso permanente y más aún si contienen información confidencial para el GADM.

Art. 66 Si por alguna razón de causas naturales, un dispositivo de almacenamiento llega a mostrar fallas, el personal tiene la obligación de reportar al departamento de sistemas este hecho y así cumplir con la evaluación del dispositivo y su respectivo informe, en caso de que tenga que ser dado de baja.

Art. 67 Es responsabilidad del personal evitar en todo momento la fuga de información, física o digital del GADM que se encuentre almacenada en los equipos de cómputo o archivadores personales que se encuentren a su cargo.

De los controles de acceso físico

Art. 68 Se deberá hacer uso de algún método que permita registrar el ingreso de cualquier persona, y si es el caso de algún elemento que no sea propiedad del GADM, para poder acceder a las áreas restringidas. En el caso de que necesite retirar materiales o herramientas

fuera del GADM se deberá cumplir con el mismo procedimiento de registro, pero en este caso del personal y del elemento extraído.

Art. 69 Las computadoras personales, las computadoras portátiles y cualquier activo informático del GADM, podrá ser extraído de las instalaciones del GADM, únicamente con una autorización formal del director de sistemas.

Art. 70 El personal debe asegurarse que toda la información que es considerada como sensible para el GADM debe ser debidamente respaldada.

Art. 71 En caso de que el personal note que la información que se encuentra a su cargo ha sido parcial o totalmente modificada, debe notificar al jefe de sistemas para que realice las acciones legales pertinentes.

De la seguridad en las estaciones de trabajo

Art. 72 Entiéndase por estación de trabajo el espacio físico que reúne las condiciones adecuadas para que cada empleado realice sus respectivas labores diarias encomendadas; por lo que es recomendable que dichas estaciones de trabajo cumplan con los requerimientos de seguridad personal básicos, para que la información que maneja cada empleado pueda mantenerse segura.

Art. 73 El personal es responsable por la información y los equipos de cómputo que maneje dentro de su estación de trabajo.

Art. 74 Las estaciones de trabajo del personal que maneja los sistemas informáticos del GADM deben tener por lo menos un control de acceso para evitar que personas ajenas al GADM tengan acceso directo a dichas estaciones.

Art. 75 Las estaciones de trabajo en donde se manejen transacciones financieras, es decir donde haya dinero de por medio, deben tener rejillas y puertas metálicas, con seguros que se vulneren con facilidad para así evitar robos o atracos por delincuentes.

Art. 76 En horas donde el personal tenga que ausentarse de su estación de trabajo, las puertas y ventanas que permitan el acceso directo a la información deben permanecer cerradas.

De la protección y ubicación de los equipos

Art. 77 El personal no debe mover o reubicar los equipos de cómputo o de comunicaciones, instalar o desinstalar dispositivos que sean de propiedad del GADM, retirar sellos o códigos sin autorización, instalar aplicaciones que provengan de un destino inseguro, desinstalar

aplicaciones que sean de propiedad del GADM, retirar o cambiar cables de los equipos de cómputo sin la previa autorización del director de sistemas; en caso de requerir uno de los servicios antes mencionados, se deberá realizar una petición formal escrito u oral al jefe de sistemas, para que él tome las medidas competentes.

Art. 78 El jefe de sistemas es el responsable de llevar un inventario actualizado, con los activos que han sido asignados a cada empleado en su estación de trabajo.

Art. 79 El jefe de sistemas prestará su firma para asegurar que las peticiones formales que se le presenten, tengan legalidad, por lo que será responsable del resguardo y la ubicación exacta de los activos informáticos del GADM.

Art. 80 El equipo de cómputo que se haya asignado a cada empleado deberá ser para uso exclusivo de las funciones que el GADM le haya encargado.

Art. 81 El personal es responsable de solicitar la capacitación pertinente para el manejo de las herramientas informáticas que utilizará en su equipo, si ese fuera el caso; esto con el fin de evitar riegos por mal uso o inexperiencia.

Art. 82 En caso de que el personal manejare una carpeta compartida con los demás departamentos, es de su total responsabilidad almacenar la información en la carpeta que se le haya asignado.

Art. 83 Queda totalmente prohibido tratar de explorar las carpetas a las cuales el personal tiene acceso restringido.

Art. 84 Mientras el personal se encuentre operando los equipos de cómputo, queda prohibido ingerir cualquier tipo de alimentos o bebidas.

Art. 85 Es responsabilidad del personal verificar que los equipos de cómputo que se encuentran a su cargo tengan una adecuada ventilación, tanto en su armazón como ambientalmente; caso contrario informal al personal del área de sistemas.

Art. 86 El personal debe verificar constantemente que los equipos de cómputo que se encuentran en su estación de trabajo se mantengan en las condiciones adecuadas de limpieza.

Art. 87 Queda terminantemente prohibido que el personal desarme o cambie piezas de los equipos de cómputo.

Art. 88 Todo el equipo de cómputo debe poseer un seguro antirrobos.

De las pérdidas de los equipos

Art. 89 El personal que tenga a su cargo algún equipo de cómputo, será responsable de su uso y custodia; por lo tanto por lo tanto deberá responder por dicho bien en caso de robo, extravío o pérdida del mismo.

Art. 90 El préstamo interno de los equipos de cómputo lo manejará y autorizará el director de sistemas.

Art. 91 En caso de desaparición, robo o extravío de los equipos de cómputo o dispositivos bajo su cargo; el personal deberá dar aviso inmediato al personal del área de sistemas.

Del uso de dispositivos especiales

Art. 92 En ocasiones es necesario el uso de dispositivos especiales tales como discos duros externos, tarjetas de almacenamiento, cámaras fotográficas, cámaras de video, o cualquier dispositivo necesario para desarrollas las funciones específicas, por lo que es de total responsabilidad del personal responder por dichos dispositivos a su cargo.

Art. 93 Todo el personal que por sus funciones necesitare de estos dispositivos, deberá realizar una petición formal al custodio de los mismos, explicando los motivos de su uso, y una vez finalizada su labor justificar con evidencias el uso al que fue sometido.

Art. 94 En caso de presentarse algún tipo de fallo en dichos dispositivos informar al personal del área de sistemas.

Art. 95 En caso de que los dispositivos sufran algún tipo de fallo por maltrato, descuido, negligencia o mal manejo por parte del personal a cargo, deberá responder por ello ante el director de sistemas para que tome las medidas pertinentes.

5. POLÍTICAS DE GESTIÓN DE INCIDENTES

Entiéndase por incidente de seguridad de la información, cualquier acto que de manera fortuita o planificada, tenga como finalidad causar algún tipo de daño al buen funcionamiento de todo el recurso informático del GADM, incluido la infraestructura física y los equipos de comunicaciones.

Art. 96 Se deben establecer responsabilidades y procedimientos para tratar los eventos y los puntos débiles de la seguridad de la información de forma efectiva. Una vez que se hayan comunicado a través de un proceso de mejora continua, el grupo de resolución de

problemas se encargará de analizar la causa y evaluarla conforma al proceso de gestión de problemas del GADM.

Art. 97 Todo el personal del GADM incluidas las terceras partes deben anotar y comunicar de manera oportuna al personal del Área de Sistemas, cualquier incidente de seguridad de la información que hayan observado o que sospechen que exista en los sistemas o servicios, ya sea de forma verbal o mediante un documento formal, indicando claramente los datos por los cuales los considera un incidente de seguridad de la información.

Art. 98 El departamento encargado de la Gestión Tecnológica, debe asegurarse de que los eventos y los puntos débiles de seguridad de la información asociados con el recurso informático del GADM, se comunican de forma que sea posible emprender acciones correctivas de manera oportuna y sin paralizar el acceso a los activos, servicios y aplicaciones.

Art. 99 Se debe establecer un procedimiento formal de comunicación de eventos de seguridad de la información, junto con un procedimiento de respuesta y escalado de incidentes, mismo que debe determinar la respuesta que debe darse cuando se recibe un informe de un evento de seguridad de la información.

Art. 100 En caso de que un empleado que hace uso de los equipos de cómputo del GADM, identifique o sospeche de la presencia de un virus en el sistemas, debe desconectar el equipo de la red de datos y notificar inmediatamente al personal del Área de Sistemas, para la eliminación del virus antes de reestablecer la conexión a la red de datos.

Art. 101 Cuando se detecte por primera vez un incidente de seguridad de la información, puede que no resulte evidente si dicho evento tendrá como consecuencia una acción legal. Por este motivo, existe el peligro de que se destruyan de forma intencional o accidental las pruebas necesarias antes de tomar conciencia de la verdadera gravedad del incidente, es por ello que se debe asesorar en cuanto a los procesos jurídicos antes de proceder con cualquier acción legal, más aún si el incidente es causado por una persona ajena al GADM.

Art. 102 Cuando se inicie una acción contra una persona u organización, después de un incidente de seguridad de la información, que implique medidas legales (tanto civiles como penales), deberían recopilarse con anticipación las pruebas necesarias, mismas que deben conservarse y presentarse de manera que se ajusten a las normas legales vigentes.

6. POLÍTICA DE CONTINUIDAD DE LAS OPERACIONES Y RECUPERACION ANTE DESASTRES

De las actividades previas al desastre

Art. 103 El Área de Sistemas del GADM, conjuntamente con el Área de Planificación deben realizar actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de los activos de la infraestructura tecnológica del GADM, que aseguren un proceso de recuperación de desastres con el menor costo posible.

Art. 104 Se deberá establecer un plan de acción que ayude a coordinar las acciones a llevarse a cabo con los equipos de cómputo y los respaldos de información, antes, durante y después del desastre.

Art. 105 Para los equipos de cómputo, es necesario realizar un inventario actualizado de los equipos, especificando su contenido. (software, marcas y licencias)

Art. 106 Para los respaldos de información, se deberá establecer los procedimientos para obtención de copias de seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los programas, aplicaciones y/0 sistemas del GADM. Copias del sistemas operativo (en caso de contar con varios), herramientas de trabajo, bases de datos y aplicativos.

Art. 107 Los respaldos de información o backups se deben almacenar en condiciones ambientas óptimas, dependiendo del medio empleado para el almacenamiento.

Art. 108 Se debe hacer una revisión periódica de los elementos de respaldo, en caso de utilizar medios electromagnéticos, para reemplazarlo de forma oportuna antes de cumpla con su periodo de vida útil.

De las actividades durante el desastre

Art. 109 Una vez que se presente la contingencia, falla o siniestro, se debe ejecutar las actividades previamente planificadas.

Art. 110 Se deberá ejecutar un plan de emergencias, en donde se establecen las acciones a realizar cuando se presente un falla o desastre, así como la coordinación y comunicación de la misma.

Art. 111 Es muy conveniente prever los posibles escenarios de ocurrencia del siniestro, el cual puede presentarse de forma improvista.

Art. 112 El plan de emergencia debe contemplar la participación y actividades a realizar por todas las personas que se puedan encontrar presentes en el área de ocurrencia, detallando las salidas de emergencia, vías de evacuación, señalización y demarcación de las señales de auxilio (extintores, cajas de revisión, cajas térmicas, linternas, lámparas de mano, números telefónicos de emergencia y nombres de los funcionarios a contactar), así como también la ubicación específica de los puntos seguros.

Art. 113 Se debe establecer un programa de entrenamiento contra los posibles desastres que puedan ocurrir en la región, al menos una vez al año, de acuerdo a los roles que se hayan asignado en los planes de evacuación.

Art. 114 Un aspecto importante a tomar en cuenta es que el personal debe tomar conciencia de que los desastres (incendios, inundaciones, temblores, tormentas eléctricas, etc.) pueden realmente ocurrir y se debe tomar con absoluta responsabilidad y seriedad los entrenamientos, para estos efectos es necesario de todos los funcionarios, directivos, administrativos y terceras personas que se encuentren presentes en el momento del entrenamiento.

De las actividades después del desastre

Art. 115 Se debe realizar una evaluación de daños, inmediatamente después de ocurrido el desastre, esto con el fin de evaluar la magnitud del daño producido, equipos no funcionales, equipos que sufrieron daños recuperables y la estimación del tiempo de la recuperación total del desastres ocurrido.

Art. 116 La recuperación y puesta en marcha de algún tipo de servicio afectado se realizará en dos fases, la primera para reestablecer el servicio afectado usando los recursos propios del GADM y la segunda con el apoyo de proveedores y entes tanto gubernamentales como no gubernamentales.

Art. 117 Una vez finalizada la fase de recuperación, se debe evaluar objetivamente las actividades realizadas, el porcentaje de eficiencia y efectividad, tiempo de recuperación total, inconvenientes presentados, colaboración y apoyo.

Art. 118 Con la evaluación de los resultados se debe actualizar el plan de contingencia original, mejorando las actividades más complejas y reforzando las que no respondieron adecuadamente.

7. POLÍTICA DE GESTIÓN DE ACTIVOS

Art. 119 Para asegurar que los activos de la información reciben el nivel de protección adecuado, el Área de Sistemas del GADM es responsable de definir la metodología de clasificación de los activos de información, mismos que se deben clasificar según la necesidad, las prioridades y el grado de protección esperado en el manejo de los mismos.

Art. 120 La información debe estar inventariada y tener identificados los riesgos y exposiciones de seguridad; con el objetivo de evitar pérdidas financieras, operativas y/o de la buena imagen del GADM, la información deberá ser clasificada como restringida, confidencial, de uso interno o general; así:

- Restringida: información con mayor grado de sensibilidad, el acceso a esta información debe ser autorizada caso por caso.
- Confidencial: información sensible que solo debe ser divulgada a aquellas personas que la necesitan para el cumplimiento de sus tareas.
- De uso interno: datos generales para facilitar las operaciones diarias; deben ser manejados de una manera discreta, pero no requieren de medidas de seguridad.
- General: información que es generada específicamente para su divulgación a la población en general o a los usuarios.

Art. 121 La información que se catalogue como secreta o restringida debe estar soportada por un acuerdo de confidencialidad o de no-divulgación cuando sea compartida con terceros.

Art. 122 El GADM es propietario de los activos de información que se manejen en la planta central o en cualquiera de sus dependencias; y los administradores de estos activos son los funcionarios, empleados, ejecutivos o demás colaboradores del GADM (denominados "usuarios") que se encuentren debidamente autorizados y sean responsables por la información de los procesos a su cargo, de los sistemas de información o aplicaciones informáticas, hardware o infraestructura de tecnologías de la información y comunicaciones (TIC).

Art. 123 Los usuarios deberán utilizar únicamente los programas y equipos autorizados por el Área de Sistemas del GADM.

Art. 124 Todos los colaboradores, contratistas, administrativos, empleados y terceras partes que hagan uso de los activos de información que sean de propiedad del GADM, son

responsables de acoger con integridad la Política de gestión de los activos para dar un uso racional y eficiente de los recursos asignados.

Art. 125 El GADM proporcionara al usuario los activos informáticos y los programas instalados en ellos, los datos/información creados, almacenados y recibidos serán de propiedad del GADM, los administradores solo podrán realizar respaldos de sus archivos personales o de información pública, para copiar cualquier tipo de información clasificada o reservada se debe contar con la autorización de un jefe inmediato superior, de acuerdo a las normas sobre clasificación de la información acorde a los niveles de seguridad establecidos por el GADM. La copia, sustracción, daño intencional o utilización para fines a las laborales propias del GADM, serán sancionadas de acuerdo con las normas y legislación vigentes en la región.

Art. 126 Todos los requerimientos de aplicativos, sistemas y activos informáticos deben ser solicitados al personal del Área de sistemas con sus correspondiente justificación para su respectiva viabilidad.

Art. 127 Estarán bajo custodia del Área de sistemas los medios magnéticos o electrónicos que vengan originalmente con el software y sus respectivos manuales y licencias de uso, adicionalmente las claves para descargar las actualizaciones del fabricante del software de sus páginas web o sitios de Internet y los passwords de administración de los activos informáticos, sistemas de información o aplicativos.

Art. 128 El Área de sistemas debe implementar las medidas necesarias para la protección frente al riesgo de la utilización de equipos y comunicación móvil. Se prestará especial cuidado para asegurar que no se comprometa la información del GADM, teniendo en cuenta los riesgos que conlleva el trabajar con equipos móviles en entornos desprotegidos.

Art. 129 Se debe elaborar y mantener un inventario de los activos importantes asociados a cada sistema de información. Cada activo debe ser claramente identificado, así como su propietario y clasificación en cuanto a seguridad deben ser acordados y documentados, junto con la ubicación vigente del mismo (importante cuando se emprende una recuperación posterior a una pérdida o daño). Ejemplos de activos asociados a sistemas de información son los siguientes:

- Recursos de información: bases de datos y archivos, documentación de los sistemas, manuales de usuario, material de capacitación, procedimientos operativos o de soporte, planes de contingencia, disposiciones relativas a sistemas de emergencia para la reposición de información perdida, información archivada.

- Recursos de software: software de aplicaciones, software de sistemas, herramientas de desarrollo y utilitarios.
- Activos físicos: equipamiento informático (procesadores, monitores, computadoras portátiles, módems), equipos de comunicaciones (routers, PBX, máquinas de fax), medios electromagnéticos (discos duros, dispositivos de almacenamiento externo, CD, DVD), otros equipos técnicos (suministro de electricidad, unidades de aire acondicionado, extintores, medios de iluminación), mobiliario.
- Servicios: servicios informáticos y de comunicaciones, utilitarios generales, entre otros.

8. REGLAS DE COMPORTAMIENTO

Expectativa de privacidad

Art. 130 Cada empleado dentro de su estación de trabajo tiene absoluta privacidad para manejar las acciones para las que fue destinado.

Art. 131 Para salvaguardar la privacidad en los documentos físicos que se manejen con reserva, se debe proveer de un mecanismo de almacenamiento con llaves, mismas que manejen solo el personal que tenga acceso a dichos documentos.

Art. 132 En caso de que los temas a tratarse por uno o varios empleados del GADM sea de absoluta confidencialidad, y deba ser manejado con prudencia, se escogerá un área llamada "oficina cerrada", esto con el fin de asegurar que los temas allí discutidos no sean de dominio público.

Art. 133 El Área de sistemas del GADM, debe proveer los mecanismos para asegurar el control de privacidad siempre que fuere necesario.

Art. 134 El control de privacidad es un mecanismo que permite que la información sea conocida solo por las personas autorizadas, por lo que no se debe utilizar este mecanismo de manera inadecuada, para justificar actividades que están fuera de este principio.

Internet

Art. 135 El acceso a la Internet provisto a los usuarios del GADM es de uso exclusivo para actividades relacionadas con las necesidades del cargo y función que desempeña.

Art. 136 El acceso a la Internet tiene que realizarse a través de los canales de acceso provistos por el GADM, en caso de necesitar una conexión especial, ésta tiene que ser notificada y aprobada por el jefe del Departamento de sistemas.

Art. 137 El usuario debe abstenerse de descargar programas que realicen conexiones automáticas o visores de sitios clasificados como pornográficos, y la utilización de los activos del GADM para la redistribución de este tipo de material, ya se vía web o mediante la utilización de medios magnéticos.

Art. 138 Se debe abstener el uso de sitios conocidos como túneles, mismos que están destinados a desafiar la seguridad del servidor de acceso a la Internet (proxy)

Art. 139 No está permitido el uso de la Internet con fines comerciales, políticos particulares o cualquier otro que no sea laboral.

Art. 140 El Área de sistemas debe establecer procedimientos e implementar controles operacionales para evitar la descarga de software no autorizado y evitar códigos maliciosos provenientes de la Internet.

Art. 141 De ser conveniente se deben generar registros de navegación y los accesos de los usuarios ala Internet, así como establecer e implementar procedimientos de monitoreo sobre la utilización del servicio de Internet, esto con el fin de salvaguardar el control del no repudio.

Art. 142 En caso de que existan invitados en el GADM y requieran de una conexión a la Internet, previamente se deberá realizar una pequeña charla respecto a las precauciones que se deben tener en cuenta cuando se hace uso de este servicio.

E-mail

Art. 143 El GADM como muestra del respeto por los principios de libertad de expresión y privacidad de la información, no genera a los usuarios ninguna expectativa de privacidad en cualquier elemento que almacene, envíe o reciba por medio de su correo electrónico personal.

Art. 144 Las comunicaciones vía correo electrónico entre los usuarios y sus equivalentes de otras entidades públicas o privadas deben realizarse a través del correo institucional proporcionado por el GADM. No es permitido utilizar cuentas personales para comunicarse con el público de interés del GADM, ni para transmitir cualquier tipo de información respecto al GADM.

Art. 145 A los usuarios que de acuerdo con sus funciones requieran de una cuenta de correo institucional, esta se les asignará en el servicio contratado por el GADM una vez que sean vinculados.

Art. 146 La cuenta de correo electrónico institucional estará activa durante el tiempo que dure la vinculación del empleado con el GADM, excepto en casos de fuerza mayor o mala utilización, que eventualmente puedan causar la suspensión o cancelación de la misma. Una vez que se produzca la desvinculación del empleado, la cuenta será dada de baja en el servidor de hosting del GADM.

Art. 147 El uso del correo electrónico institucional debe ser usado solamente para fines propios del GADM. En su uso el empleado actuará siempre con respeto y cortesía, no podrá crear, distribuir o reenviar mensajes que ofenden la dignidad, intimidad y buen nombre de las personas, de las instituciones, o para realizar algún tipo de acoso, difamación, calumnia, con intención de intimidar, insultar o cualquier otra forma de actividad discrepante; de igual forma se prohíbe difundir ideas políticas, religiosas, propagandas, entre otros.

Art. 148 El GADM se abstiene de enviar o recibir los mensajes de sus empleados con contenido impropio, difamatorio, ilícito, obsceno, indecente o que contengan difusión de noticias sin identificación plena de su autor; adicionalmente los usuarios no podrán enviar anónimos, propagandas o literatura de cualquier índole, encuestas, concursos, esquemas piramidales, cartas en cadena, mensajes no deseados, o cualesquiera que contenga mensajes duplicativos o no solicitados, u otra información ajena a las labores que se desempeñen en el cargo al que fue designado.

Art. 149 Respetar la privacidad de las cuentas de otros usuarios del servicio de correo electrónico, tanto dentro como fuera de la red municipal.

Art. 150 Si utiliza el servicio de correo electrónico institucional, se recomienda que no se deje mensajes almacenados por mucho tiempo. Se debe tener presente descargarlos con frecuencia, preferiblemente a diario ya que el tamaño del buzón del correo es limitado.

Mensajería instantánea

Art. 151 El uso de servicios de mensajería instantánea y el acceso a redes sociales estarán autorizados solo para un grupo reducido de usuarios, teniendo en cuenta sus funciones y para facilitar canales de comunicación con la ciudadanía.

Art. 152 No se permite el envío de mensajes con contenido que atente contra la integridad de las personas o instituciones o cualquier contenido que represente riesgo de código malicioso.

Art. 153 En el caso de que se haga uso de una aplicación de mensajería instantánea se debe tomar en cuenta los aspectos básicos de la seguridad de la información, y no utilizarlas para circular por este medio, datos que sean de tipo restringido o reservados del GADM.

Art. 154 La información que se publique o divulgue por cualquier medio de Internet, de cualquier funcionario, empleado o colaborador del GADM, que sea creado a nombre personal, en las redes sociales como twitter, facebook, youtube, likedink o blogs, se considera fuera del alcance del sistema de seguridad del GADM, y por lo tanto su confiabilidad, integridad y disponibilidad; así como los daños y perjuicios que puedan llegar a causar serán de completa responsabilidad de la persona que las haya generado.

Del control de acceso remoto

Art. 155 El departamento de sistemas es responsable de proporcionar el servicio de acceso remoto a los usuarios que lo necesitaran, garantizando que se use con fines constructivos.

Art. 156 Cualquier usuario interno o externo que requiera acceso remoto a la red o a la infraestructura de procesamiento de información del GADM del Cantón Mira, sea este por medio de la Internet, telefónica o por cualquier otro medio, debe estar debidamente autenticado y sus conexiones deberán utilizar el cifrado de datos.

Art. 157 Dependiendo de la información que vaya a circular por medio del acceso remoto, el usuario deberá escoger si la realiza vía Telnet, en caso de que la información no sea de importancia, o SSH en caso de que la información sea de tipo confidencial.

Uso de dispositivos móviles y cámaras

Art. 158 El GADM proveerá las condiciones para el manejo de los dispositivos móviles institucionales (teléfonos inteligentes y tabletas, cámaras digitales, entre otros) y personales que hagan uso de los servicios del GADM. Así mismo, velara porque los funcionarios hagan uso responsable de los servicios y equipos proporcionados.

Art. 159 El Área de sistemas debe establecer un método de bloqueo (por ejemplo: contraseñas, biométricos, patrones, reconocimiento de voz) para los dispositivos móviles institucionales que serán entregados a los usuarios. Se debe configurar dichos dispositivos para que pasado un tiempo de inactividad pasen automáticamente a modo de suspensión y, en consecuencia, se active el bloqueo de la pantalla el cual requerirá del método de desbloqueo configurado.

Art. 160 Los usuarios deben evitar usar los dispositivos móviles y las cámaras institucionales en lugares que no ofrezcan las garantías de seguridad física necesarias para así evitar la pérdida o robo de los mismos.

Art. 161 Los usuarios no deben almacenar videos, fotografías o información personal en los dispositivos móviles y cámaras institucionales asignados.

Utilización de impresoras, escáner y fax

Art. 162 Los documentos que se impriman en las impresoras del GADM deben ser de carácter institucional.

Art. 163 Es responsabilidad del usuario conocer el adecuado manejo de los equipos de impresión (escáner, fotocopiado y fax) para que no se afecte su correcto funcionamiento.

Art. 164 Ningún usuario debe realizar labores de reparación o mantenimiento de las impresoras y equipos de fax. En caso de presentarse alguna falla se debe reportar al personal del Área de sistemas.

Uso de ordenadores particulares para actividades corporativas.

Art. 165 El personal del GADM debe evitar en la medida que sea posible la utilización de ordenadores que no sean de propiedad del GADM para realizar sus actividades laborales, ya que esto conlleva que se tenga la posibilidad de filtrar la información que se esté manejando en ese momento.

Art. 166 En el posible caso de que se haga uso de un ordenador en un cyber, se debe tratar de no utilizar las herramientas de la Internet para generar información del GADM, y al finalizar, borrar todo tipo de información que se pudo haber generado.

Art. 167 En el caso de que el empleado se encontrará fuera de la cuidad, deberá hacer una petición de los ordenadores móviles para poder llevar a cabo sus labores corporativas.

9. POLITICA DE ADQUISISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS DE INFORMACIÓN.

Art. 168 El Área de sistemas del GADM debe proveer las medidas de seguridad en los sistemas de información desde la fase de requerimientos, y deben ser incorporados en las etapas de desarrollo, implementación y mantenimiento.

Art. 169 Todos los sistemas de información o desarrollos de software deben tener un área específica dentro del GADM formalmente asignada.

Art. 170 Las áreas asignadas a los sistemas de información, en acompañamiento con la Oficina de gestión de riesgos, deben establecer las especificaciones de adquisición o desarrollo de sistemas de información considerando los principios básicos de seguridad de la información.

Art. 171 Los administradores de los sistemas de información deben definir los datos sensibles que pueden ser eliminados de sus sistemas y solicitar que éstos soporten la eliminación de dicha información, como es el caso de los datos personales o financieros, cuando éstos ya no son requeridos.

Art. 172 La Oficina de gestión de riesgos debe liderar la definición de requerimientos de seguridad de los sistemas de información, teniendo en cuenta aspectos tales como la estandarización, controles de acceso y arquitectura de las aplicaciones; entre otros.

Art. 173 Los desarrolladores de in sistemas de información deben certificar que el sistema adquirido o desarrollado utilice herramientas de desarrollo licenciadas y reconocidas en el mercado.

Art. 174 El GADM velara porque el desarrollo interno, de ser el caso, o externo de los sistemas de información cumpla con los requerimientos de seguridad esperados, con las buenas prácticas para desarrollo seguro de aplicativos, así como con metodologías para la realización de pruebas de aceptación y seguridad al software desarrollado. Además, se deberá asegurar que todo software desarrollado o adquirido, interna o externamente cuente con el nivel de soporte requerido por el GADM.

Art. 175 El Área de sistemas será la única dependencia autorizada para realizar copias de seguridad del software original.

Art. 176 En caso de la adquisición de un nuevo sistema de información, o actualización, es necesario efectuar una solicitud por parte del ente competente, con la debida justificación, misma que se analizará para su evaluación y aprobación.

Art. 177 Se requiere de un control estricto en la implementación de cambios. Los procedimientos de control de cambios deben validar que los procesos de seguridad y control operacional no estén comprometidos; igualmente se debe cerciorar que los programadores de apoyo posean acceso solo a las partes en el sistema necesarias para llevar a cabo su trabajo, que dichos cambios sean aprobados con un procedimiento adecuado y con la documentación correspondiente.

10. POLÍTICA DE GESTIÓN DE PROVEEDORES

Art. 178 Todo acceso por parte de los proveedores debe ser autorizado por un responsable interno, quien debe asumir la responsabilidad por las acciones que puedan realizar los mismos; por lo que si se requiere de acceso especial a los sistemas de información del GADM se lo debe realizar únicamente cuando sea necesario.

Art. 179 Todo proveedor debe de firmar un acuerdo de no-divulgación antes de tener acceso a la información del GADM.

Art. 180 Los contratos relacionados a los servicios de tecnologías de la información que puedan brindar los proveedores deben ser aprobados por el área legal del GADM; y en caso de que afecten la seguridad o las redes de la entidad deben ser aprobados adicionalmente por el Área de sistemas. Bajo determinadas condiciones, como en la ejecución de servicios críticos para el GADM, se debe considerar efectuar una revisión independiente de la estructura de control interno hacia el proveedor.

Art. 181 En los contratos de procesamiento de datos externos se debe especificar los requerimientos de seguridad y acciones a tomar en caso de violación de alguna de las cláusulas estipuladas en el contrato. Siempre en todos los contratos que se refieran a temas de seguridad de la información del GADM se debe incluir una cláusula donde se establezca el derecho del GADM para nombrar a un representante autorizado para evaluar la estructura de control interno del proveedor.

Art. 182 El proveedor debe ser responsable de informar inmediatamente al ejecutor del contrato sobre cualquier brecha de seguridad de la información que pueda comprometer al GADM.

Art. 183 Cualquier empleado del GADM debe informar al Área de sistemas en caso de que exista algún tipo de violación a la seguridad de la información por parte de los proveedores.

11. POLÍTICAS DE GESTIÓN DE COMUNICACIONES Y OPERACIONES

11.1. OPERACIONES INTERNAS

Adaptación de deberes

Art. 184 La adaptación de los deberes es un método para reducir el riesgo de un mal uso accidental o deliberado de los sistemas.

Art. 185 Los deberes y áreas de responsabilidad deben estar adaptadas para reducir las oportunidades de una modificación no-autorizada o mal uso no-intencional o mal uso de los activos de la organización.

Art. 186 Se debe tener cuidado con el acceso, modificación o uso de los activos sin autorización o detección de intrusos

Art. 187 En caso de que sea difícil el proceso de adaptación de deberes, se deben considerar otros controles como el monitoreo de actividades, rastros de auditoría y supervisión gerencial. Es importante que la auditoría de seguridad se mantenga de manera independiente.

Gestión de seguridad de la red

Art. 188 Una gestión segura de las redes puede abarcar los límites organizacionales, requiere de una cuidadosa del flujo de datos, implicaciones legales, monitoreo y protección. También se puede requerir de controles adicionales para proteger la información confidencial que pasa a través de redes públicas.

Art. 189 Se deben establecer controles especiales para salvaguardar la confidencial y la integridad de los datos que circula a través de las redes públicas o las redes inalámbricas.

Art. 190 Se deben establecer responsabilidades y procedimientos para la gestión de equipos remotos, incluyendo el equipo en las áreas del usuario.

Art. 191 La documentación relativa a configuración, instalación, procesos de sistemas y servicios de información, bases de datos, conectividad de redes, servicios de respaldo de energía, entre otros, deben resguardarse a efecto de prevenir el acceso no autorizado. El acceso a esta documentación deberá estar restringido sólo al personal autorizado.

11.2. OPERACIONES EXTERNAS

Gestión de la entrega de servicios de terceros

Art. 192 Se debe implementar y mantener un nivel apropiado de seguridad de la información y entrega de servicios en línea con los acuerdos de entrega de servicios de terceros.

Art. 193 El GADM debe examinar la implementación de acuerdos, monitorear su cumplimiento con los estándares y manejar los cambios para asegurar que los servicios sean entregados para satisfacer todos los requerimientos acordados por la tercera persona.

Art. 194 Se debe asegurar que los controles operacionales de seguridad de la información, definiciones de los servicios y niveles de entrega incluidos en los acuerdos de la entrega de un determinado servicio por parte de terceras personas se implemente, operen y mantengan.

Art. 195 La entrega de un servicio por parte de una tercera persona deberá incluir los acuerdos de seguridad pactados por parte del GADM y la institución que presta el servicio, definiciones del servicio y aspectos de la gestión del servicio.

Art. 196 El GADM debe asegurar que las terceras personas mantengan una capacidad de servicio aceptable, junto con los planes de trabajo diseñados para asegurar que se mantengan los niveles de continuidad del servicio después de fallas importantes en el servicio o un desastre.

Protección contra código malicioso y móvil

Art. 197 Se requiere tomar las debidas precauciones para evitar y detectar la introducción de códigos maliciosos y códigos móviles no-autorizados.

Art. 198 La protección contra códigos maliciosos se debe basar en la detección de dichos códigos y la reparación del software implicado en este tipo de ataque, la implantación de los controles apropiados de acceso a la red LAN del GADM y gestión de cambio.

Art. 199 Se debe establecer una política formal que prohíba el uso de software no-autorizado por personas ajenas al GADM, en cualquier tipo de medio electrónico que no forme parte del inventario informático.

El código móvil, es un tipo de código de software que se transfiere de un ordenador a otro y luego se ejecuta automáticamente para realizar una función específica, con muy poca o ninguna interacción.

Art. 200 Para asegurar que el código móvil no contenga códigos maliciosos, un control de código móvil es esencial para evitar el uso no-autorizado o interrupción de un sistema o recursos de las aplicaciones y otras fallas en la seguridad de la información.

11.3. PROCEDIMIENTOS OPERATIVOS DE SEGURIDAD DE INFORMACIÓN DE TI

Procedimientos y responsabilidades operacionales

Art. 201 Se debe asegurar y garantizar el funcionamiento de la operación correcta y segura de los medios de procesamiento de la información.

Art. 202 Se deben establecer las responsabilidades y procedimientos para la gestión y operación de todos los medios de procesamiento de la información.

Art. 203 Se debe implementar la segregación de deberes para reducir el riesgo de negligencia o mal uso deliberado de un sistema informático.

Procedimientos de operación documentados

Art. 204 Se debe contar con procedimientos debidamente documentados para los procesos en que se sustenten los productos y servicios emanados desde las Unidades de Operaciones, Sistemas, Comunicaciones y Servicios a la ciudadanía; mismos que deben describir las actividades y tareas que deben ejecutarse para la obtención de los mismos.

Art. 205 Los procedimientos de operación se deberían documentar, mantener y poner a disposición de todos los usuarios que así los necesiten.

Art. 206 Se deben preparar procedimientos documentados para las actividades de sistemas asociados con los medios de procesamiento de la información y comunicación; tales como: procedimientos para encender y apagar los computadores, copias de seguridad, mantenimiento del equipo, manejo de medios, cuarto de comunicaciones o data center, manejo del correo institucional y seguridad.

Art. 207 Los procedimientos de operación deberían especificar las instrucciones para la ejecución detallada de cada trabajo incluyendo:

a) Identificación y registro de cambios significativos
b) Procesamiento y manejo de la información
c) Evaluación de los impactos potenciales de los cambios, incluyendo los impactos de seguridad.
d) Instrucciones para el manejo de errores u otras condiciones excepcionales, las cuales podrían surgir durante la ejecución del trabajo, incluyendo las restricciones sobre el uso de las utilidades del sistema.
e) Contactos de soporte en el evento de dificultades operacionales o técnicas inesperadas.
f) Instrucciones para el manejo de documentos físicos y medios de almacenamiento, tales como el uso de papelería especial o el manejo de documentos confidenciales incluyendo los procedimientos para la eliminación segura de los documentos de trabajo fallidos.

Art. 208 Los procedimientos de operación y los procedimientos documentados para las actividades del sistema debieran ser tratados como documentos formales y cambios en los mismos deben ser autorizados por el ente responsable.

12. POLÍTICA DE CUMPLIMIENTO

Art. 209 Toda ley, norma, regulación o acuerdo contractual debe ser documentado y revisado por el área legal del GADM. Requerimientos específicos para controles y otras actividades relacionadas a estas regulaciones legales deben ser delegados al área organizacional respectiva, la cual es responsable por el cumplimiento de la norma en cuestión.

Art. 210 Los administrativos y jefes departamentales deben asegurarse que las responsabilidades de seguridad sean cumplidas y las funciones relacionadas se ejecuten apropiadamente.

Art. 211 Es responsabilidad del personal encargado de la administración de la seguridad y de auditoria interna verificar el cumplimiento de las políticas de seguridad. Las excepciones deben ser reportadas al director departamental pertinente.

Art. 212 El GADM velará por la identificación, documentación y cumplimiento de la legislación relacionada con la seguridad de la información, entre ellas las referentes a los derechos de autor y propiedad intelectual, razón por la cual propenderá porque el software instalado en los ordenadores de la plataforma tecnológica cumpla con los requerimientos legales y de licenciamiento aplicables.

Art. 213 El Departamento Jurídico y el Área de Gestión de Riesgos deben identificar, documentar y mantener actualizados los requisitos legales, reglamentarios o contractuales aplicables al GADM y relacionados con seguridad de la información.

Art. 214 El Área de Sistemas debe certificar que todo el software que se ejecuta en el GADM esté protegido por los derechos de autor y requiera licencia de uso o, en su lugar sea software de libre distribución y uso.

13. POLÍTICA DE GESTIÓN DE RIESGOS

Art. 215 Los inventarios de activos ayudan a garantizar la vigencia de una protección eficaz de los recursos, y también pueden ser necesarios para otros propósitos del GADM, como los relacionados con sanidad y seguridad, seguros o finanzas (administración de recursos). El proceso de compilación de un inventario de activos es un proceso importante de la gestión de riesgos. El GADM debe contar con la capacidad de identificar sus activos y el valor relativo e importancia de los mismos. Sobre la base de esta información, el GADM

puede entonces, asignar niveles de protección proporcionales al valor e importancia de los activos.

Art. 216 Los propietarios de la información y jefes departamentales son conjuntamente responsables de desarrollar un plan de gestión de riesgos corporativo de los sistemas a su cargo, preferencialmente en un periodo de un año.

Art. 217 Como parte del plan de gestión de riesgos se debe identificar las aplicaciones de alta criticidad para la recuperación ante los desastres. Es importante identificar:

- Áreas vulnerables
- Pérdida potencial
- Selección de controles y objetivos de control para mitigar los riesgos, indicando las razones para su inclusión o exclusión (seguridad de datos, plan de contingencia, procedimientos y estándares de operación)

Art. 218 El plan de gestión de riesgos debe tener un propósito claramente definido y delimitado, existiendo dos posibilidades: cumplimiento con los controles y/o medidas de protección o la aceptación del riesgo.

Art. 219 El cumplimiento satisfactorio del proceso de evaluación del riesgo se caracteriza por:

- Identificación y clasificación correcta de los activos a ser protegidos.
- Aplicación consistente y continua de los controles y/o medidas para mitigar el riesgo (seguridad efectiva de datos, recuperación ante desastres adecuado)
- Detección temprana de los riesgos, reporte adecuado de pérdidas, así como una respuesta oportuna y efectiva ante las perdidas ya materializadas.

Art. 220 La gerencia responsable puede obviar algún control o requerimiento de protección y aceptar el riesgo identificado solo cuando ha sido claramente demostrado que las opciones disponibles para lograr el cumplimiento han sido identificadas y evaluadas, y que éstas tendrían un impacto significativo y no aceptable para el GADM. La aceptación de riesgo por falta de cumplimiento de los controles y/o medidas de protección debe ser documentada, revisada por las partes involucradas, comunicada por escrito y aceptada por las áreas responsables de la administración de la seguridad.

FORMULARIO PARA LA CREACIÓN DE CUENTAS DE USUARIO

CREACIÓN ☐ MODIFICACIÓN ☐ ELIMINACIÓN ☐

No.	Nombre y Apellidos Usuario	Dependencia	ID-Usuario	Consecutivo	Observaciones

FORMULARIO PARA LA SOLICITUD DE CREACIÓN DE CUENTAS DE USUARIO

DE: _____
Jefe o Director de Sección, Dependencia u Oficina

PARA: _____
Secretaría General o Ente Encargado

FECHA DE SOLICITUD:

DD	MM	AAAA

	CREACIÓN		MODIFICACIÓN		ELIMINACIÓN

NOMBRES: _____ APELLIDOS: _____

CARGO: _____ USUARIO: _____

OBSERVACIONES: _____

_____

Jefe o Director de Sección, Dependencia u Oficina

Secretaría General o Ente Encargado

FORMATO PARA SEGUIMIENTO DE LAS PLÍTICAS DE SEGURIDAD DE LA INFORMACIÓN

Logotipo de la Institución	Descripción/Titulo	Versión	

Nombres y Apellidos	Cargo/Asignación	Respaldos		Fecha de Evaluación	Firma	Fecha de Aprobación	Observaciones
		SI	NO				

Firma de Responsable del Área

Firma de la Persona que Aprueba

FORMATO DE SOLICITUD DE ADQUISICIÓN, REPARACIÓN, ACTUALIZACIÓN, MANTENIMIENTO O CAMBIO DE MATERIALES Y EQUIPOS

Fecha de Solicitud	Día	Mes	Año	Tipo de Solicitud	Adquisición		Revisión		
					Actualización		Cambio		
					Mantenimiento		¿Otro?		
Solicitante				Cargo			Dependencia		
Tipo				Discriminación					
Equipo		Herramienta		Marca					
Materiales		Papelería		Modelo					
Insumos		Aseo		Serie					
Otro		Otro		Nro. en Inventario					
¿Cuál?				Ubicación					
				Responsable					
Breve descripción de la razón de la solicitud o del contenido de la solicitud									
			Día	Mes	Año				
Nombre del servidor o funcionario que recibe la solicitud	Cargo del servidor o funcionario		Fecha de recibo de la solicitud			Firma del servidor o funcionario que recibe la solicitud			
Concepto del servidor o funcionario que recibe la solicitud			Aprueba			No Aprueba			
Para uso exclusivo del proceso de Gestión de Bienes y Servicios									
Servidor / Contratista para atender la solicitud						Nro. de orden			
Fecha de solicitud	día		mes	año		Hora			
Para uso exclusivo del Servidor / Contratista									
Fecha de solicitud	día		mes	año		Hora			
Descripción de lo realizado						Firma del Servidor / Contratista			
Para uso exclusivo del solicitante									
Nombre de quien recibe	Cargo					Dependencia			
Fecha de entrega	día		mes	año		Hora:			
Fue recibido a satisfacción									
A la espera de capacitación para el uso correcto									
Queda pendiente por repuestos y partes									
Queda pendiente para ser retirado y reparado en el taller del contratista									
						Firma de recibo			

FORMATO DE SOLICITUD TÉCNICA PARA DAR BAJA A UN ACTIVO INFORMÁTICO

Dependencia					
Fecha de solicitud	DD	MM	AAAA	**Nro. De Solicitud**	
Nombre del Funcionario					
Cargo del Funcionario					
Nombre del Jefe Inmediato					
Características del Bien Informático					
Descripción:					
Marca	**Modelo**	**Nro. De Inventario**	**Nro. De Serie**	**Valor estimado**	**Motivo de Baja**