Auditoría de seguridad informática siguiendo la metodología OSSTMMv3: caso de estudio.

Cristian L. Bracho, Fabian G. Cuzme
{clbrachoo, fgcuzme}@utn.edu.ec
Universidad Técnica del Norte

***Abstracto*— En este artículo se trata de explicar el proceso de aplicación de una auditoría de seguridad informática, tomando como referencia las recomendaciones de la metodología OSSTMM versión 3 que engloba 5 canales fundamentales; para la comprensión de su aplicabilidad en un entorno práctico se tomó como caso de estudio al Gobierno Autónomo Descentralizado del Cantón Mira. La metodología permite medir la seguridad actual de cinco canales diferentes, los mismos que son: humano, físico, comunicaciones inalámbricas, telecomunicaciones y de redes de datos; así mismo se consideran tres medidas importantes para el cálculo de cada canal: la porosidad (OpSec), los controles y las limitaciones; en donde los resultados finales una vez realizado el análisis pertinente, permiten determinar los valores numéricos de cada uno de estos ítems, siendo necesario acogerse a las recomendaciones de los tipos de pruebas que la metodología recomienda para calcularlos. Los resultados que se obtienen una vez aplicada la metodología permiten comprender en cada ámbito las deficiencias o excesos de controles operacionales de seguridad que se manejan en una empresa u organización, siendo un punto importante para controlar las vulnerabilidades que se detecten internamente y poder solucionarlas en su debido momento.**

***Palabras Clave*- auditoria, controles, canales, limitaciones, OSSTMM, porosidad, seguridad**

I. INTRODUCCIÓN

La administración de justicia en la sociedad se ha visto profundamente transformada con la aparición de las nuevas tecnologías de la información y las comunicaciones (TICs); las omnipresentes computadoras interconectadas en la red mundial llamada Internet son el signo más evidente del impacto que tiene hoy. Según [2], para las telecomunicaciones, el tráfico comercial y el entretenimiento, estás tecnologías son prácticamente indispensables. Sin la ayuda de esta valiosísima herramienta, en la actualidad es prácticamente imposible alcanzar resultados económicos aceptables y beneficiosos, tanto como para la administración en particular, como para la administración de la justicia en la sociedad en general; por lo tanto este principio es perfectamente aplicable al sistema judicial ecuatoriano, que para poder cumplir con si función de administrar la justicia, debe tratar con información en cantidades crecientes.

El medio electrónico se ha convertido en un blanco para cometer diferentes actos ilegales tales como: extorsión, robo, fraude, suplantación de identidad, entre otros [2]. La delincuencia Informática es difícil de comprender ya que a menudo se la considera como una conducta olvidada por la legislación, porque implica la utilización de diversas tecnologías para la consecución del delito.

Enrique Mafla, [3] experto en Seguridad Informática, sostuvo que no existen sistemas informáticos seguros. "Incluso han hackeado a la Central de Inteligencia Americana (CIA) y la Oficina Federal de Investigación (FBI, por sus siglas en inglés)".

Según [3], en Ecuador se empezó a hablar de delitos informáticos en el año 2009, desde entonces, las autoridades han registrado 3143 casos, cifra que contempla los robos denunciados hasta el primer trimestre del año 2011; pero existiría un subregistro de aquellas personas que no reportaron la pérdida. Pichincha es la provincia que más registra delitos informáticos, muy por encima de Guayas y del resto del país; siendo dicha provincia la que tiene mayor acceso a Internet, contemplando alrededor del 30% de su población conectada, seguida de Azuay con un 16%.

En el 2011 el Director Nacional de la Unidad de Tecnologías de la Información de la Fiscalía, manifestó que hasta esa fecha, el uso de servicios conectados a la red el principal motivo del aumento de casos de delitos informáticos, señalando como delitos más frecuentes la apropiación ilícita de montos o valores, falsificación electrónica de identidad y daños informáticos (cuando el custodio es un funcionario público) [3]

En una investigación realizada por [4], se señala que en el año 2013 se cometieron alrededor de 1013 fraudes a través de cajeros automáticos y páginas web, clonación de las bandas magnéticas de las tarjetas de crédito. Aunque no existen cifras exactas de la cantidad de dinero que se pierde por este mecanismo delincuencial, según la Fiscalía General del Estado, solo en 2014, en Ecuador el robo cibernético ascendió a más de dos millones de dólares, además esta misma entidad registró 530 delitos informáticos en los primeros cinco meses del año 2016 [5], en el mismo período el año anterior se

Documento recibido el 31 de Mayo del 2017. Esta investigación se realizó como un trabajo de grado previo para la obtención del título profesional en la carrera de Ingeniería en Electrónica y Redes de Comunicación de la Facultad de Ingeniería en Ciencias Aplicadas de la Universidad Técnica del Norte.
C. L. Bracho, egresado de la Carrera de Ingeniería en Electrónica y Redes de Comunicación (teléfono: +5939-8557174; e-mail: clbrachoo@utn.edu.ec).
F.G. Cuzme, docente de la Carrera de Ingeniería en Electrónica y Redes de

presentaron 635 denuncias, si bien las denuncias presentan una disminución, se tendría que evaluar las cifras en lo que resta del año [4].

Como una medida interventiva, para frenar este foco delincuencial, la Asamblea Nacional del Ecuador ha elaborado dentro de su nuevo COIP (Código Orgánico Integral Penal), 6 normativas que pretenden solucionar o frenar en cierta medida la falta de efectividad de la Administración de la Justicia en función de este tipo de delitos. [2] manifiesta que es imprescindible que la Administración de la Justicia elabore y profundice los requerimientos necesarios para el proceso de acreditación de especialistas en la materia, dado que aunque exista la normativa, si hay falta de entendimiento en la aplicación de la ley en una actividad ilícita realizada por medios electrónicos de nada servirá la nueva normativa.

Kaspersky compañía de seguridad, detecto un malware que ha afectado a 140 organizaciones de 40 países diferentes, entre ellos Estados Unidos, Francia, Ecuador, Kenia y el Reino Unido los cinco países más afectados. En Ecuador hay al menos 9 instituciones, según este informe [12]. Lo que conlleva a considerar la seguridad de la información como un punto importante para las organizaciones.

II. SEGURIDAD INFORMÁTICA

Es común hablar de seguridad informática y de seguridad de la información como si fueran la misma cosa y, a primera vista, parecería 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 a manejarla a través de un sistema informático [8]. Sin embargo, aunque tengan la necesidad de trabajar en armonía, cada uno de estos aspectos tiene objetivos y actividades diferentes.

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 [7]. 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.

Por otra parte, seguridad de la información se refiere a todas aquellas medidas que procuren resguardar la información ante cualquier irregularidad [7]. 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.

A. Auditoria de Seguridad Informática

Una auditoría de seguridad informática o auditoría de seguridad de sistemas de información, 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 [9].

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 del sistema, 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 [9].

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 [1].

Fase de Inducción

En esta fase, el analista comienza la auditoría entendiendo los requisitos, el alcance y las limitaciones de la misma en dicho alcance. A menudo, el tipo de prueba se determina mejor después de esta fase [1].

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 [11].

Fase de Indagación

Cuando ya se ha completado la fase de interacción, 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. [11]

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 [1].

B. Legislación Ecuatoriana que Regula los delitos Informáticos

A pesar de que en el Ecuador no se tomaba en cuenta a los delitos informáticos en materia de jurisprudencia, en la actualidad en la legislación ecuatoriana se amparan leyes y decretos que establecen apartados y especificaciones acorde con la importancia de la información y de las tecnologías, entre ellas tenemos:

- 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)

En base a declaraciones de [6], los Departamentos tanto de la Fiscalía General del Estado como los de la Policía Judicial sirven como puntos de contacto nacionales para una cooperación internacional formal o informal basada en redes transaccionales de confianza entre los agentes de aplicación de la Ley; lo cual es posible mediante la aplicación del artículo 226 de la Constitución y la Ley de Comercio Electrónico Firmas Electrónicas y Mensajes de Datos.

La cooperación multinacional de grupos especiales multinacionales puede resultar ser particularmente útil; y efectivamente existen casos en que la cooperación internacional ha sido muy efectiva en la resolución de algún tipo particular de delito electrónico.

III. CASO DE ESTUDIO

En esta parte se hace una breve descripción de los principales datos de relevancia del Gobierno Autónomo Descentralizado del Cantón Mira (GADM-Mira), basándose en la información proporcionada por la persona encargada del Área de Sistemas, quien se encarga de administrar toda la infraestructura de la red de datos la entidad, y visitas técnicas a las instalaciones físicas donde se encuentran los diferentes dispositivos de comunicaciones.

A. Red Activa Actual

La red LAN está funcionando aproximadamente desde finales del año 2007 y tomando en cuenta que su actual edificación fue reconstruida, ésta fue proyectada pensando en los nuevos avances tecnológicos y en el uso de una red LAN de datos, para ello se construyó dos ductos, para la distribución del cableado estructurado que viene desde el cuarto de telecomunicaciones hacia las diferentes plantas del edificio; 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 es de tipo Ethernet y posee una distribución topológica tipo árbol como se aprecia en la Fig. 2. Al momento de su implementación se pensó en una red escalable en el tiempo, teniendo actualmente 75 puntos de red para computadoras de escritorio y portátiles.

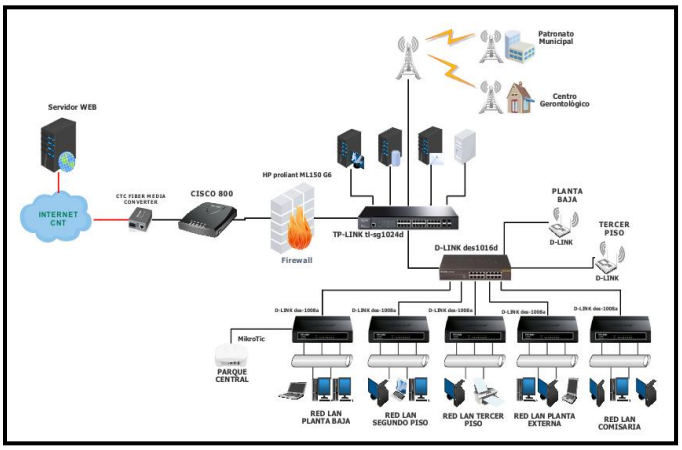

Fig. 1. Topología física de la red LAN del GADM-Mira

B. Equipos de enrutamiento

El GADM-Mira no cuenta con un equipo propio de enrutamiento, mantiene un router 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 a los usuarios de la red LAN mediante el uso de enrutamiento estático.

C. Enlace WAN

El GADM-Mira posee un contrato por concepto de servicios de Internet con la empresa CNT E.P. con un ancho de banda total de 13 Mbps simétricos por medio de una conexión de Fibra Óptica monomodo sin backup, como se puede ver en la Fig. 3. Para control del tráfico de red tanto de entrada como de salida desde y hacia la Internet se hace uso del servicio de Firewall.

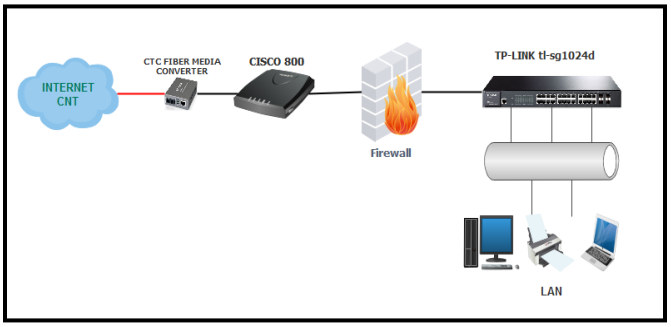

Fig. 2. Conexión hacia la Internet del GADM-Mira

D. Direccionamiento

El direccionamiento asignado para los equipos de comunicación, los ordenadores y/o dispositivos terminales del GADM-Mira hace uso de un direccionamiento clase C, teniendo así 254 direcciones IP disponibles para hosts, a la fecha no se requiere más de 100 direcciones disponibles por el

hecho de ser una red parcialmente pequeña, pero si se ha considerado un porcentaje de escalabilidad en el tiempo.

E. 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 que empieza por el switch de core, luego al switch de distribución y finalmente a los switches de acceso, como se mostró en la Fig. 2. En caso de necesitar más puertos para las estaciones de trabajo se deja un puerto libre en el 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 estaciones de trabajo requeridas para cada planta del edificio.

F. 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 físicamente en el cuarto de telecomunicaciones. 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, el servicios web y hosting para cuentas de correo electrónico son prestados por la empresa NIC.EC.

G. Enlaces Inalámbricos

El GADM maneja dos enlaces principales, uno de radiofrecuencia, con su respectivo back-up que se encuentra 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, con la finalidad de aprovechar la elevación que tiene dicha infraestructura, en donde se puede repartir de mejor manera varios radioenlaces a diferentes instituciones y dependencias que forman parte de la jurisdicción administrativa de la Institución, facilitando así su conexión al servicio de Internet. El otro enlace que brinda el GADM-Mira es el que está dirigido a la ciudadanía de forma gratuita, ofreciendo el servicio de Internet gratuito o Wi-Fi Zone en el parque central de la cuidad.

H. Gestión del Software, Hardware y Antivirus

La gestión del software se realiza manualmente en el ordenador que presente problemas, o en caso de que un nuevo funcionario vaya hacer uso de la misma 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 instala en ese momento, y para finalizar, el nuevo empleado debe firmar un acuerdo de responsabilidad de uso del computador.

La gestión del Hardware se la lleva a cabo de forma semiautomática, por lo que los registros se los lleva con la ayuda de una hoja de Excel, en donde se registran ciertas características importantes como: marca, modelo, etc. En caso de presentar problemas con el equipo informático se da solución inmediata en caso de que el problema no sea de gravedad, caso contrario el equipo se lo traslada al departamento informático para su reparación. De igual forma se llevan procesos sistematizados en caso de que haya la necesidad de dar de baja a un equipo informático, cuando ya haya cumplido su vida útil dentro de la Institución.

Para la gestión del Antivirus, hace un año se la realizaba mediante un servidor (RAID 0) para la administración del antivirus y sus respectivas actualizaciones en cada uno de los ordenadores; actualmente se realiza de forma manual tanto la instalación de todo el paquete de antivirus en cada ordenador, como su actualización. La empresa que provee de este servicio es ESET con un contrato por un año, así que el GADM-Mira 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.

I. 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

IV. APLICACIÓN DE LA METODOLOGÍA

Es necesario indicar que el caso de estudio considerado para la aplicación de la presente metodología es con la finalidad de obtener resultados reales de la aplicación de la misma. Sin embrago, se pueden seguir los pasos aquí descritos para adaptarla a cualquier ambiente organizacional en la que se requiera obtener información importante de una auditoria de seguridad informática, aplicándola en todos los ámbitos de una organización.

A continuación se hace una breve descripción de 7 pasos que se deberían seguir para llevar a cabo una prueba de seguridad exitosa [1]:

1. Definir lo que se 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, en donde se deben incluir los mecanismos de protección y los procesos o servicios construidos en torno a los activos**.** Esto se conoce como la **Zona de enfrentamiento.**
3. Definir todo fuera de la zona de enfrentamiento que es necesario para mantener a los activos operativos, tales como: electricidad, alimentos, agua, aire, suelo estable, información, legislación y reglamentos; y los ambientes y cosas con las que puede trabajar. Eso se conoce como el **alcance** de la prueba.
4. Definir como el alcance interactúa dentro de sí y con el exterior, para ello es necesario fraccionar los activos dentro

del alcance conforme la dirección de las interacciones tales como: del interior al exterior, del exterior al interior, en el interior para el interior, etc. Esto se conoce como los **vectores**, idealmente, cada vector debería considerar una prueba separada con una duración corta, antes de que el ambiente de la prueba presente cambios notables.

5. Identificar los equipos que serán necesarios para cada prueba. Dentro de cada vector, las interacciones pueden ocurrir en varios niveles, mismos que se clasifican según su función en cinco **canales.** Los canales se los puede apreciar de mejor manera en la tabla 1.
6. Determinar la información que se desea obtener de la prueba. El **tipo de prueba** debe ser definido de forma individual, sin embargo [1] identifica seis tipos: Blindaje o Hacking Ético, Caja Negra, Caja Gris, Caja Blanca, Secuencial y de Inversión; de los cuales, dependiendo de la cantidad de información que el auditor conoce acerca de los objetivos y lo que el objetivo espera de la prueba, se deberá definir de forma individual la que más se adapte a las necesidades del proceso a desarrollarse en la evaluación de cada uno de los canales.
7. Asegurar que la prueba de seguridad cumpla con **las normas judiciales,** esto con el fin de asegurar que el proceso que se lleve a cabo no genere malentendidos, confusiones o falsas expectativas.

TABLA 1
CLASIFICACIÓN DE LOS CANALES

Clase	Canal	Descripción
Seguridad Física (PHYSSEC)	Humano	Comprende el elemento humano de la comunicación donde la interacción es tanto física o psicológica.
	Físico	Comprende el elemento tangible de la seguridad donde la interacción requiere esfuerzo físico o un transmisor de energía para manipular.
Seguridad Inalámbrica (SPECSEC)	Inalámbricos	Comprende todas las comunicaciones electrónicas, señales y emanaciones que tienen lugar sobre el espectro electromagnético EM.
Seguridad en las Comunicaciones (COMSEC)	Telecomunicaciones	Comprende todas las redes de telecomunicación, digitales o analógicas, donde la interacción se lleva a cabo a través de un teléfono determinado o similar a las líneas de la red telefónica pública.
	Redes de datos	Comprende todos los sistemas electrónicos y redes de datos donde la interacción se lleva a cabo a través de un cable establecido y líneas de la red cableadas.

A. Métricas de la Seguridad Operacional

La información de cada uno de los canales auditados se encuentra resumida en el Rav, que no es nada más que el balance de la porosidad, los controles y las limitaciones. Cabe señalar que para el cálculo del valor final de la seguridad actual se lo puede realizar de dos maneras: una de manera manual (aplicando varias fórmulas), o de manera automatizada (haciendo uso de una hoja de Excel).

La hoja de cálculo del Rav se la puede descargar del sitio web oficial de ISECOM (http://www.isecom.org/research/ravs.html), en la cual se debe ingresar los valores numéricos encontrados de cada ítem y el valor de la seguridad actual se obtiene de forma automática.

Para calcular el valor numérico de la seguridad actual de cada canal, que es la medida que permite evaluar el porcentaje de eficiencia de los controles operacionales implementados para cada uno, es necesario tomar en cuenta las recomendaciones que dicta la metodología para ponderar por separado cada uno de los ítems por los que está compuesto [1]:

- Porosidad: se mide como la suma de visibilidad (P_V), acceso (P_A) y confianza (P_T).
- Controles
  - ✓ Clase A: autenticación (LC_{Au}), indemnización (LC_{Id}), resistencia (LC_{Re}), subyugación (LC_{Su}), continuidad (LC_{Ct}).
  - ✓ Clase B: no-repudio (LC_{NR}), confidencialidad (LC_{Cf}), privacidad (LC_{Pr}), integridad (LC_{It}) y alarma (LC_{Al})
- Limitaciones: vulnerabilidad (L_V), debilidad (L_W), preocupación (L_C), exposición (L_E) y anomalía (L_A).

Para encontrar los valores de la debilidad y la preocupación es necesario hacer referencia a la Figura 3, de donde se toma los siguientes criterios:

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

Fig. 3. Relación de la Porosidad, Controles y Limitaciones

La debilidad se calcula contabilizando cada defecto o error en los controles interactivos o de Clase A: $(FC_{Au})(FC_{Id})(FC_{Re})(FC_{Su})(FC_{Ct})$ Por lo tanto:

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

La preocupación se calcula contabilizando cada defecto o error en los controles de proceso o de Clase B: $(FC_{NR})(FC_{Cf})(FC_{Pr})(FC_{It})(FC_{Al})$ Por lo tanto:

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

El valor de la seguridad actual se mide en base a un nivel de referencia de 100rav, donde más de 100rav significa que se invierte un costo demasiado en controles, y menos de 100rav significa que los controles operacionales adoptados por la

entidad protegen a todo el sistema del canal auditado, pero con varias limitaciones.

Pruebas realizadas

Para este apartado es necesario indicar que sólo se muestra un ejemplo de la utilización de la hoja de cálculo del RAV en el canal humano, para los demás canales el procedimiento a seguir es el mismo.

Pruebas de Seguridad Humana

En primer lugar, para tener un punto de partida para evaluar este canal fue necesario aplicar una encuesta a 10 empleados que interactúen en mayor frecuencia con el Área de Sistemas del GADM-Mira, mismos que se encuentran comprendidos por los departamentos del proceso habilitante de apoyo tomados de su Organigrama Institucional por Procesos.

Para calcular el valor de la porosidad en este canal, fue necesario aplicar varias técnicas de ingeniería social tales como: observación directa, observación y persuasión, y llamadas telefónicas falsas; esto con el fin de obtener los valores de la visibilidad, acceso y confianza, mismos que se resumen en la siguiente tabla.

TABLA 2
CÁLCULO DE LA POROSIDAD

POROSIDAD u Op-Sec		
Ítem	**Prueba**	**Total**
Visibilidad	Contabilizar qué departamentos o áreas del GADM-Mira están autorizados a realizar interacciones con el cuarto de telecomunicaciones	5
Acceso	Contabilizar los escenarios donde puede ocurrir una interacción sin que se necesite una autorización del empleado guardián de la información generada en su estación de trabajo	4
Confianza	Contabilizar el acceso a la información o a los activos físicos de empleados que no generaron o están a cargo de los mismos respectivamente	3

El siguiente paso para definir el RAV es calcular los controles, que no son nada más que los mecanismos de seguridad puestos en marcha para proteger las operaciones, los resultados de estas medidas operacionales se resumen a continuación en la siguiente tabla.

TABLA 3
CÁLCULO DE LOS CONTROLES

CONTROLES		
Controles de interacción o de Clase A		
Ítem	**Prueba**	**Total**
Autenticación	Contabilizar los métodos por los cuales se puede interactuar con el personal de recepción	4
Indemnización	Contabilizar los documentos legales a los que deben someterse los empleados del GADM-Mira para resguardar la información generada o manejada por sus empleados	4
Resistencia	Contabilizar los empleados que permiten acceder sin autorización a los activos del cuarto de telecomunicaciones	1
Subyugación	Contabilizar los activos que pueden ser comunicados a través de canales en los cuales los controles no son necesarios, pueden ser eludidos o ignorados	0
Continuidad	Contabilizar el personal que genera conflictos en cuanto a retrasos de acceso	1
Controles de Proceso o de Clase B		
Ítem	**Prueba**	**Total**
No-repudio	Contabilizar quiénes del personal de recepción identifican y registran adecuadamente el acceso o las interacciones con los activos del GADM	2
Confidencialidad	Contabilizar los segmentos de comunicación con el personal dentro del alcance que son eficientes	3
Privacidad	Contabilizar los métodos eficientes para asegurar este control	1
Integridad	Contabilizar los métodos eficientes aplicados por el GADM 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 tengan conocimiento de ello.	2
Alarma	Contabilizar la utilización de sistemas de advertencia o sistemas de alarma en todo el alcance	3

A continuación, se deben ponderar las Limitaciones, mismas que se calculan de forma individual, para ellos se siguió el procedimiento mostrado en la siguiente tabla.

TABLA 4
CÁLCULO DE LAS LIMITACIONES

LIMITACIONES		
Ítem	**Prueba**	**Total**
Vulnerabilidad	Contabilizar las fallas o errores por las cuales una persona o proceso puede ganar o denegar el acceso a los demás	2
Debilidad	Contabilizar las posibles fallas o errores que pueden presentarse en los controles de Clase A	3
Preocupación	Contabilizar los posibles defectos o errores que puedan presentarse en los controles de Tipo B	3
Exposición	Contabilizar las acciones injustificadas, fallas o errores que proporcionen una visibilidad directa o indirecta de los activos dentro del alcance	3
Anomalías	Contabilizar los elementos desconocidos que no pueden tomarse en cuenta en las operaciones normales del GADM	3

Una vez que ya se han obtenido todos los valores individuales de cada ítem, se debe ingresar los mismos en los espacios en blanco dispuestos en la hoja de cálculo del Rav, y a continuación los demás valores se mostraran automáticamente, tal como se muestra en la Figura 4.

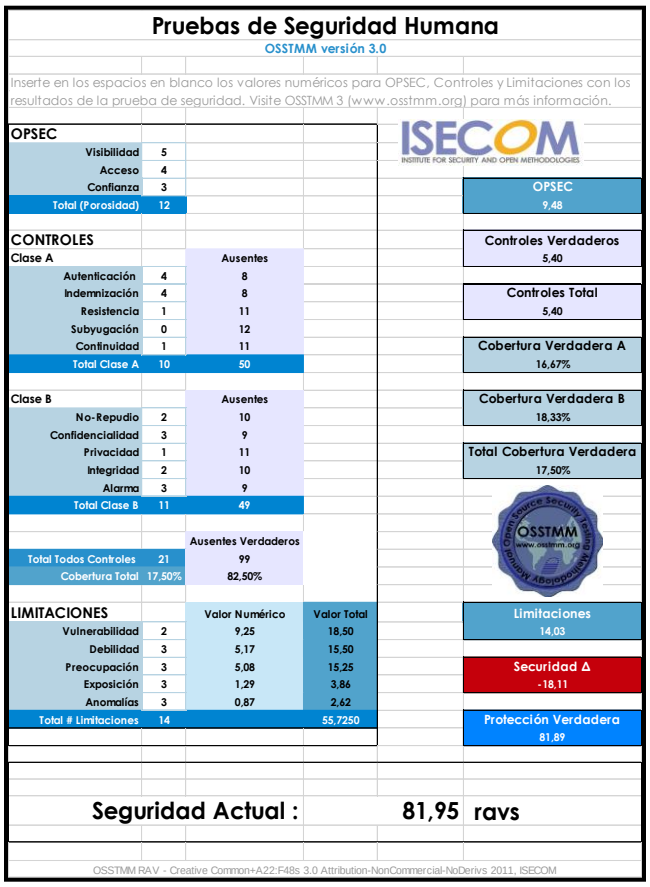

Fig. 4. Resultados obtenidos en la auditoria del canal humano en el GADM Mira

Resultados de las Pruebas de Seguridad Física, Inalámbrica y de Redes de Datos

En la siguiente tabla se resume los valores numéricos obtenidos para la Porosidad, Controles y las Limitaciones, luego de haber realizado las diferentes pruebas que dicta [1].

TABLA 5
VALORES NUMÉRICOS DE LAS MÉTRICAS OPERACIONALES

SEGURIDAD OPERACIONAL			
Canal / **Ítem**	**Físico**	**Inalámbrico**	**Redes de Datos**
Visibilidad	11	4	21
Acceso	13	3	20
Confianza	0	1	1
CONTROLES			
Canal / **Ítem**	**Físico**	**Inalámbrico**	**Redes de Datos**
Autenticación	1	5	6
Indemnización	8	0	9
Resistencia	5	1	4
Subyugación	1	0	2
Continuidad	9	1	1
No-Repudio	1	0	1
Confidencialidad	1	1	0
Privacidad	2	2	19
Integridad	3	2	0
Alarma	0	0	2
LIMITACIONES			
Canal / **Ítem**	**Físico**	**Inalámbrico**	**Redes de Datos**
Vulnerabilidad	7	0	25
Debilidad	4	3	7
Preocupación	2	2	4
Exposición	3	0	2
Anomalía	0	1	1

Pruebas de Seguridad de las Telecomunicaciones

Para este canal en particular, [1] recomienda 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

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 del GADM.

En consecuencia, para este canal se apelará al recurso que dicta [1] 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 del GADM-Mira. 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.

V. RESULTADOS

Existen dos expresiones que permiten realizar una interpretación de los valores obtenidos en la seguridad actual del canal auditado, la primera es Seguridad Δ como se muestra en la figura 4 marcada de color rojo, 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.

Las limitaciones que se identificaron en el análisis de resultados de la metodología dándoles un orden prioritario se encuentra en primer lugar las de tipo financieras por no asignar los recursos necesarios al departamento de sistemas para que se implementen los controles necesarios y en segundo lugar están las competencias estratégicas debido a que no existen planes de capacitación continua para el personal que debe ofrecer seguridad a la información de la institución, así como crear políticas de acceso a recursos de la red.

La otra expresión permite analizar el riesgo de la superficie de ataque es la Seguridad Actual cuyos valores se pueden apreciar en la tabla 6, en donde en promedio para los cuatro canales auditados posee un valor numérico de aproximadamente 80 ravs, lo que se traduce en una deficiencia del alcance de aproximadamente un 20%; y por tanto se puede asegurar que existe un porcentaje considerable de vulnerabilidades dentro del sistema de seguridad que se maneja dentro de la Institución.

TABLA 6
RESULTADOS FINALES

VALORES DE ANÁLISIS					
Canal / **Item**	**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

VI. CONCLUSIONES

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.

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.

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.

VII. REFERENCIAS

[1] P. Herzog, OSSTMM 3. Manual de la Metodología Abierta de Testeo de Seguridad, New York: ISECOM, 2010.

[2] E. Chiluiza, «Los delitos informáticos en el COIP,» *La Verdad*, 10 01 2015.

[3] Diario La Hora, «Se disparan los delitos informáticos,» *La Hora*, 21 Agosto 2011.

[4] AGN, «En Ecuador, aumentan los delitos cibernéticos,» *El Mercurio*, 02 01 2015.

[5] El Telégrafo , «En Ecuador, el 85% de los delitos informáticos ocurre por descuido del usuario,» *El Telégrafo*, 16 08 2016.

[6] S. Acurio del Pino, «inforc ECUADOR,» 29 02 2012. [En línea]. Available: http://www.inforc.ec. [Último acceso: 05 05 2017].

[7] G. A. Toth, «Implementación de la guía NIST SP800-30 mediante la utilización de OSSTMM,» Neuquén, 2014.

[8] G. Escrivá, R. Romero, D. Ramada y R. Onrabia, Seguridad Informática, Madrid: Macmillan Iberia, 2013.

[9] J. Costas Santos, Seguridad Informática, Madrid: Ra-Ma Editorial, 2010.

[10] ISACA, COBIT 5 para Seguridad de la Información, Madrid: ISACA Framework, 2012.

[11] E. Chicano Tejada, Auditoría de seguridad informática, Andalucía: IC Editorial, 2014.

[12] Karpesky Lab, «Karpesky,» 2017. [En línea]. Available: http://media.kaspersky.com/en/business-security/fileless-attacks-against-enterprise-networks.pdf.

VIII. BIOGRAFÍA

Cristian L. Bracho. Nació el 26 de Diciembre de 1 990 en la cuidad de Mira; provincia del Carchi. Realizó sus estudios primarios en la Escuela Gral. Rafael Arellano, sus estudios secundarios en la U.E. León Rúales y actualmente es egresado de la Universidad Técnica del Norte.

Realizó varios cursos en la Universidad Técnica del Norte: Armar y dar mantenimiento a computadores, 2008; Linux Básico, 2016; Bases de datos, 2016.

Fabian G. Cuzme. Nació el 14 de Noviembre de 1985 en la cuidad de Portoviejo, sus estudios secundarios los realizó en el colegio Dr. Bruno Sánchez Carreño de la misma ciudad. Ingeniero en Sistemas Informáticos de la Universidad Técnica de Manabí. Magister en Redes de Comunicación de la Pontificia Universidad Católica del Ecuador. Actualmente se desempeña como docente de la Universidad técnica del Norte en la Carrera de Ingeniería en Electrónica y Redes de Comunicación.