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:

HACKING ÉTICO PARA DETECTAR FALLAS EN LA SEGURIDAD INFORMÁTICA DE LA INTRANET DEL GOBIERNO PROVINCIAL DE IMBABURA E IMPLEMENTAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI), BASADO EN LA NORMA ISO/IEC 27001:2005.

AUTOR: BRAULIO FERNANDO ORTIZ BELTRÁN

DIRECTOR: MSC. EDGAR MAYA

IBARRA – ECUADOR

2015

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 determina la necesidad de disponer de textos completos en formato 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 DEL CONTACTO	
Cédula de Identidad	1002979985
Apellidos y Nombres	Ortiz Beltrán Braulio Fernando
Dirección	Eugenio Espejo 9-114 y Carlos Emilio Grijalva
Email	fher_ortiz_b@hotmail.com
Teléfono Fijo	062585714
Teléfono Móvil	0993648457
DATOS DE LA OBRA	
Título	HACKING ÉTICO PARA DETECTAR FALLAS EN LA SEGURIDAD INFORMÁTICA DE LA INTRANET DEL GOBIERNO PROVINCIAL DE IMBABURA E IMPLEMENTAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI), BASADO EN LA NORMA ISO/IEC 27001:2005
Autor	Ortiz Beltrán Braulio Fernando
Fecha	05 de Enero de 2015
Programa	Pregrado
Título por el que se aspira	Ingeniero en Electrónica y Redes de Comunicación
Director	Msc. Edgar Maya

2. AUTORIZACIÓN DE USO A FAVOR DE LA UNIVERSIDAD

Yo, Braulio Fernando Ortiz Beltrán, con cédula de identidad Nro. 1002979985, 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 uso del archivo digital en la Biblioteca de la Universidad con fines académicos, para ampliar la disponibilidad de material y como apoyo a la educación, investigación y extensión; en concordancia con la ley de Educación Superior Artículo 144.

III

UNIVERSIDAD TÉCNICA DEL NORTE

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

Yo, Braulio Fernando Ortiz Beltrán, con cédula de identidad Nro. 1002979985, manifiesto mi voluntad de ceder a la Universidad Técnica del Norte los derechos patrimoniales consagrados en la Ley de Propiedad Intelectual del Ecuador, artículos 4. 5 y 6, en calidad de autora de la obra o trabajo de grado denominado: **"HACKING ÉTICO PARA DETECTAR FALLAS EN LA SEGURIDAD INFORMÁTICA DE LA INTRANET DEL GOBIERNO PROVINCIAL DE IMBABURA E IMPLEMENTAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI), BASADO EN LA NORMA ISO/IEC 27001:2005"**, que ha sido desarrollado para optar por el título de: **Ingeniera en Electrónica y Redes de Comunicación** en la Universidad Técnica del Norte, 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 citada. 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:
Nombre: Braulio Fernando Ortiz Beltrán
Cédula: 1002979985
Ibarra a los cinco días del mes de Enero de 2015

IV

UNIVERSIDAD TÉCNICA DEL NORTE

DECLARACIÓN

Yo BRAULIO FERNANDO ORTIZ BELTRÁN 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.

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, reglamentos y normatividad vigente de la Universidad Técnica del Norte.

Firma:

Nombre: Braulio Fernando Ortiz Beltrán

V

UNIVERSIDAD TÉCNICA DEL NORTE

CERTIFICACIÓN

Certifico, que el presente trabajo de titulación "HACKING ÉTICO PARA DETECTAR FALLAS EN LA SEGURIDAD INFORMÁTICA DE LA INTRANET DEL GOBIERNO PROVINCIAL DE IMBABURA E IMPLEMENTAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI), BASADO EN LA NORMA ISO/IEC 27001:2005" fue desarrollado en su totalidad por el Sr. Braulio Fernando Ortiz Beltrán, bajo mi supervisión.

Es todo cuanto puedo certificar en honor a la verdad.

Msc. Edgar Maya
DIRECTOR

PREFECTURA DE IMBABURA

CERTIFICACIÓN

Ibarra, 19 de diciembre de 2014

Señores
UNIVERSIDAD TÉCNICA DEL NORTE
Presente

De mis consideraciones:

Siendo auspiciante del proyecto de tesis del Egresado BRAULIO FERNANDO ORTIZ BELTRÁN con CI: 1002979985 quien desarrolló su trabajo con el tema "HACKING ÉTICO PARA DETECTAR FALLAS EN LA SEGURIDAD INFORMÁTICA DE LA INTRANET DEL GOBIERNO PROVINCIAL DE IMBABURA E IMPLEMENTAR UN SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI), BASADO EN LA NORMA ISO/IEC 27001:2005", me es grato informar que se ha superado con satisfacción el cumplimiento de los requerimientos propuestos, por lo que se recibe el proyecto como culminado y realizado por parte del egresado BRAULIO FERNANDO ORTIZ BELTRÁN. Una vez hemos recibido la capacitación y documentación respectiva, nos comprometemos a continuar utilizando la mencionada información en beneficio de nuestra institución.

El egresado BRAULIO FERNANDO ORTIZ BELTRÁN puede hacer uso de este documento para los fines pertinentes en la Universidad Técnica del Norte.

Atentamente:

GOBIERNO PROVINCIAL DE IMBABURA
GESTION TECNOLÓGICA

Ing. Cosme Ortega
Director de Tecnologías de la Información
Prefectura de Imbabura

DEDICATORIA

El proyecto de titulación se lo dedico a Dios, a mis padres, mis abuelitos, mis hermanos, mi esposa y mí amado hijo Misael quienes han sido un pilar fundamental de apoyo y motivo de inspiración.

Braulio F. Ortiz B.

AGRADECIMIENTOS

Mi agradecimiento al Señor Dios por haberme dado unos padres y hermanos cuyo apoyo ha sido incondicional, y sobre todo las gracias a mi esposa y mi querido hijo Misael.

Mi agradecimiento a la Universidad Técnica del Norte, por haberme brindado la oportunidad de obtener un título profesional.

A los docentes de la Carrera de Ingeniería Electrónica y Redes de Comunicación de la Facultad de Ingeniería en Ciencias Aplicadas por su dedicación al servicio de la formación de futuros profesionales y sobre todo el apoyo moral.

Al Msc. Edgar Maya director de mi Trabajo de Grado por su apoyo incondicional demostrando siempre su profesionalismo, apoyo y comprensión.

A todos los funcionarios del departamento de Gestión de Tecnologías de la Información del Gobierno Provincial de Imbabura,

Braulio F. Ortiz B.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente proyecto aborda la seguridad de la información de los elementos involucrados en el procesamiento, almacenamiento o transporte de la información en el Gobierno Provincial de Imbabura.

La norma ISO/IEC 27001:2005 ha sido seleccionada como guía para el desarrollo de las actividades descritas en este documento con el objetivo de implementar un sistema de gestión de seguridad de la información.

La norma ISO/IEC 27001:2005 establece tres requisitos previos para el análisis del diseño del sistema de gestión de seguridad de la información, el primero de ellos es un inventario de activos de información del Gobierno Provincial de Imbabura, para lo cual se ha tomado énfasis en el data center como centro de operaciones y procesamiento de la información. A partir de este requerimiento se realiza el análisis de riesgos, es decir identificar las amenazas de los activos de información, y el tercer requisito es la identificación de vulnerabilidades.

El proceso de análisis de riesgos se lo realiza bajo los lineamientos estipulados en la metodología Magerit, encargada de guiar todo el proceso abarcando la clasificación de los activos, las relaciones de dependencia, la selección de las amenazas y la valoración de las mismas en base a las propiedades de la información.

La detección de las vulnerabilidades es realizada en base a técnicas de hacking ético desde una perspectiva black-box (caja negra), es decir existe un desconocimiento inicial de los sistemas a evaluar y paulatinamente mediante varios procesos descubrir las características del equipo y las respectivas vulnerabilidades. De esta forma se pretende imitar un ataque hacker desde cualquier parte del mundo con intenciones maliciosas.

Una vez se ha identificado los problemas se procede a seleccionar los controles recomendados por la norma ISO/IEC 27001:2005 para el tratamiento del riesgo de los activos de la información, finalizando con la implementación de los controles seleccionados entre ellos la política de seguridad de la información.

ABSTRACT

This project addresses the information security of the elements involved in the processing, storage or transport of information in the Gobierno Provincial de Imbabura.

The ISO/IEC 27001:2005 has been selected as a guide for the development of the activities described in this document with the target to implement an information security management system.

The ISO/IEC 27001:2005 establishes three prerequisites for the analysis of design of Information security management system, the first of which is an inventory of information assets of Gobierno Provincial de Imbabura, for which it has taken emphasis in the data center as a hub and information processing. From this requirement is done the analysis and management of risks, namely threats identify information assets, and the third requirement is to identify vulnerabilities.

The risk analysis process is done under the guidelines set forth in the Magerit methodology, which guides the whole process covering the classification of assets, dependency relations, selecting threats and evaluating them based on the properties of the information.

Detection of vulnerabilities is performed based on ethical hacking techniques from a black-box perspective, namely there is an initial lack of systems to evaluate and gradually by various processes discover the characteristics of the equipment and the respective vulnerabilities. This is intended to mimic a hacker attack from anywhere in the world with malicious intentions.

Once you have identified the problems it proceeds to select the controls recommended by the standard ISO/IEC 27001:2005 for risk treatment information assets, ending with the implementation of the selected controls including security policy information.

PRESENTACIÓN

La información es un activo de gran valor para las instituciones mucho más cuando se refiere a instituciones públicas en la que la imagen y el prestigio son recursos intangibles, que al ser afectados tanto la reputación como la confianza se perderán en los usuarios produciendo descontento en las autoridades de la organización, autoridades superiores del Gobierno y los propios funcionarios y usuarios de los servicios.

Sin duda alguna la seguridad de la información debe asegurarse, como también los elementos involucrados en la manipulación de la información. Es el tiempo se establecer oportunamente procedimientos de trabajo, operación y detección de anomalías a nivel tecnológico. Hasta el momento la seguridad de la información era confidencial y sólo las autoridades o personal experto debía conocer los procedimientos de resguardo de la información, sin embargo el punto más débil en la cadena de la seguridad de la información es el recuro humano. Es aquí en donde se debe preparar y capacitar al personal para que sean una ayuda y no un problema más en la seguridad de la información.

No se debe dejar a la suerte los procesos críticos del negocio, se debe analizar las causas y solucionarlas en base a una metodología relacionada directamente con la seguridad de la información. La norma ISO/IEC 27001:2005 es la ideal no sólo como herramienta de auditoría sino más bien como soporte a consultar y seleccionar las medidas más acertadas que la institución necesita.

CAPÍTULO I

El primer capítulo aborda la definición de los conceptos clave relacionados con la seguridad de la información necesaria para comprender y aprovechar el presente proyecto. Actualmente los programas en materia de seguridad de la información se encuentran estandarizados bajo la norma ISO/IEC 27001 como medio para la creación de un sistema de gestión de seguridad de la Información (SGSI). Se describe las leyes vigentes en el Ecuador relacionadas con el delito informático y sus principales características.

En el mismo sentido se describe la teoría y la metodología necesaria para el desarrollo del análisis de riesgos, requisito indispensable previo el diseño del sistema de gestión de seguridad de la información.

1.1 Seguridad de la información

Las instituciones o empresas independientemente de la actividad económica o productiva a la que se dediquen, basan su desarrollo en la información la misma que se considera como un activo de gran valor para la organización, debe protegerse adecuadamente debido a la exposición permanente de una gran variedad de amenazas y vulnerabilidades, colocando en riesgo la confidencialidad, integridad y disponibilidad de la misma.

Debido a que la información puede adoptar diversas formas sea escrita en papel, correo electrónico, almacenada digitalmente, transmitida mediante voz, video, medios electrónicos entre otros, también existen varias maneras por las que pueden ser sustraídas, robadas o modificadas gracias a la interconectividad de las redes.

López Neira & Ruiz Spoh, (2012) afirman en su página web que “La seguridad de la información, según ISO 27001, consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una

organización.”, es decir, asegurar la continuidad de las actividades de la organización mediante una rápida y oportuna reacción ante desastres, minimizando los daños y maximizando el retorno de las inversiones y las oportunidades de negocios. Bajo estos tres parámetros se construye la seguridad de la información.

1.1.1 Confidencialidad de la información

Acceso a la información únicamente por los usuarios autorizados. La información se reserva exclusivamente para quien posee los permisos y privilegios correspondientes que permiten acceder a dicha información, el acceso no autorizado, clandestino, fuga de información o sustracción de la misma está protegido por las leyes vigentes en el país.

1.1.2 Integridad de los datos

Garantizar que la información sea la misma en todo momento, es decir no debe ser modificada o eliminada durante la transmisión o almacenamiento. La información al ser alterada, modificada o corrupta afecta directamente con las operaciones de la institución.

1.1.3 Disponibilidad

Acceso a los activos de la información en cualquier momento por parte de usuarios autorizados. Sea la información o los servicios siempre deben estar listos y disponibles cuando los usuarios así lo requieran.

1.1.4 Autenticidad

Es asegurar que una entidad es quien dice ser, en otras palabras se debe estar seguro de la fuente de la información. Afecta a la autenticidad suplantación de identidad o manipulación del origen ya que actualmente existen ataques enfocados suplantar la identidad

de dispositivos de red de transporte de datos como son switchs, routers, destinatarios de origen y destino.

1.1.5 Trazabilidad

Consiste en conocer cuando se requiera las acciones que han realizado los usuarios y en el tiempo en que lo han hecho. Este concepto también se extiende a la capacidad del administrador de consultar en tiempo real todo lo que sucede en la red con el fin de identificar usuarios o dispositivos que estén afectando el normal funcionamiento de la red, perseguir a posibles atacantes y aprender de la experiencia en la toma de decisiones futuras en la selección de medidas de seguridad.

1.2 El delito informático

1.2.1 Introducción

Según lo afirmado en el Convenio de cyber-delincuencia del Consejo de Europa (Council of Europe, 2001), se define a los delitos informáticos como los actos dirigidos contra la confidencialidad, integridad y disponibilidad de los sistemas informáticos, redes y datos informáticos, así como el mal uso de los mismos.

Las nuevas tecnologías de información han permitido a la población el desarrollo de la economía, aumento del conocimiento, intercambio de información rápida, entre otras debido a la interconexión de la redes a nivel global, por el contrario ésta es la misma causa que ha dado paso a la rápida evolución de nuevas formas de delinquir con el inconveniente que el perjuicio puede ser aún mayor en comparación si se efectuase un acto ilegal tradicional, sumándose a ello la dificultad en la recolección de pruebas incriminatorias debido en gran parte a la ubicación física del atacante el cual puede residir en cualquier parte del mundo.

1.2.2 Elementos del delito informático

1.2.2.1 El comportamiento humano

La acción delictiva es un acto humano independientemente del tipo de delito ya sea un homicidio, una violación o un ataque informático, ante la justicia la persona como tal es responsable del delito. La diferencia radica en que los delitos informáticos no son los típicos delitos tradicionales, por el contrario son actuales en los cuales los autores poseen conocimientos avanzados de informática, redes, computadoras, programación y en ciertas ocasiones comprenden el comportamiento humano llamado ingeniería social, sumándose a todo esto en que los ataques puede ser realizados desde cualquier parte del mundo limitando enormemente la tarea de recolectar evidencia incriminatoria que sea utilizado como prueba ante un juicio.

El penalista Raúl Plascencia Villanueva (2004) afirma:

> Para la consumación de un tipo penal se requiere la confluencia de un comportamiento humano lesivo a los intereses de la sociedad, y si la persona humana es la única reconocida con capacidad para exteriorizar una voluntad dañosa, entonces, ni las cosas inanimadas ni los animales pueden ser considerados sujetos activos del delito. (p. 70).

Ante la consumación de cualquier tipo de delito la ley establece a los participantes del hecho delictivo como son el sujeto activo, el sujeto pasivo y el bien jurídico lesionado.

Se denomina sujeto activo del delito a la persona natural o jurídica cuya participación como autor, coautor, cómplice o encubridor cometa cualquiera de las infracciones penales estipuladas en el actual código integral penal ecuatoriano (COIP, 2014) en los artículos 15, 42 y 43.

El sujeto pasivo en la perpetración de un delito "Es quien sufre directamente la acción, es sobre quien recaen todos los actos materiales utilizados en la realización del ilícito, es el titular del derecho dañado o puesto en peligro" (López Betancourt, 2007, p.3). Según el artículo 16 inciso cuatro del COIP quienes pueden ser sujetos pasivos del delito son el Estado, la naturaleza, el hombre individual, grupo de personas y la sociedad.

1.2.2.2 El Bien Jurídico

De acuerdo con la definición tradicional acerca del bien jurídico tenemos el concepto dado por el Dr. Santiago Acurio Del Pino en su obra Delitos Informático: Generalidades "El objeto jurídico es el bien lesionado o puesto en peligro por la conducta del sujeto activo. Jamás debe dejar de existir ya que constituye la razón de ser del delito y no suele estar expresamente señalado en los tipos penales." (p. 20).

Uno de los objetivos del código penal es la protección de los bienes jurídicos estableciendo como delito a las conductas que los destruyen, lastiman o ponen en riesgo sin embargo gracias a la nueva era en la que los sistemas informáticos gestionan gran parte de la actividad humana se considera que "El bien jurídico en los delitos informáticos es la información en sí misma, en todos sus aspectos, como interés macro-social o colectivo, porque su ataque supone una agresión a todo el complejo entramado de relaciones socio-económico-culturales" (Carrión, 2001, p. 7).

Al considerarse a la información como bien jurídico de un sistema informático es necesario ser consciente en que dicha información puede adoptar diversas formas, tiene la facilidad de almacenarse y transportarse en diferentes medios electrónicos o físicos y al ser un bien intangible también puede poseer cierto valor económico.

1.2.2.3 La Tipicidad

Para que un hecho delictivo sea considerado como delito y merecedor de una pena debe estar descrita expresamente en la ley, es decir no se puede sancionar al sujeto activo si no existe una ley que mencione que una acción en particular este considerada como un delito.

Este era un punto crítico en la legislación del Ecuador porque con las leyes vigentes hasta finales del año 2013 no se conseguía establecer una pena a los considerados delitos informáticos simplemente porque no eran mencionados (tipificados) en la ley. Para solucionar dicha situación como método alterno se denunciaba al sujeto activo con delitos tipificados en el código penal como son robo, fraude, estafa entre otros.

1.2.2.4 El dolo y la culpa

Según se estipula en el artículo 14 de la sección Infracciones en General del Código Penal del Ecuador afirma que "La infracción dolosa, que es aquella en que hay el designio de causar daño, es:

- **Intencional:** cuando el acontecimiento dañoso o peligroso, que es el resultado de la acción o de la omisión de que la ley hace depender la existencia de la infracción, fue previsto y querido por el agente como consecuencia de su propia acción u omisión; y,
- **Preterintencional:** cuando de la acción u omisión se deriva un acontecimiento dañoso o peligroso más grave que aquél que quiso el agente."

Del mismo modo el artículo 14 menciona lo que se considera una infracción a culpa, "La infracción es culposa cuando el acontecimiento, pudiendo ser previsto pero no querido por el agente, se verifica por causa de negligencia, imprudencia, impericia, o inobservancia de ley, reglamentos u órdenes."

1.2.2.5 La Antijuricidad

La ley establece las conductas indebidas consideradas como delito, si un sujeto realiza un tipo de acción u omisión sea doloso o culposo la cual no está justificada o dicha acción no está autorizada se considera como una acción antijurídica porque va en contra de las normas, de lo estipulado en la ley y obedece a una conducta que no se encuentra permitida por ningún precepto jurídico. (Nieves, 2010)

Finalmente para que el sujeto activo sea merecedor de una pena producto de una acción ilícita tipificada en la ley, éste debe hallarse culpable del delito.

1.2.3 Legislación del Ecuador relacionadas con delitos informáticos

Desde la constitución de la república del Ecuador hasta el recientemente aprobado código orgánico integral penal en el año 2014, existen varias leyes relacionadas con la seguridad de la información siendo este último el de mayor importancia y trascendencia al tratar y sancionar las actividades ilícitas contra los sistemas informáticos, brindando mayor castigo si los sistemas afectados pertenecen al Estado Ecuatoriano o si quien atenta contra dicha infraestructura es un funcionario público. Las leyes que brindan soporte en estos temas son los siguientes:

- Constitución de la República del Ecuador
- 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 de Control Constitucional (Reglamento Habeas Data).
- Ley Orgánica de Comunicación

- Código Orgánico Integral Penal.

1.2.3.1 Constitución de la República del Ecuador

La Constitución de la República del Ecuador fue publicada en el registro oficial No. 449 el 22 de octubre del 2008, es la norma suprema que está sobre cualquier otra norma jurídica proporcionando los lineamientos para la organización del Estado, la existencia del Ecuador y quienes nos gobiernan. En ella se estipula los principios por los cuales han sido creadas todas las leyes incluyendo las mencionadas en esta sección.

La ley Orgánica de Transparencia y Acceso a la Información Pública se basa los artículos 18, 91 y 92 de nuestra Constitución garantizando el derecho a los ciudadanos de buscar, recibir, intercambiar, producir o difundir información con responsabilidad sobre sí misma, o sobre sus bienes existente en entidades públicas, o en las privadas que manejen fondos del Estado o realicen funciones públicas.

La Defensoría del Pueblo ampara y protege los derechos de los ecuatorianos en el país y fuera de él facilitando soporte ante reclamos por mala calidad o indebida prestación de los servicios públicos o privados, según lo dictamina el artículo 215.

La ley de propiedad intelectual se ampara en los artículos 322 y 402 de nuestra Constitución básicamente prohibiendo la apropiación de los conocimientos colectivos en ciencias, tecnologías y saberes ancestrales; también de los recursos genéticos que contienen la diversidad biológica y la agro-biodiversidad y finalmente no se puede otorgar derechos sobre productos derivados o sintetizados de la biodiversidad nacional.

1.2.3.2 Ley Orgánica de Transparencia y Acceso a la Información Pública

La Ley Orgánica de Transparencia y Acceso a la Información pública en el Registro Oficial Suplemento 337 del 18 de Mayo del 2004 garantizando el derecho fundamental de los

Ecuatorianos a buscar, recibir, intercambiar, producir y difundir información pública o de entidades privadas que se relacionen con el Estado.

Mediante esta ley la ciudadanía conoce lo que sucede en el país, cuales son las decisiones adoptadas, quien las toma, porque causas, uso de los recursos, rendición de cuentas, fiscalización de recursos públicos es decir se fomenta una sociedad democrática.

1.2.3.3 Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

La ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos fue publicada en el Registro Oficial Suplemento No. 577 de 17 de abril de 2002, el propósito de la ley es regular la información que circula a través de las redes de telecomunicaciones, incluyendo el comercio electrónico y protección a los usuarios.

La ley reconoce la importancia de los mensajes de datos y le concede el mismo valor jurídico que los mensajes escritos otorgándole los principios de confidencialidad, reserva y propiedad intelectual del mensaje al emisor estipulando de esta manera sanciones conforme a lo dispuesto en la ley si se viola dichos principios particularmente aquellas referidas a la intrusión electrónica, transferencia ilegal de mensajes de datos o violación del secreto profesional.

Se le atribuye a la firma electrónica el mismo valor jurídico que una firma manuscrita entendiéndose que el titular de la firma aprueba y reconoce la información contenida en el mensaje de datos y puede ser considerada como prueba ante un juicio, del mismo modo el certificado de la firma electrónica certifica la identidad del titular con la firma electrónica.

El Consejo Nacional de Telecomunicaciones "CONATEL" será la entidad de autorización, registro, regulación y acreditación de las entidades de certificación de información. La Superintendencia de Telecomunicaciones es el organismo de control de las

entidades de certificación que velará por el eficiente funcionamiento respetando la ley, podrá imponer sanciones administrativas por incumplimiento de obligaciones en el servicio entre otros.

La ley protege a los consumidores en la actividad comercial que utilicen los medios electrónicos como es el internet para la prestación de bienes o servicios, el oferente deberá presentar toda la información de los requisitos, condiciones y restricciones para que el consumidor pueda adquirir el bien o servicio, así mismo la publicidad dirigida al consumidor será regulada y deberá cumplir con lo dispuesto en la ley, el usuario podrá confirmar su suscripción o solicitar su exclusión en donde se halle inscrito y que ocasione el envío de la publicidad hasta él.

1.2.3.4 Ley de Propiedad Intelectual.

La Ley de Propiedad Intelectual publicada en el Registro Oficial N° 320 del 19 de mayo de 1998 considera la protección de las creaciones intelectuales como un derecho fundamental de los Ecuatorianos fomentando así la libre competencia y el desarrollo tecnológico y económico del país.

Esta ley fue creada para proteger las invenciones en todos los campos de la tecnología, programas de ordenador, obras audiovisuales, obras arquitectónicas, obras de artes plásticas entre otras mediante la concesión de patentes de invención o de procedimientos siempre y cuando la adquisición sea legal.

Los autores de las creaciones intelectuales pueden acogerse a la no divulgación de la información puede referirse a las características o finalidades de los productos; a los métodos o procesos de producción; la configuración y composición precisas de sus elementos; o, a los medios o formas de distribución o comercialización de productos o prestación de servicios.

Se protege la información no divulgada relacionada con los secretos comerciales, industriales o cualquier otro tipo de información confidencial contra su adquisición, utilización o divulgación no autorizada del titular

Según el artículo 83 de la presente ley también se considera como "Información no divulgada el conocimiento tecnológico integrado por procedimientos de fabricación y producción en general; y, el conocimiento relativo al empleo y aplicación de técnicas industriales resultantes del conocimiento, experiencia o habilidad intelectual, que guarde una persona con carácter confidencial".

Según los artículos tres y 346 de la presente ley el IEPI[1] es un organismo con autonomía administrativa, económica, financiera, operativa y patrimonio propio que posee la facultad para velar por el cumplimiento y respeto de los principios establecidos en esta Ley, el respeto de los derechos de propiedad intelectual, promover y fomentar la creación intelectual en todos los campos de la producción , así como la difusión de los conocimientos tecnológicos dentro de los sectores culturales y productivos; y establecer medidas preventivas que pongan en riesgo la propiedad intelectual y la libre competencia.

1.2.3.5 Ley Especial de Telecomunicaciones.

La Ley Especial de Telecomunicaciones fue publicada en el Registro Oficial N° 770 del 30 de Agosto de 1995, en la que se declara a los servicios de telecomunicaciones como un sector estratégico y de gran importancia para el desarrollo del país, por lo que es necesaria la creación de un marco legal que regule y gestione la prestación de los servicios radioeléctricos y de telecomunicaciones.

[1] **IEPI:** Instituto Ecuatoriano de Propiedad Intelectual

Esta ley regula en todo el territorio nacional la instalación y operación de los sistemas de transmisión y recepción de información video, voz y datos a través de cualquier tipo de medio de transmisión sea sistemas electromagnéticos, medios ópticos, radioeléctricos entre otros.

Mediante esta ley se establece el control en los servicios de telecomunicaciones portadores y finales, declara que los servicios públicos tienen la prioridad en la obtención de títulos habilitantes y asignación de frecuencia. El CONATEL es el organismo que protege y promueve la libre competencia, control en la prestación de servicios de las diferentes empresas y fomentar la interconexión de los diferentes prestadores de servicios.

Según el artículo 22 de la presente ley se define como Servicio Universal a la obligación de extender el acceso de un conjunto definido de servicios de telecomunicaciones a todos los habitantes del territorio nacional; si los prestadores de servicios no establecen proyectos de Servicio Universal, los fondos del FODETEL[2] financiarán dichos proyectos.

1.2.3.6 Ley orgánica de garantías jurisdiccionales y control constitucional

La ley orgánica de garantías jurisdiccionales y control constitucional fue publicada en el Registro Oficial N° 52 del 22 de Octubre del 2009

En la Constitución Política de la República del Ecuador en su artículo 92 establece la acción de hábeas data como un derecho de los ciudadanos "a conocer de la existencia y a acceder a los documentos, datos genéticos, bancos o archivos de datos personales e informes que sobre sí misma, o sobre sus bienes, consten en entidades públicas o privadas, en soporte material o electrónico."

---

[2] **FODETEL:** Fondo para el Desarrollo de las Telecomunicaciones en Áreas Rurales y Urbano-Marginales

Según los artículos uno, seis y 74 del presente reglamento, esta ley tiene la misión de regular la jurisdicción constitucional para garantizar los derechos establecidos en la Constitución y la inviolabilidad de los tratados internacionales en materia de derechos humanos y medio ambiente; como también garantizar la unidad y coherencia del ordenamiento jurídico a través de la identificación y la eliminación de las incompatibilidades normativas, por razones de fondo o de forma.

1.2.3.7 Ley orgánica de comunicación

La ley orgánica de comunicación fue publicada en el registro oficial Nº 22 el 25 de Junio del 2013 cuyas facultades corresponden el desarrollar, proteger y regular el derecho a todo tipo de información u opinión de las personas ecuatorianas, extranjeras y compatriotas residentes en el exterior a través de los medios de comunicación social en base a la correcta explotación de las tecnologías de información.

El derecho al acceso universal a las tecnologías de la información y comunicación se expresa en el artículo 35 en el que se confiere a todas las personas el derecho al acceso, la capacitación y uso de las tecnologías de información y comunicación para potenciar el disfrute de sus derechos y oportunidades de desarrollo.

1.2.3.8 Código orgánico integral penal.

El Código Penal es un instrumento del Estado para sancionar o imponer penas a quienes se hallaron culpables en la materialización de un delito tipificado en la ley, el antiguo código ha sido modificado por varias leyes entre las que constan la ley de comercio electrónico, firmas electrónicas y mensajes de datos publicada en el Registro Oficial Suplemento No. 577 de 17 de abril de 2002.

El 28 de Enero del año 2014 se aprobó el nuevo código orgánico integral penal el cual ha cambiado el sistema jurídico de varios delitos entre las que se incluyen una sección acerca de los delitos contra la seguridad de los activos de los sistemas de información y comunicación tratados desde el artículo 229 hasta el 234.

Según el código penal entre las acciones sancionadas penalmente respecto a la seguridad de la información se encuentra:

- La prohibición de revelar información contenida en bases de datos o medios semejantes a través de cualquier sistema informático que viole la privacidad de las personas.
- La información registrada obtenida ilegalmente en el origen, destino o en el interior de un sistema informático.
- El uso de cualquier mecanismo tecnológico que induzca a una persona a ingresar a un sitio web diferente al solicitado, incluidos los servicios financieros.
- El desarrollo, distribución, o ejecución de software que modifique de cualquier forma un servicio financiero induciendo a una persona a ingresar a un sitio web diferente al solicitado.
- Distribución de dispositivos electrónicos destinados en la comisión de delitos informáticos.
- Modificación del funcionamiento de sistemas informáticos y mensajes de datos.
- Ataques a la integridad de los sistemas informáticos.
- Distribución, desarrollo o uso de software malicioso.
- Destrucción o alteración de infraestructura tecnológica.
- Destrucción o inutilización de información clasificada.

Es importante recordar la naturaleza de los ataques informáticos y la forma en que son realizados, independientemente del motivo que lleva un hacker a actuar ilícitamente los ataques en su mayoría son remotos posiblemente desde otros países, por tal motivo el actual código penal en los artículos 14 y 15 sanciona toda infracción cometida en el territorio nacional y las cometidas fuera del territorio ecuatoriano cuando la infracción penal produzca efectos en el Ecuador o si es cometida en el extranjero contra una o varias personas ecuatorianas y no ha sido juzgada en el país donde se cometió el delito. (COIP, 2014).

Los artículos tipificados en el código penal en la sección tercera del capítulo tercero pretenden abarcar la mayoría de las acciones o técnicas utilizadas por los hackers informáticos en contra de sistemas, personas o bienes tanto públicos como privados; sin embargo la Asamblea Nacional en su afán de evitar dejar vacíos legales en este tema expide el artículo 190 enfatizando nuevamente en algunos puntos citados en los anteriores artículos y también añade como infracción la inutilización de sistemas de alarma, seguridades electrónicas, descifrado de calves secretas o encriptadas o uso de instrumentos de intrusión tanto físicos como informáticos.

1.3 La norma ISO/IEC 27001:2005

1.3.1 Introducción

La información es el activo de mayor valor para una organización independientemente del medio electrónico o físico donde se transmita o encuentre almacenada, debe ser un objetivo primordial la protección de dicha información y de los sistemas que la procesan.

“Para la adecuada gestión de la seguridad de la información, es necesario implantar un sistema que aborde esta tarea de una forma metódica, documentada y basada en unos

objetivos claros de seguridad y una evaluación de los riesgos a los que está sometida la información de la organización" (López Neira & Ruiz Spoh, 2012, p. 2).

ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission) están formados por los organismos de normalización más representativos de cada país, ambos desarrollaron la familia de estándares ISO/IEC 27000 que norman la manera para desarrollar, implementar, mantener y mejorar un sistema que gestione la seguridad de la información en cualquier tipo de organización a nivel mundial.

"Este Estándar Internacional proporciona un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI)". "El diseño e implementación del SGSI de una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados y el tamaño y estructura de la organización". (ISO/IEC27001, 2005).

Esta norma permite integrar al SGSI con otros estándares de gestión (ISO 9000, ISO 14001, etc.), esto quiere decir que la norma es flexible para organizaciones de todo tipo de actividad.

Asimismo adopta un enfoque por procesos de manera cíclica conocida como modelo PDCA, descrito así por las iniciales de las palabras del inglés que son Plan, Do, Check y Act traducidas sería Planear, Ejecutar, Seguimiento y Mejorar, en el cual empieza conociendo los requisitos de seguridad de la información que necesita de organización para implementar los controles necesarios que manejen los riesgos de seguridad de la información, y así una vez que el sistema se encuentre trabajando se debe monitorear y revisar periódicamente la efectividad del SGSI con el fin de corregir errores, mejorar el diseño e iniciar el ciclo nuevamente garantizando así la seguridad de la información.

1.3.2 Origen

En 1995 el BSI (British Standards Institution), publicó la norma BS 7799 que proporcionaba un conjunto de buenas prácticas para la gestión de la seguridad de su información, lo que hoy se conoce como norma ISO/IEC 27002. El inconveniente era que no existía otra norma que permita certificar el anterior esquema de certificación, por lo que en 1998 el BSI publicó la segunda parte (BS 7799-2) en la que se establece los requisitos para certificar un sistema de gestión de seguridad de la información (SGSI).

ISO e IEC conjuntamente han creado un comité técnico para tratar temas relacionados con las tecnologías de la información llamado ISO/IEC JTC 1 (Joint Technical Committee 1), el cual en el año 1999 tras revisar la norma BS 7799 se obtiene como resultado la adopción de la primera parte de la norma Británica y publicándola bajo el nombre de ISO/IEC 17799-1 en el año 2000.

La segunda parte BS 7799-2 tras empezar a ser revisada en 2002 se adopta y publica bajo el nombre de ISO/IEC 27001 en el año 2005. Finalmente en el 2007 una vez revisada y actualizada la norma ISO17799 se publica balo el nombre de ISO/IEC 27002:2005.

Debido a la importancia de proteger la información de nuevas amenazas debido a la evolución tecnológica, ISO continúa desarrollando otras normas dentro de la serie 27000 que sean utilizadas como apoyo a las organizaciones en la interpretación e implementación de ISO/IEC 27001, que es la norma principal y única certificable dentro de la serie.

1.3.3 Alcance

ISO/IEC 27001 ha sido diseñada para la adecuada selección de los controles de seguridad para la protección de la información, cumpliendo con las siguientes características:

- Los requisitos establecidos en este Estándar Internacional pueden ser aplicables a todas las organizaciones, sin importar el tipo, tamaño y naturaleza.
- ISO/IEC 27001 especifica los requisitos para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un SGSI documentado dentro del contexto de los riesgos comerciales generales de la organización.
- Especifica los requisitos para la implementación de controles de seguridad personalizados para las necesidades de las organizaciones individuales o partes de ella.
- El SGSI está diseñado para asegurar la selección adecuada y proporcionar controles de seguridad que protejan los activos de información y den confianza a las partes interesadas.
- La no implementación de ciertos controles debe ser justificada, proporcionando la información necesaria de los riesgos que la organización está dispuesta asumir.

La norma claramente indica que el éxito del SGSI depende de la aplicación de la norma ISO/IEC 27002:2005, Tecnología de la información – Técnicas de seguridad – Código de práctica para la gestión de la seguridad de la información.

1.4 La norma ISO/IEC 27002:2005

1.4.1 Introducción

Los sistemas de información realizan bien el trabajo al intercambiar datos entre los usuarios pero eso no quiere decir que sean seguros y se debe a que la seguridad involucra muchas áreas, la aplicación de medidas tecnológicas no protege completamente los sistemas de información se complementa con una adecuada gestión de los activos de información y procedimientos precisos para mantenerlo y mejorarlo.

La elaboración de un SGSI requiere la identificación de las necesidades de seguridad de la organización para lo cual es necesario analizar tres fuentes principales, la primera es identificar las amenazas de los activos, evaluar las vulnerabilidades y valorar los riesgos, otra fuente son los requisitos legales de la organización, socios, contratistas y proveedores con la sociedad, por último son los objetivos y requisitos que la organización ha establecido para mantener en funcionamiento el procesamiento de la información.

Los requisitos de seguridad identificados hasta el momento sirven como punto de partida para la adecuada selección de los controles que eliminarán las vulnerabilidades y mitigarán los riesgos asociados a los activos.

1.4.2 Objetivo y campo de aplicación

La Norma ISO/IEC 27002 es una guía de buenas prácticas obtenida como resultado de la experiencia de muchos profesionales coincidiendo en objetivos mayoritariamente aceptados para alcanzar la gestión de la seguridad de la información en el que se establece los lineamientos generales para el inicio, implementación, mantenimiento y mejora del SGSI (Gómez Fernández & Andrés Álvarez, 2012).

No todos los controles de este estándar pueden ser aplicables a todos los sistemas de gestión debido a que los requisitos de seguridad de cada SGSI son únicos y diferentes a cada organización. La norma ISO/IEC 27002 no es una norma certificable.

1.4.3 Controles de la norma ISO/IEC 27001:2005

Esta norma contiene 11 objetivos de control de seguridad, sumando en total 133 controles de seguridad. Los objetivos de control se enumeran a continuación:

1.4.3.1 Política de Seguridad de la Información

Dirigir gerencialmente la seguridad de la información en relación con los requisitos comerciales, leyes y regulaciones vigentes, cuenta con dos controles:

- Documento de política de seguridad de la información.
- Revisión de la política de seguridad de la información.

1.4.3.2 Organización de la Seguridad de la Información

1.4.3.2.1 Organización Interna

Gestionar la seguridad de la información en el interior de la organización, adoptada con ocho controles:

- Comité de gestión de seguridad de la información.
- Coordinación de la seguridad de la información.
- Asignación de responsabilidades sobre seguridad de la información.
- Proceso de autorización de recursos para el tratamiento de la información.
- Acuerdos de confidencialidad.
- Contacto con autoridades.
- Contacto con grupos de interés especial.
- Revisión independiente de la seguridad de la información.

1.4.3.2.2 Seguridad en los accesos de terceras partes

Mantener la seguridad en el momento que terceras personas accedan a la información de la organización y los medios de procesamiento de información. Posee tres controles:

- Identificación de riesgos por el acceso de terceros.
- Requisitos de seguridad cuando sea trata con clientes.

- Requisitos de seguridad en contratos con empresas externas.

1.4.3.3 Clasificación y control de activos

1.4.3.3.1 Responsabilidad sobre los activos

Asignar un propietario a todos los activos de la organización y así mantener la protección apropiada a cada uno de ellos, con tres controles:

- Inventario de activos.
- Propiedad de los activos.
- Uso adecuado de los activos.

1.4.3.3.2 Clasificación de la información

Asegurar un nivel de protección adecuado a los activos de información. Se detallan los siguientes controles:

- Guías de clasificación.
- Marcado y tratamiento de la información.

1.4.3.4 Seguridad en Recursos Humanos

1.4.3.4.1 Seguridad antes del empleo

La organización debe asegurar que al frente de cada rol en la empresa debe estar el personal apropiado y cada trabajador debe comprender sus responsabilidades.

- Roles y Responsabilidades.
- Selección y política de personal.
- Acuerdos de confidencialidad.

1.4.3.4.2 Durante el empleo

Hacer conciencia a todos los colaboradores de la organización de las amenazas y los riesgos en materia de seguridad de la información y para reducir el riesgo de error humano deben acatar la política de seguridad de la organización. Obtiene tres controles:

- Responsabilidades de la gerencia.
- Conocimiento, educación y entrenamiento de la seguridad de información.
- Proceso disciplinario.

1.4.3.4.3 Finalización o cambio del empleo.

El proceso de salida o cambio de empleo de los colaboradores de la organización debe ser ordenado y enfocado en las respectivas responsabilidades.

- Responsabilidades de finalización.
- Retorno de activos.
- Retiro de los derechos de acceso.

1.4.3.5 Seguridad Física y del Entorno

1.4.3.5.1 Áreas seguras

Evitar accesos no autorizados, daños e interferencias contra los locales y la información de la organización, tienen seis controles:

- Perímetro de seguridad física.
- Controles físicos de entradas.
- Seguridad de oficinas, despachos y recursos.
- Protección contra amenazas externas y ambientales.
- El trabajo en las áreas seguras.

- Acceso público, áreas de carga y descarga.

1.4.3.5.2 Seguridad de los equipos

Evitar pérdidas, daños o comprometer los activos así como la interrupción de las actividades de la organización, con siete controles:

- Instalación y protección de equipos.
- Suministro eléctrico.
- Seguridad del cableado.
- Mantenimiento de equipos.
- Seguridad de equipos fuera de los locales de la organización.
- Seguridad en el rehúso o eliminación de equipos.
- Retiro de la propiedad.

1.4.3.6 Gestión de Comunicaciones y Operaciones

1.4.3.6.1 Procedimientos y responsabilidades de operación

Asegurar la operación correcta y segura de los recursos de tratamiento de información, posee cuatro controles:

- Documentación de procedimientos operativos.
- Gestión de Cambios.
- Segregación de tareas.
- Separación de los recursos para desarrollo y para producción.

1.4.3.6.2 Gestión de servicios externos

Implementar y mantener un nivel apropiado de seguridad y de entrega de servicio en línea con los acuerdos con terceros. Se listan los controles:

- Servicio de entrega.
- Monitoreo y revisión de los servicios externos.
- Gestionando cambios para los servicios externos.

1.4.3.6.3 Planificación y aceptación del sistema

Minimizar el riesgo de fallos de los sistemas. Adopta los siguientes controles:

- Planificación de la capacidad.
- Aceptación del sistema.

1.4.3.6.4 Protección contra software malicioso

Proteger la integridad del software y de la información, mediante:

- Medidas y controles contra software malicioso.
- Medidas y controles contra código móvil.

1.4.3.6.5 Gestión de respaldo y recuperación

Mantener la integridad y la disponibilidad de los servicios de tratamiento de información y comunicación, para lograrlo se vale del control denominado recuperación de la información en la que recomienda realizar copias de seguridad periódicas de la información de la institución y el software.

1.4.3.6.6 Gestión de seguridad en redes

Asegurar la salvaguarda de la información en las redes y la protección de su infraestructura de apoyo con dos controles:

- Controles de red.
- Seguridad en los servicios de redes.

1.4.3.6.7 Utilización de los medios de información

Prevenir acceso no autorizado, modificaciones, evitar daños a los activos e interrupciones de las actividades de la organización. Los controles son:

- Gestión de medios removibles.
- Eliminación de medios.
- Procedimientos de manipulación de la información.
- Seguridad de la documentación de sistemas.

1.4.3.6.8 Intercambio de información

Evitar la pérdida, modificación o mal uso de la información intercambiada entre organizaciones. Recomienda cinco controles:

- Políticas y procedimientos para el intercambio de información y software.
- Acuerdos de Intercambio.
- Medios físicos en tránsito.
- Seguridad en la mensajería electrónica.
- Sistemas de Información de Negocios.

1.4.3.6.9 Servicios de correo electrónico

Asegurar la seguridad de los servicios de comercio electrónico y de su uso seguro.

- Comercio Electrónico.
- Transacciones en línea.
- Información pública disponible.

1.4.3.6.9 Monitoreo

Detectar las actividades de procesamiento de información no autorizadas.

- Registro de la auditoria.
- Monitoreando el uso del sistema.
- Protección de la información de registro.
- Registro de administradores y operadores.
- Registro de la avería.
- Sincronización del reloj.

1.4.3.7 Control de Accesos

1.4.3.7.1 Requisitos de negocio para el control de accesos.

Controlar los accesos a la información mediante la documentación de la Política de control de accesos.

1.4.3.7.2 Gestión de acceso de usuarios.

Asegurar el acceso autorizado de usuario y prevenir accesos no autorizados a los sistemas de información, posee cuatro controles:

- Registro de usuarios.
- Gestión de privilegios.
- Gestión de contraseñas de usuario.
- Revisión de los derechos de acceso de los usuarios.

1.4.3.7.3 Responsabilidades de los usuarios

Evitar el acceso de usuarios no autorizados y el compromiso o hurto de la información y de las instalaciones del procesamiento de información. Contiene tres controles:

- Uso de contraseñas.
- Equipo informático de usuario desatendido.
- Política de pantalla y escritorio limpio.

1.4.3.7.4 Control de acceso a la red

Prevenir el acceso no autorizado de los servicios de la red con siete controles:

- Política de uso de los servicios de la red.
- Autentificación de usuario para conexiones externas.
- Identificación de equipos en las redes.
- Diagnostico remoto y configuración de protección de puertos.
- Segregación en las redes.
- Control de conexión a las redes.
- Control de enrutamiento en la red.

1.4.3.7.5 Control de acceso al sistema operativo

Evitar accesos no autorizados a los computadores, recomienda seis controles:

- Procedimientos de conexión de terminales.
- Identificación y autenticación del usuario.
- Sistema de gestión de contraseñas.
- Utilización de las facilidades del sistema.
- Desconexión automática de sesiones.

- Limitación del tiempo de conexión.

1.4.3.7.6 Control de acceso a las aplicaciones y la información

Prevenir el acceso no autorizado a la información contenida en los sistemas estableciendo restricciones al acceso de la información y aislando los sistemas sensibles.

1.4.3.7.7 Informática móvil y teletrabajo

Garantizar la seguridad de la información cuando se usan dispositivos de informática móvil y teletrabajo. Adopta dos controles:

- Informática móvil y comunicaciones.
- Teletrabajo.

1.4.3.8 Adquisición, desarrollo y mantenimiento de los sistemas de información

1.4.3.8.1 Requerimientos de seguridad de los sistemas de información

Garantizar que la seguridad sea una parte integral de los sistemas de información mediante el análisis y especificación de los requerimientos de seguridad.

1.4.3.8.2 Seguridad de las aplicaciones del sistema

Evitar pérdidas, modificaciones o mal uso de los datos de usuario en las aplicaciones con cuatro controles:

- Validación de los datos de entrada.
- Control del proceso interno.
- Integridad de mensajes.
- Validación de los datos de salida.

1.4.3.8.3 Controles criptográficos

Proteger la confidencialidad, autenticidad o integridad de la información mediante el establecimiento de política de uso de los controles criptográficos y gestión de claves.

1.4.3.8.4 Seguridad de los archivos del sistema

Asegurar la seguridad de los archivos del sistema con tres controles:

- Control del software en producción.
- Protección de los datos de prueba del sistema.
- Control de acceso a los códigos de programas fuente.

1.4.3.8.5 Seguridad en los procesos de desarrollo y soporte

Mantener la seguridad del software de aplicación y la información

- Procedimientos de control de cambios.
- Revisión técnica de los cambios en el sistema operativo.
- Restricciones en los cambios a los paquetes de software.
- Fuga de Información.
- Desarrollo externo del software.

1.4.3.8.6 Gestión de la vulnerabilidad técnica

Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas mediante el control de las mismas.

1.4.3.9 Gestión de incidentes en la seguridad de información

1.4.3.9.1 Reportando eventos y debilidades de la seguridad de información

Ante la ocurrencia de algún incidente de seguridad o detección de vulnerabilidades se debe comunicar rápidamente lo sucedido que permita una acción correctiva a tiempo.

- Reportando los eventos en la seguridad de información
- Reportando debilidades en la seguridad de información.

1.4.3.9.2 Gestión de las mejoras e incidentes en la seguridad de información

Asegurar un alcance consistente y efectivo aplicado a la gestión de incidentes en la seguridad de información.

- Responsabilidades y procedimientos.
- Aprendiendo de los incidentes en la seguridad de información.
- Recolección de evidencia.

1.4.3.10 Gestión de continuidad del negocio

1.4.3.10.1 Aspectos de la gestión de continuidad del negocio

Reaccionar a la interrupción de actividades del negocio y proteger sus procesos críticos frente a grandes fallos de los sistemas de información o desastres.

- Incluyendo la seguridad de información en el proceso de gestión de la continuidad del negocio.
- Continuidad del negocio y evaluación de riesgos.
- Redacción e implantación de planes de continuidad que incluyen la seguridad de información.
- Marco de planificación para la continuidad del negocio.
- Prueba, mantenimiento y re-evaluación de los planes de continuidad.

1.4.3.11 Cumplimiento

1.4.3.11.1 Cumplimiento con los requisitos legales

Evitar los incumplimientos de cualquier ley civil o penal, requisito reglamentario, regulación u obligación contractual, y de todo requisito de seguridad con los siguientes controles:

- Identificación de la legislación aplicable.
- Derechos de propiedad intelectual (DPI).
- Protección de los registros de la organización
- Protección de los datos y de la privacidad de la información personal.
- Prevención en el mal uso de los recursos de tratamiento de la información.
- Regulación de los controles criptográficos.

1.4.3.11.2 Revisiones de la política de seguridad y de la conformidad técnica

Asegurar la conformidad de los sistemas con las políticas y normas de seguridad

- Conformidad con la política de seguridad y los estándares.
- Comprobación de la conformidad técnica.

1.4.3.11.3 Consideraciones sobre la auditoria de sistemas

Maximizar la efectividad y minimizar las interferencias en el proceso de auditoría del sistema.

- Controles de auditoria de sistemas.
- Protección de las herramientas de auditoria de sistemas.

1.5 Sistema de gestión de seguridad de la información (SGSI)

Un Sistema de Gestión de Seguridad de la Información es una herramienta que permite descubrir las vulnerabilidades de la organización, reducir los riesgos con el establecimiento y seguimiento de los controles, y minimizar la materialización de una posible amenaza que atente contra la seguridad de la información.

Gestionar los riesgos a través de un SGSI garantiza la Confidencialidad, Integridad y Disponibilidad de la información y sus sistemas de procesamiento, aportando con ellos la tranquilidad en las operaciones de la empresa ya que si se produce un incidente no deseado los daños serán mínimos y las actividades no se detendrán.

La elaboración del SGSI obedece al uso del modelo de cuatro fases PDCA descrito en la sección 1.3.1 el cual se detalla a continuación.

1.5.1 Establecimiento del SGSI

Definir el alcance y políticas del SGSI en base a los objetivos, necesidades, activos y tecnología de la empresa es decir en el diseño del sistema se define las áreas involucradas en el cambio.

Establecer una metodología de valoración de riesgo para identificar, analizar y evaluar los riesgos con el fin de seleccionar los objetivos de control y controles para gestionar y minimizar los riesgos.

Se necesita el apoyo y aprobación de la dirección para la implementación y operación del SGSI, involucra también informar acerca de los cambios a realizarse en el proceso del tratamiento del riesgo.

1.5.2 Implementación del SGSI

En esta fase se implementan los controles de seguridad seleccionados en la etapa anterior con la respectiva documentación y adecuada capacitación al personal de la empresa ya que ellos deben conocer y aprender a trabajar con los cambios realizados en el sistema, esto implica asignar la protección de los activos al personal apropiado en función de roles y responsabilidades.

Establecer la forma como se medirá la efectividad de los controles y los medios para detectar rápidamente algún incidente de seguridad. Es importante señalar que la solución más sencilla a implementar puede ser la más apropiada.

1.5.3 Seguimiento del SGSI

Reportar en el menor tiempo posible los incidentes de seguridad, como violaciones de seguridad exitosos y fallidos, cumplimiento o no de la protección de los activos por parte del personal asignado entre otros.

Revisar la efectividad del SGSI mediante el análisis de la política de seguridad, los controles, incidentes, indicadores, sugerencias y opiniones de los involucrados.

1.5.4 Mantener y mejorar el SGSI

En este punto se mejora o corrige la o las fallas encontradas en la fase de seguimiento, también es importante comunicar los cambios realizados hasta el momento a las partes interesadas. Cabe recalcar que todos los cambios deben ser debidamente documentados.

Una vez culminado el proceso y según la norma ISO/IEC 27001 que adopta el modelo PDCA nuevamente comienza el ciclo en la fase de Planificación pero en esta ocasión se parte con los resultados que arroje la etapa de mejoramiento del SGSI.

1.6 Introducción al análisis de riesgos.

Sin duda alguna la información es el activo de gran valor para la organización en el que su aseguramiento involucra la aplicación de muchos recursos tecnológicos, económicos, físicos y del comportamiento humano. La información es un elemento atractivo para quienes buscan poseerla y es cuanto más segura debe estar, a mayor importancia mayor riesgo.

En el medio actual existe una gran cantidad de empresas e instituciones dedicadas a cubrir las más variadas necesidades de la población, sin importar la actividad económica a la que se dediquen, el objetivo común es el desarrollo y el progreso para ello cada organización posee los medios que han considerado necesarios para el fiel cumplimiento de los objetivos propuestos.

Los objetivos empresariales establecen el curso a seguir y sirven para guiar, justificar y coordinar todas las actividades de la organización impulsando la creatividad, la creación de políticas, herramientas, restricciones, estrategias, acuerdos de cooperación inter-institucional, inversiones, justificación de gastos, entre otros en los cuales están inmersos el uso de recursos tecnológicos para la manipulación de la información requeridos diariamente por la institución.

Toda empresa está expuesta a varios tipos de riesgo y amenazas que atentan contra los intereses de la institución evitando así el cumplimiento de los objetivos previamente establecidos. Amenazas que pueden tener origen en el interior de la organización o fuera de ella, ser fortuitos o con mala intención colocando en riesgo intereses económicos, tecnológicos, legales y sociales.

El análisis de riesgo permite conocer a profundidad el comportamiento de los sistemas, las carencias y los elementos que posee con el fin de tomar las mejores decisiones

para gestionar eficientemente los recursos humanos, tecnológicos, económicos o asignar otros.

Las medidas de seguridad seleccionadas deben adaptarse a las necesidades de operación de la información, más no la información se adapta a las medidas de seguridad existentes. Aquí radica la diferencia en tener un sistema informático seguro o expuesto a las más simples amenazas, colocando a los activos de información a niveles de riesgo alto innecesariamente.

El análisis de riesgos no tiene como fin criticar la forma como se ha llevado la administración del sistema informático, consiste en crear conciencia y notar cómo está actualmente funcionando el sistema, en otras palabras el descubrimiento de vulnerabilidades o amenazas es algo común y no tiene que entenderse como falla en la gestión de riesgos, por el contrario se debe comprender la inexistencia de la seguridad perfecta porque lo que es seguro ahora será vulnerable en el futuro, debido al desarrollo de la tecnología, el descubrimiento de nuevas vulnerabilidades y la creación de nuevos exploits.

1.6.1 Magerit

La norma ISO/IEC 27001:2005 no establece metodologías a seguir para el análisis de riesgos, por lo cual para el desarrollo del presente trabajo se ha seleccionado la metodología Magerit (Metodología de análisis y gestión de riesgos de los sistemas de información).

El análisis de riesgos bajo las directrices de la metodología Magerit proporciona al usuario una herramienta completa, en una estructura sistemática en la que ofrece todo lo necesario para analizar los riesgos derivados del uso de las tecnologías de información y comunicación con el objetivo de descubrir cuáles son los riesgos a los que están expuestos

para conocer la realidad de la seguridad de la institución y gestionarlos para mantener los riegos bajo control.

Magerit proporciona la teoría necesaria para entender la terminología, los conceptos y los procedimientos utilizados por la metodología con un lenguaje de fácil comprensión y entendimiento para el lector. De esta manera se garantiza el aprendizaje de los procesos de la metodología y la eficiencia en el desarrollo del análisis de vulnerabilidades.

1.6.2 Software PILAR

Cada activo sometido al análisis de riesgos involucra gran cantidad de datos, conforme el procedimiento continúa y se aumenta la cantidad de activos el volumen total del proyecto adquiere un gran tamaño y gestionar toda aquella información se torna difícil, por tal razón se utiliza el software PILAR.

PILAR "Procedimiento informático lógico para el análisis de riesgos" es un software creado específicamente bajo los lineamientos de la metodología Magerit y para utilizarlo exclusivamente con esta Metodología.

La versatilidad de la herramienta en la navegación por las diferentes secciones hace de su uso una tarea fácil, todas las opciones se encuentran organizadas por categorías según los requerimientos de Magerit. La identificación y valoración de los activos y amenazas es un proceso personalizado. (Véase Figura 1)

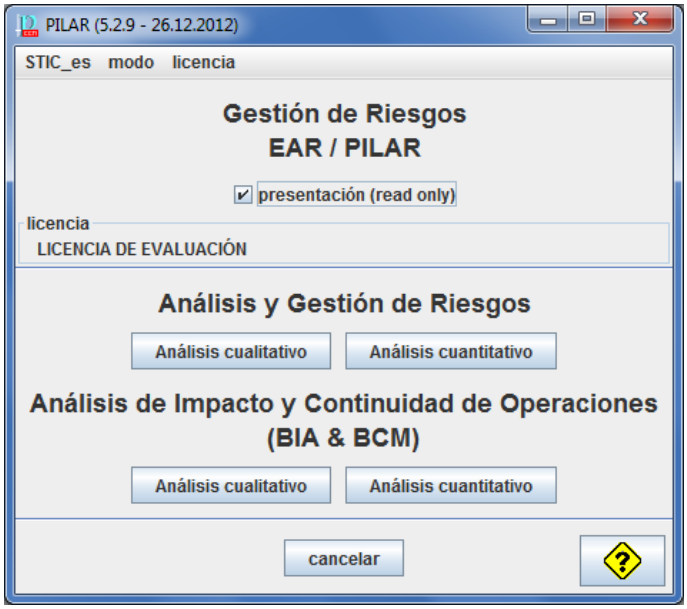

Figura 1: Herramienta PILAR 5.2.9

1.6.3 Activos de información

Se entiende por activo de información cualquier componente que procesa, modifique, transporte o almacene la información considerada valiosa para la organización y cuya falla o ausencia por cualquier índole, produzca consecuencias fatales para la organización. Según la Metodología Magerit se clasifican a los activos en doce categorías como son:

- Activos esenciales
- Arquitectura del sistema
- Datos o información
- Claves criptográficas
- Servicios
- Software o aplicaciones informáticas
- Equipamiento informático
- Redes de comunicaciones
- Soportes de información
- Equipamiento auxiliar

- Instalaciones y
- El personal.

Esta clasificación de los activos ayuda a realizar mejor el análisis de riesgos, porque dependiendo de la naturaleza de los activos existen determinadas amenazas y vulnerabilidades que ponen el peligro a los mismos. Los activos de información pueden pertenecer a varios tipos de activos si lo amerita, en el mismo sentido no es necesario cumplir con todos los tipos de activos porque no todas las empresas poseen activos para cada clase.

1.6.3.1 Activos esenciales

Para un sistema de información se considera esencial o de suma importancia a la información que se maneja y los servicios que ofrecen relacionados con datos de carácter personal, datos vitales como registros de la organización o información confidencial.

1.6.3.2 Arquitectura del sistema

Se refiere a elementos estructurales del sistema como puntos de interconexión para intercambio de información o la prestación de servicios tanto en arquitectura interna como desde el exterior.

1.6.3.3 Datos o información

La información es el activo más importante en la organización y constituye la razón de ser de los servicios permitiendo el trabajo diario mediante dispositivos de almacenamiento como bases de datos, medios magnéticos, copias de respaldos, además del transporte de un punto a otro gracias a los medios de transmisión de datos y el procesamiento o transformación de la información. (MAGERIT, 2012).

1.6.3.4 Claves criptográficas

Se utiliza técnicas criptográficas como mecanismo de protección de documentos, datos o envío de credenciales de autenticación para la identificación entre los miembros inmersos en la transferencia de información secreta.

1.6.3.5 Servicios

Gracias a la interconexión entre usuarios a través de la red informática se puede optimizar el trabajo de los colaboradores realizando más eficiente el trabajo diario. Gracias a la existencia de las redes se brinda a los usuarios herramientas informáticas que sirven a los trabajadores para que realicen su trabajo de manera eficiente.

La prestación de los servicio de red obedece a la existencia de un sistema que actúe como servidor y otro u otros como clientes. El modelo cliente/servidor permite a un equipo servidor realizar las acciones necesarias que el cliente solicita. En esta categoría se considera los servicios prestados a usuarios internos y externos.

1.6.3.6 Software o aplicaciones informáticas

Esta categoría se refiere a los programas informáticos instalados tanto a nivel de servidores y equipos de usuarios automatizando tareas directamente relacionadas con el transporte, modificación o transformación de la información.

1.6.3.7 Equipamiento informático

Son los elementos físicos que forman parte de la infraestructura informática como dispositivos de red, estaciones de trabajo servidores entre otros con el propósito de servir como instrumentos de prestación de todo tipo de servicios.

1.6.3.8 Redes de comunicaciones

Este apartado incluye las tecnologías de la información y comunicación relacionadas con el transporte de la información entre diferentes puntos dentro de la red local o redes externas mediante la contratación de proveedores de servicio de terceros.

1.6.3.9 Soportes de información

Se consideran los dispositivos físicos electrónicos o no electrónicos utilizados en el almacenamiento de la información temporal o permanente.

1.6.3.10 Equipamiento auxiliar

En esta sección se categorizan los diferentes equipos que no pertenecen a otras categorías pero sin embargo sirven de soporte o ayudan al correcto funcionamiento de activos superiores.

1.6.3.11 Instalaciones

Es la infraestructura física o los lugares en donde permanecen los sistemas de información y comunicación, sean principales o instalaciones de respaldo.

1.6.3.12 El personal

Un elemento clave a considerar en la cadena de la seguridad de la información es el recurso humano, en esta sección se refiere a los usuarios, operadores, administradores o programadores cuyas responsabilidades o funciones afecten directamente a los sistemas de información y comunicación.

1.6.4 Dependencias entre activos

Para que la información y los servicios tengan valor para la organización deben ser utilizados y valorados por los usuarios, para ello los activos vitales necesitan de muchos otros de menor jerarquía para poder funcionar, es decir cada activo depende de otros que están por debajo de éste, del mismo modo un activo de menor rango puede prestar servicio a varios activos que se encuentren sobre él. Ésta idea pone en consideración que si un activo menor es dañado y no está operante, puede afectar gravemente a la organización porque afectará directamente en la prestación de servicios superiores, por lo que dicho activo de menor jerarquía tendrá un valor alto debido a la dependencia que posee con otros activos.

1.6.5 Valoración

La valoración de los activos equivale a la asignación de un valor numérico que represente el grado de importancia del activo en la organización y el nivel de desastre que produciría si es atacado.

En el proceso de valoración de los activos se considera las propiedades fundamentales de la información como son la confidencialidad, la integridad y la disponibilidad como también la autenticidad y la trazabilidad.

- **Disponibilidad:** El análisis en base a este parámetro consiste en determinar la importancia que tendría si un activo no estuviese disponible por cortos o largos períodos de tiempo.
- **Integridad:** Se analiza la importancia que tendría si los datos fuesen modificados, en qué grado afectaría a la organización la alteración de la información sea por causas intencionadas o accidentales.

- **Confidencialidad:** Cual sería la valoración de los datos si estos son conocidos por usuarios no autorizados. Si la publicación de los datos no suponen riesgo alguno entonces no tienen mucha importancia por lo tanto la valoración en confidencialidad es baja.
- **Autenticidad:** El análisis de la autenticidad se centra en el acceso a los servicios considerando dos aspectos. El primer análisis se refiere en tener la certeza de que los servicios son en verdad utilizados por los usuarios acreditados, el segundo aspecto a tomar en cuenta consiste en garantizar que la fuente de la información es en verdad de quien dice ser.
- **Trazabilidad:** Se refiere en cuestionarse si es importante o no conocer en cualquier momento quienes han sido los usuarios que han utilizado el servicio, como también a que datos concretos o servicios han accedido.

El valor de un activo puede ser propio cuando las actividades dependen de sí mismo, y acumulado cuando un activo en la mayoría de ocasiones inferior, acumula el valor de los activos superiores a los que presta el servicio, por lo que al final del análisis el activo inferior deja de llamarse activo inferior y se lo denomina activo esencial.

1.6.6 Amenazas

Una amenaza es cualquier causa potencial intencional o fortuita que cause daño a un recurso de información, y por extensión a otros activos de información que dicho recurso brinda el servicio.

El siguiente paso consiste en la identificación de las amenazas que ponen en riesgo a los activos, realizando la valoración en función del impacto que tendría en la organización la materialización de un incidente, ya sean daños materiales o informáticos en los activos.

Según la metodología de Magerit se han clasificado las amenazas en cinco grupos que se enumeran a continuación.

1.6.6.1 Desastres naturales

Se refiere a los desastres naturales como son los terremotos, incendios, inundaciones, erupción de volcanes entre otros afectando así a los sistemas de información. Es importante conocer la zona donde se encuentran funcionando las instalaciones es decir, si el asentamiento es en una zona de alta actividad sísmica, si está a orillas del mar, cerca de algún volcán activo, entre otras.

1.6.6.2 De origen industrial

Los accidentes industriales o tecnológicos son eventos que no han sido causados por la naturaleza, por el contrario su origen se debe a las actividades propias de la organización o el medio lo que produce accidentes como explosiones, contaminación, energización, terrorismo entre otros.

1.6.6.3 Errores y fallos no intencionados

El eslabón más débil en la cadena de la seguridad de la información son las personas, debido a la imprudencia o falta de capacitación cometen errores sin intención o por la omisión de alguna medida o proceso.

1.6.6.4 Ataques intencionados

Los usuarios de los sistemas de información pueden causar daños de forma intencional mediante ataques internos al sistema, con ánimo de lucro, insatisfacción en el trabajo, curiosidad. No todas las amenazas afectan a todos los activos, existe una relación entre el tipo de activo y lo que le podría ocurrir.

1.6.6.5 Correlación de errores y ataques

El error o descuido de las personas con o sin mala intención en los sistemas informáticos combinando con las amenazas propias de loa activos pueden desencadenar daños mayores.

1.6.6.6 Valoración de las amenazas

Este proceso permite valorar la influencia del activo ante el riesgo de la materialización de una amenaza debido a que no todas las amenazas afectan a todos los activos, todo depende de los parámetros de la seguridad de la información a ser afectados.

La valoración del impacto de las amenazas obedece al análisis de dos propiedades como son la degradación y la probabilidad.

- **Degradación**

La degradación representa el nivel de daño que un incidente puede causar sobre un activo. Cualquier incidente en contra de la seguridad de la información afecta negativamente la confidencialidad, la integridad y disponibilidad de los activos, disminuyendo la capacidad de operación del mismo bien y por escalamiento de las actividades en la organización. Cualquier ataque causa la degradación del activo, es decir el activo es dañado parcialmente o en su totalidad.

Aunque no es necesario que existan atentados en contra de los activos para que éstos se degraden, el simple hecho del uso representa un gasto es decir una degradación causando la disminución paulatina de la capacidad de operación del activo y el tiempo de vida útil.

Éste factor ayuda mucho en la planeación de las acciones a tomar en caso de ocurrencia de un incidente, porque dependiendo del daño y las causas se establece el

procedimiento a seguir para subsanar y corregir a tiempo y con eficiencia las fallas en los activos afectados. Si el daño es realizado por un usuario inconscientemente entonces la degradación es baja porque el usuario no posee muchos privilegios para modificar archivos importantes o configuración del sistema.

- **La probabilidad**

Indiscutiblemente una amenaza es un riesgo potencial y latente acechando la seguridad del sistema pero no se conoce con certeza cuando atacará. La probabilidad mide la factibilidad en que se materialice una amenaza y se convierta en un desastre.

El cálculo de la probabilidad de un incidente de seguridad supone el análisis de todos los eventos posibles que pueden conllevan afectar un activo de información; es decir, cuántas formas posibles existen de dañar un activo.

1.6.7 Medidas de seguridad

El objetivo de las medidas de seguridad son para proteger a los activos de información de las amenazas mediante la disminución del riesgo y del impacto y son diseñadas e implementadas dependiendo de la forma como operan y prestan los servicios, mas no los servicios se adaptan a las medidas de seguridad que posee el sistema.

Debido a que cada activo de información trabaja de forma única y diferente respecto a los demás, las medidas de seguridad también pueden no ser las mismas entre los activos, sin embargo es posible agrupar activos semejantes y protegerlos bajo un mismo sistema de seguridad.

Los resultados del análisis de riesgos al permitir evaluar las vulnerabilidades y determinar las amenazas de los activos, posibilitan el análisis de las medidas de seguridad ideales a implementarse para la protección y garantizar las operaciones de los activos.

El análisis de las medidas de seguridad conlleva poseer mucha información previa, se parte del inventario de los activos a ser protegidos, el resultado del análisis de riesgos, las relaciones de dependencia determinando el valor del activo si es acumulado o propio diferenciando así los activos más importantes cuya protección es prioritaria, asimismo las medidas de protección difieren de la categorización de los activos.

Otras aspectos analizar son los parámetros de seguridad a proteger como es la confidencialidad, la integridad y la disponibilidad, también va a depender del tipo de amenaza al que está sometido el activo y de la probabilidad que éste se materialice.

Finalmente de las medidas de seguridad adoptadas en conjunto con las que se encuentran en funcionando hasta el momento también son sometidas a un análisis con el fin de comprobar si aún sus servicios son útiles para el sistema o por el contrario van a ser desechadas e implementarse otras mucho más eficientes.

1.6.8 Riesgo residual

Por más que se intente proteger los sistemas con las medidas de seguridad seleccionadas es imposible eliminar el riesgo en su totalidad, dicho riesgo no eliminable se lo denomina residual porque es el que sobra después de implementar las medidas de seguridad.

Según la siguiente frase de autor anónimo “La seguridad absoluta tendría un costo infinito” se aplica en esta sección y los responsables de la seguridad del sistema deben comprender y aceptar que por más medidas de seguridad que se implemente en un sistema siempre existirá un riesgo el cual no puede ser controlado, pero siempre permanecer atentos y vigilantes.

CAPÍTULO II

SITUACIÓN ACTUAL DE LA RED

2.1 Información preliminar

El Gobierno Provincial de Imbabura es una institución de derecho público encargada del desarrollo económico, social y ambiental de los seis cantones, mediante el fortalecimiento de la productividad en la agricultura, riego, cooperación internacional vialidad, manejo adecuado de los recursos naturales con el fin de mejorar la calidad de vida de todos los habitantes. (García Pozo, 2013).

Para cumplir con los objetivos planteados, la institución cuenta con el personal apropiado en la ejecución de las actividades necesarias para desarrollar y ejecutar los proyectos que la provincia necesita. Cada funcionario dependiendo del área en la que trabaja utiliza varias herramientas y servicios de red que le permiten desarrollar y producir con eficiencia en cada uno de los puestos de trabajo. Las instalaciones del Gobierno Provincial de Imbabura (GPI) se encuentra localizado en las calles Simón Bolívar y Miguel Oviedo esquina en la ciudad de Ibarra.

2.2 Atención al público

Según la Constitución de la República del Ecuador la vialidad es un servicio público siendo responsable el Estado, cuya planificación y mantenimiento del sistema vial inter-cantonal e interprovincial de Imbabura es competencia de la prefectura en representación del Estado según lo dictamina el artículo 263 de la Constitución de la República del Ecuador.

Por tal razón y en base a la autonomía política, administrativa y financiera, el Gobierno Provincial de Imbabura recibe los pagos, tasas o contribuciones especiales referentes a la matriculación vehicular en la provincia cada año.

Los usuarios que deseen realizar estos y otros trámites son atendidos en las oficinas de atención al público del edificio central del GPI ubicado en las calles Simón Bolívar y Miguel Oviedo esquina.

Entre otros de los servicios dirigidos al público en general son la emisión de certificados de no adeudar al GPI, recepción de documentos de usuarios que tramitan algún proceso en la institución, envió de oficios dirigidos a funcionarios de la institución.

2.3 Centro de procesamiento de datos (Data center)

El centro de procesamiento de datos se encuentra ubicado en el segundo piso del edificio GPI exactamente en la sección del departamento de tecnologías de la información y comunicación. Las paredes están construidas con bloque formando un área total 15 metros cuadrados cuyas dimensiones son 3m de ancho, 5m de largo y 4m de altura. En cada una de las paredes ha sido colocado puntura resistente al fuego y de fácil limpieza.

2.4 Servidor de gestión documental Quipux

Quipux es un sistema de control, organización y gestión de documentos electrónicos utilizado para agilizar los trámites administrativos, reducir el consumo de papel, disminuir el espacio que ocuparía el almacenamiento de documentos impresos y el tiempo que se demoraría en buscarlos, entre otras características importantes.

La Subsecretaria de Informática del Ecuador ha desarrollado la plataforma denominada Quipux el cual está basado en el sistema de gestión documental ORFEO,

prácticamente corresponde a un fork[3] de este software pero adaptado a las necesidades de las instituciones del Ecuador. (Véase figura 2)

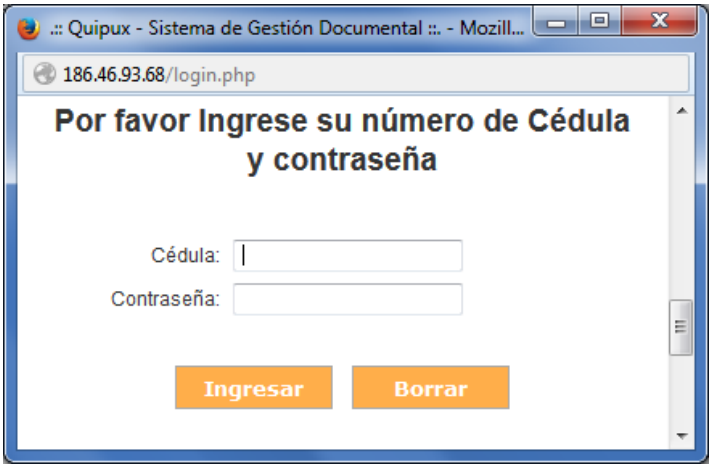

Figura 2: Sistema de Gestión documental del Gobierno Provincial de Imbabura

2.5 Servidor de correo institucional Zimbra

La institución cuenta con un servidor de correo institucional denominado Zimbra, la versión open source[4] es la actualmente utilizada brindando un entorno de configuración gráfico vía web con los siguientes servicios:

- Correo
- Calendario
- Contactos
- Mensajería instantánea
- Almacenamiento de documentos
- Mensajes en cola
- Archivos adjuntos
- Entre otros.

[3] **Fork:** Es un software desarrollado en base a otro siguiendo el mismo lineamiento u otro.
[4] **Open source:** Es el software distribuido y desarrollado libremente permitiendo el acceso al código fuente y modificarlo sin recurrir en una infracción legal.

Zimbra se encuentra instalado en un sistema operativo Linux “CentOS” versión 5, el acceso al servicio está localizado bajo el dominio http://imbabura.gob.ec:8081/#. La publicación del nombre de dominio con la respectiva dirección IP pública está a cargo de la Corporación Nacional de Telecomunicaciones al ser el proveedor de servicio de internet. (Véase figura 3)

Figura 3: Servidor de correo institucional

2.6 Servidor Web

El servidor web es una aplicación encargada de interactuar con los programas de navegación de en otras computadoras mediante la atención de peticiones con la información solicitada por los usuarios al servidor bajo los protocolos http o https. Tienen la capacidad de almacenar páginas web y todo tipo de archivos.

El Gobierno Provincial de Imbabura posee la página web www.imbabura.gob.ec por medio de la cual la ciudadanía en general puede informarse de las actividades realizadas por las autoridades de la institución en beneficio de la provincia para fortalecer los ejes de desarrollo productivo. La página web es muy dinámica con el usuario brindando varios tipos de contenido informativo a elección del usuario.

La página web www.imbaburaturismo.gob.ec es muy interactiva con el usuario enfocado en la promoción turística de todos los rincones de la provincia de Imbabura con información climática, densidad poblacional, descripción de las características principales del lugar, actividades de entretenimiento, atractivos turísticos entre otras. El usuario tiene la opción de visitar el sitio web por cantones, por actividades recreativas o indagar algún lugar o tema en particular mediante el buscador. (Véase figura 4)

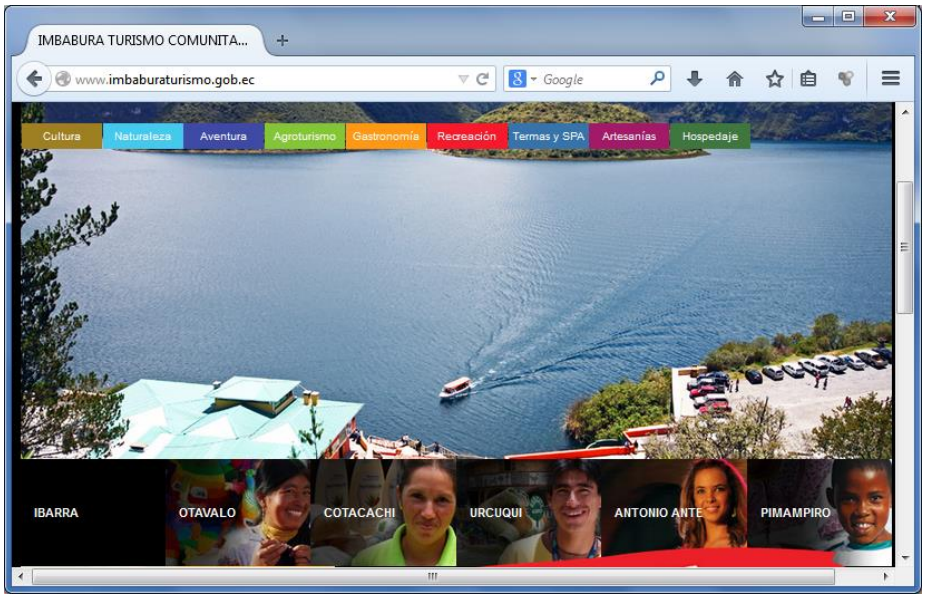

Figura 4: http://www.imbaburaturismo.gob.ec/

Las principales funciones del tercer servidor web son el brindar el servicio de correo electrónico institucional, se aloja la página web del complejo turístico cachimbiro, una página web de publicación de noticias para las comunidades de la provincia y varias aplicaciones de consulta referentes a contratos, proyectos, contratistas entre otros. (Véase figura 5)

Figura 5: Página web http://imbabura.gob.ec/chachimbiro/

2.7 Servidor Proxy

El servidor proxy intercepta las comunicaciones entre los clientes o usuarios de la red y los servidores, el tráfico es permitido o denegado en base a las reglas establecidas como medidas de seguridad. Actualmente el servidor proxy también impide las comunicaciones de ciertas subredes hacia otras de administración, equipos o cámaras de acuerdo a las funciones en cada departamento o subred.

2.8 Telefonía IP

El servicio de voz sobre IP permite realizar llamadas telefónicas entre usuario de la misma red o hacia el exterior de la institución utilizando la tecnología digital de transmisión de paquetes IP. Cada cliente utiliza para la comunicación un software de telefonía SIP o un teléfono IP sin embargo existe un servidor central con software libre “Elastix” el cual trabaja como una central PBX digital.

EL servidor de VoIP presente en el GPI es un equipo ELX-800 con software Elastix preinstalado con un diseño para empotrar sin dificultad en el rack del data center. La

administración se basa en una interfaz web con opciones para monitorear los recursos físicos del servidor, la capacidad de almacenamiento en los discos duros, estado de la memoria, el procesador. También permite configurar las opciones de la PBX como la creación de extensiones restricción de llamadas, creación de grupos, reportes gráficos, asignación de privilegios y las configuraciones de red necesarias, entre otras.

2.9 Sistema de información provincial geodatabase (Geoportal Sig)

El servidor geoportal sig contiene información cartográfica, mapas con variación de los niveles de escalas y brinda servicios utilizados como parte del plan de desarrollo y ordenamiento territorial de la provincia de Imbabura. Presenta varios servicios como la creación de mapas temáticos, procesamiento de información geográfica, vistas en segunda y tercera dimensión, modificación de objetos visuales y descarga de archivos. (Véase figura 6)

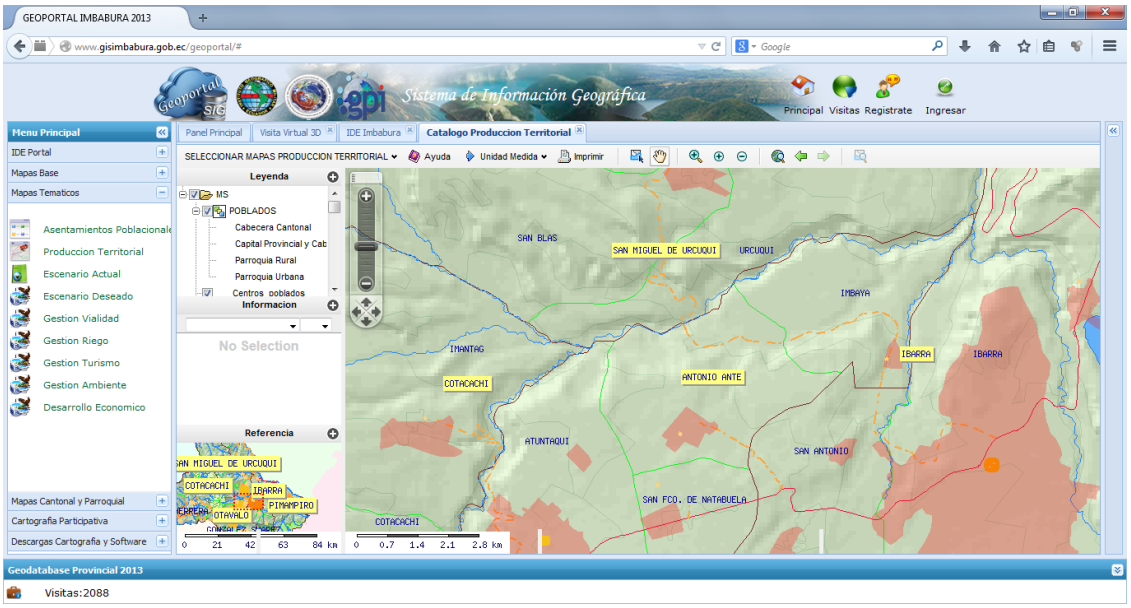

Figura 6: Geoportal GPI

Es una herramienta a disposición de instituciones gubernamentales, organizaciones sociales, ONG o empresa privada con énfasis en programas de producción, servicios, vialidad, urbanismo, gestión ambiental y sistemas de planificación de desarrollo y

ordenamiento territorial. Se encuentra alojada en la dirección www.gisimbabura.gob.ec la misma que ofrece la opción de acceder a la base de datos del portal mediante la interfaz web como se aprecia en la figura 7.

Figura 7: Acceso a la base de datos del geoportal

2.10 Sistema Contable Financiero OLYMPO

El sistema Olympo es un software enfocado a las tareas financieras y contables permitiendo realizar actividades como inversiones, administración de deudas por cobrar y pagar, depósitos, anticipos, kardex, reportes y otros.

El administrador del sistema tiene la capacidad de administrar a los usuarios, gestionar permisos o acceso a determinados módulos, configuraciones de red, reportes, restauración y respaldo de la base de datos. Es importante mencionar

2.11 Servidor blade

El servidor blade está basado en la tecnología “blade server” de séptima generación bajo la marca HP, es una solución tecnológicas de muchas prestaciones destinado al centro de procesamiento de datos optimizando el espacio, el ahorro del consumo de energía. Permite

trabajar con los servidores independientemente en cualquier momento sin la necesidad de apagar el todo sistema, es decir en caliente.

2.12 Switch de core

El switch principal es de marca CISCO modelo Catalyst 4503E SUP 6L-E con características y funciones de capa tres según el modelo de referencia OSI. Tiene la capacidad de transmisión de datos bajo enlaces de fibra óptica hasta 10 Gbps.

De acuerdo a la topología actual de la red el switch cumple con las funciones de core es decir formando un modelo de núcleo colapsado al encontrase conectado con otros switch de acceso por cada planta del edificio.

2.13 Switch de acceso

La distribución de las conexiones a cada uno de los puntos de red se encuentra a cargo de los switchs de acceso administrables cisco modelo catalyst 2960-S con características de capa dos. Estos switch de 24 y 48 puertos cubren las necesidades de la institución y se acoplan perfectamente con el switch de core al enlazarse físicamente mediante fibra óptica y trabajar conjuntamente a nivel lógico.

2.14 Firewall

El firewall es un equipo marca cisco modelo ASA 5520 ubicado después del router perteneciente al ISP, en este caso CNT. La configuración del firewall es realizada mediante la interfaz amigable con el usuario

Las ventajas de este modelo es la eficiencia en respuesta a conexiones de alta velocidad en función de las necesidades. Alta disponibilidad por medio de cuatro puertos Gigabit Ethernet soportando hasta 150 redes virtuales.

2.15 Administrador de ancho de banda

La administración del ancho de banda está a cargo del equipo PacketShaper de la marca Blue Coat, permite controlar el nivel de respuesta de las aplicaciones, mejorando de esta manera el rendimiento y la calidad de servicio regulando el tráfico e incrementando la capacidad de los enlaces troncales con el proveedor de servicio de internet u otras redes anexas.

2.16 Router CNT (Corporación Nacional de Telecomunicaciones)

El proveedor de servicio de internet del GPI es la Corporación Nacional de Telecomunicaciones el cual ha instalado un router ubicado en el centro de cómputo cuyo enlace físico es mediante fibra óptica de última milla. La CNT ha proporcionado las direcciones IP públicas utilizadas en los diferentes servidores de la institución y ha transmitido en los servidores DNS los nombres de dominio de los servidores web.

2.17 Cableado estructurado

El cableado estructurado ha sido implementado con cable UTP categoría 6A de cuatro pares marca Hubbell cumpliendo con las características eléctricas, físicas y mecánicas de acuerdo a la norma TIA/EIA 568-B. Cada uno de los puntos de red ha sido certificado con el dispositivo Fluke Network 1800.

El cableado horizontal del punto más lejano de red no sobrepasa los 90 metros y ha sido distribuido utilizando bandejas, escalerillas, ductos amarraderas entre otras, y sin olvidar la respectiva identificación y documentación.

Los demás elementos como jacks, faceplaces, patch panels, los conectores Rj-45 son compatibles con la categoría 6A del cable UTP permitiendo soportar velocidades de transmisión de 10Gbps conforme las especificaciones del estándar IEEE 802.3 ab.

2.18 Backbone

El enlace de backbone está conformado por cableado de fibra óptica soportando velocidades de transmisión de 10 Gbps para la conexiones desde el data center hacia cada una de las plantas. Furukawa ha sido la marca seleccionada a implementar en todos los elementos del enlace de fibra óptica tipo OM3 y la distancia máxima no excede los 3000 metros.

2.19 Sistema de aire acondicionado

El control de la temperatura y humedad del aire a niveles recomendados por los fabricantes de los equipos instalados en el data center, se encuentra a cargo del equipo de aire acondicionado marca Stulz modelo CCD 121 A. El sistema de aire acondicionado funcionará todos los días del año las 24 horas del día, automatizando el reinicio ante cualquier interrupción de energía eléctrica.

2.20 Sistema de alimentación ininterrumpida (UPS)

En el caso de interrupción de la energía eléctrica, el data center cuenta con un equipo UPS de 8000VA y 6400 watts encargado de brindar soporte de energía a los dispositivos de red, servidores y otros sistemas electrónicos.

Recibe alimentación eléctrica monofásica de 220V el cual registra el estado del equipo por medio de una pequeña pantalla lcd. El UPS al ser un medio de respaldo eléctrico en situaciones de emergencia ha sido instalado en la parte superior del data center. El UPS brida dos circuitos de alimentación y respaldo, el primero es la rack de servidores y el segundo a los sistemas de control de accesos y sistemas de incendios.

2.21 Sistema de energía eléctrica.

El sistema eléctrico del centro de datos se encuentra conectado con acometida independiente desde la cámara de transformación de la institución mediante bandejas metálicas y tubería PVC[5] libre de humedad. El data center posee un tablero de distribución eléctrica de 220V con circuitos para protección de cargas, alimentación, aire acondicionado y para el sistema de alimentación ininterrumpida.

El aseguramiento del tiempo de vida de los equipos de red y la continuidad de las operaciones requieren del sistema de puesta a tierra. Cada uno de los racks se encuentran protegidos mediante conexiones al sistema de puesta a tierra localizado en una plancha de cobre.

2.22 Control de Acceso

El data center es una estructura ubicada en el interior del departamento de gestión de TIC´s. El ingreso hacia el data center se encuentra restringido por una puerta formada por dos planchas de acero de 2mm de espesor, en cuyo interior se encuentran dos planchas de 8mm de aislante térmico y una capa de fibra de vidrio de 25mm de espesor. Esta combinación evita el paso del fuego hasta 483ºC, líquidos, humo o gas tóxico. También posee una ventana de 30x30 cm de vidrio antibala.

La apertura de la puerta desde el interior del centro de datos se facilita con una barra anti-pánico y un brazo de cerrado lento, por el contrario para abrir la puerta desde el exterior se lo hace con la tarjeta RFID[6] acercándola al escáner de proximidad ubicado a un lado de la puerta del data center. Si el usuario se encuentra registrado la cerradura electromagnética se abre y permite el acceso.

---

[5] **PVC (Policloruro de vinilo):** Es un derivado del plástico más versátil caracterizado por su resistencia ambiental y un buen aislante eléctrico.

[6] **Tarjeta RFID:** La tarjetas RFID transmiten la identidad de un objeto mediante ondas de radio.

2.23 Cámaras de seguridad

Como parte del sistema de seguridad la institución cuenta con dos cámaras de video cumpliendo la función de grabar permanentemente el área comprendida en el acceso al data center. Son cámaras tipo IP PTZ es decir son capaces de mover el lente tanto en el plano X como en el Y, y la conectividad es gracias al protocolo IP con la particularidad de gestionar las mismas mediantes una aplicación web.

2.24 Sistema de monitoreo ambiental

El monitoreo de las condiciones ambientales en el interior del data center se encuentra a cargo del equipo Netbotz NBRK0551. Se caracteriza por la rapidez en la respuesta ante incidentes de seguridad generados en el data center. El montaje del equipo es en el rack de dispositivos siendo la administración por medio de una aplicación web. Los eventos en los cambios ambientales son recogidos por varios sondas que incorporan sensores de humedad, temperatura y detección de fluidos.

Figura 8: Sistema de monitoreo ambiental. Recuperado de: http://www.apc.com /products/moreimages.cfm?partnum=NBPD0150&aPos=2

2.25 Sistema de control de detección y extinción de incendio

El data center se encuentra protegido ante conatos de incendio con un sistema completo de detección temprana de incendios y la posterior extinción. En los 15 metros

cuadrados de área se han distribuido equitativamente cuatro sensores de humo fotoeléctricos, dos en el ambiente de equipos y otros dos debajo del piso falso.

El sistema de extinción de incendios utiliza un agente limpio Ecaro 25 el cual se distribuye por medio de tuberías hacia tres toberas con un radio de alcance de 9 metros a 180°, ubicados debajo del piso falso, encima del cielo falso y en el ambiente de los racks abarcando toda la superficie del centro de datos según el diseño de inundación total. Las ventajas de Ecaro 25 al ser un agente limpio, son de proteger a los equipos y las personas al ser un producto sin olor, no conductor de electricidad, no produce residuos entre otras características.

El diseño del sistema incorpora un panel de control de incendio ubicado en la parte exterior del data center. El panel SHP PRO de marca Fike centraliza las operaciones del sistema Ecaro 25 y los detectores de humo, también incorpora el manejo de alarmas visuales y sonoras como una sirena y luz estroboscópica con activación y desactivación manual de las alarmas. Debido a la importancia de la disponibilidad del sistema contra incendios el panel opera a 120 V y posee una batería con hasta 90 horas de funcionamiento con todos los componentes.

Figura 9: Panel de control incendios SHP PRO.
Recuperado de: http://www.fike.com/products/
shp-pro-fire-detection-fire-protection-system/

2.26 Teléfono IP

Las comunicaciones de voz son realizadas mediante el servicio de voz sobre IP utilizando una central Elastix[7] localizada en el data center, sin embargo el servicio se complementa con las extensiones hacia cada uno de los teléfonos IP distribuidos en cada oficina de los funcionarios con este dispositivo de comunicación. El Gobierno Provincial de Imbabura posee aproximadamente 100 teléfonos IP marca Cisco.

2.27 Internet

Internet es un servicio disponible para todos los funcionarios de la institución considerando como una herramienta adicional y de consulta para realizar las tareas necesarias en cumplimiento del trabajo. El internet permite las comunicaciones mediante el uso del correo electrónico, la publicación de la información por medio de los servidores web, compras entre otras necesarias en un ambiente institucional de desarrollo productivo. El servicio de internet es proporcionado por el ISP Corporación Nacional de telecomunicaciones (CNT)

2.28 Servidores reemplazados o eliminados

Después del proceso de actualización e implementación del nuevo sistema de cableado estructurado y la implementación del data center, las autoridades del departamento del tecnologías de la información procedieron a declarar en desuso o cambio de los servidores que hasta hace algún tiempo se encontraban activos.

Originalmente el programa de ordenamiento territorial (POT) ha sido reemplazado por el servidor GIS o también identificado como geoportal SIG (Sistema de información

---

[7] **Elastix:** Es un software para implementar sistemas de telefonía sobre el protocolo IP.

geográfica), albergando información cartográfica de la provincia de Imbabura, mapas 2D y 3D, información satelital entre otras.

El sistema de eficiencia y transparencia (Siseftran) encargado de la gestión del presupuesto en los proyectos de lis diferentes departamentos ha sido eliminado. El sistema financiero (Gubwin) gestiona la información para desarrollar informes financieros y administración del presupuesto también ha sido eliminado. Los dos sistemas han sido reemplazados por un solo sistema financiero cantable denominado Olympo.

El sistema de gestión vehicular encargado del control y seguimiento de los vehículos de la institución ha sido implementado por un módulo llamado Gea Tracker en el servidor Olympo que es un sistema de localización y seguimiento de vehículos para optimizar su funcionamiento y vida útil

CAPÍTULO III

HACKING ÉTICO

3.1 Definición de hacking ético

El objetivo de un hacker es explotar las vulnerabilidades de un sistema o red para encontrar la debilidad en uno o más de los elementos de seguridad (Confidencialidad, Integridad, Disponibilidad). (Graves, 2010)

Un hacker ético es un profesional que utiliza sus habilidades de hacker para fines defensivos y de protección, es decir realizar pruebas de intrusión para detectar vulnerabilidades en la red y los sistemas de seguridad con las mismas herramientas que lo haría un hacker. (Graves, 2010).

Con el desarrollo del presente trabajo se pretende concienciar al lector acerca de las técnicas y herramientas utilizadas por los hackers para detectar y descubrir las vulnerabilidades con el fin de aprender las mismas habilidades y herramientas informáticas para ser capaz de defender las propias redes. Como afirma Sun Tzu en el libro "El arte de la guerra" conoce a tu enemigo y conócete a ti mismo y en cien batallas nunca correrás peligro.

El hacker malicioso usa las habilidades de hacker con fines maliciosos enfocado en gran parte de sus acciones en conseguir beneficio económico, fines destructivos difundiendo virus, ataque de denegación de servicio, comprometer la operación de los sistemas y las redes. Los motivos que llevan a un hacker a pasarse al lado del mal puede ser por diversión, adquirir conocimientos y experiencia, rivalidad o competencia, ganar reputación, robar, dañar al rival o la competencia perjudicando su imagen en la sociedad y dañando la integridad de la organización revelando información importante, conseguir dinero fácil en obtener

información de tarjetas de crédito, poner en evidencia acciones indebidas de instituciones y personas como es hechos de corrupción, actividad ilícita, hacktivismo[8] entre otros.

3.2 Como realizar un trabajo ético

Se determina las necesidades y características del sistema, la prueba de penetración es un proceso organizado y estructurado. El hacker ético está obligado a proceder de acuerdo a la ética y la moral. La información descubierta y directamente relacionada con las pruebas de intrusión se debe manejar y almacenar de forma segura, en lo posible realizar un acuerdo de no divulgación. La información crítica nunca debe ser revelada a terceros.

Es importante que el hacker ético conozca las penalidades que la ley impone a delitos como la intrusión no autorizada a los sistemas de seguridad, es por ello que previamente de una auditoría informática siempre se recomienda poseer el consentimiento escrito expresando la autorización para el desarrollo de las actividades de hacking. Del mismo modo el evaluador debe ser consciente que no puede hacer mal uso de las habilidades que posee. El proceso de hacking debe ser realizado en base a la moral, los valores morales y respetando la reglamentación vigente.

3.3 Tipos de pruebas de intrusión

Dependiendo del conocimiento inicial acerca de la red informática a ser evaluada, los tipos de pruebas de intrusión se los clasifica en tres categorías. El enfoque Black-box también conocido como prueba de intrusión externa trata de evaluar la infraestructura de red desde un punto remoto regularmente desde el internet, se utiliza cuando no existe información alguna acerca del sistema a ser evaluado. En el enfoque White-box el pentester[9] tiene el

---

[8] **Hacktivismo:** Es toda actividad hacker motivada por fines políticos o sociales.
[9] **Pentester:** Sinónimo de hacker.

conocimiento acerca de la red a ser revisada como es la estructura interna y tecnología existente. Este enfoque facilita la tarea de evaluar el sistema y conlleva menos tiempo obteniendo de esta manera resultados más detallados de las vulnerabilidades de la red. Finalmente la combinación de los dos tipos de intrusión se llama Grey-box en el cual el pentester con limitada información que posee del sistema elegirá la mejor manera de evaluar la seguridad global (Ali & Heriyanto, 2011).

3.4 Fases de hacking ético

El proceso de hacking ético conlleva un tiempo de preparación y ejecución del ataque considerando de gran importancia el pleno conocimiento del objetivo, es decir mediante una serie de etapas o fases el hacker sabe lo que va a atacar en objetivos específicos previamente identificados por sus características propias vulnerables. Conforme avanza la investigación del objetivo es posible descubrir elementos útiles para armar una estrategia e ir perfeccionando el ataque, cada etapa del proceso de hacking ético proporciona información valiosa que alimenta una fase a la otra. El proceso de hacking ético se divide en cinco grandes etapas.

3.4.1 Recolección de información

Es una fase preparatoria de recolección inteligente de información del objetivo enfocándose en descubrir detalles útiles para el atacante mediante la búsqueda, selección y discernimiento de datos relevantes. En esta etapa, el atacante busca definir al objetivo con el mayor nivel de detalle posible, y a partir de eso, obtener la mayor cantidad de información (Jara & Pacheco, 2012, pág. 74) en medios públicos como el internet, periódicos, documentos públicos, entre otros.

Dependiendo la forma como se consigue la información puede categorizarse las técnicas de identificación como reconocimiento activo o pasivo. La búsqueda de información en recursos públicos utilizando herramientas o técnicas no intrusivas se conoce como procedimiento pasivo, por el contrario al existir una interacción directa con los sistemas del objetivo para identificar puertos, servicios, banners[10], redes, dispositivos o servidores interactuando con los recursos del sistema se considera reconocimiento activo.

3.4.2 Escaneo

El objetivo de esta etapa es conseguir un nivel de detalles más técnico de los servicios y aplicaciones en ejecución y así descubrir las vulnerabilidades a explotarse. La información a buscar en esta etapa es la detección de versiones de sistemas operativos, versiones específicas de aplicaciones en especial a nivel de servidores, servicios utilizados en la red con sus respectivos puertos abiertos de los equipos de borde y de la red interna.

---

[10] **Banner:** Es una identificación o texto describiendo el nombre de la aplicación y la versión.

3.4.3 Enumeración

La enumeración es el proceso de extracción de nombres de usuario, recursos de la red y los servicios de un sistema utilizando consultas o peticiones directamente con el objetivo. La información obtenida es utilizada para identificar vulnerabilidades o puntos débiles en el sistema de seguridad para intentar explotarlos. Las técnicas de enumeración son utilizadas en entornos de la red interna.

3.4.4 Explotación

Una vez detectadas las vulnerabilidades se procede a investigar la existencia de exploits o la manera de aprovecharse de los fallos en la seguridad. El aprovechamiento de las vulnerabilidades mediante el uso de exploits es la manera más común pero no la única, también se evalúa mediante el establecimiento de conexiones de los sistemas para aprovecharse de las configuraciones deficientes. Es importante mencionar que en el medio informático no se considera a los ataques de denegación de servicio como parte importante de la búsqueda de vulnerabilidades, las razones porque son fáciles de realizar, no involucra muchos conocimientos o experiencia pero sobre todo el impacto en la organización puede ser desastroso afectando a los servidores, bases de datos, información, disponibilidad entre otros.

3.4.5 Post-explotación

Una de las acciones a emprender luego explotar las vulnerabilidades es elevar los privilegios en los sistemas para facilitar la ejecución de acciones o modificaciones en los equipos, instalar malware, descargar archivos, desactivar controles de seguridad y evitar activar alarmas para no ser detectados.

Quienes logran acceder a los sistemas buscan asegurar el mantenimiento del acceso en futuras ocasiones mediante la instalación de puertas traseras, conexiones remotas a servidores externos, instalación de software espía, subir virus, activar servicios entre otras.

Los hackers que actúan con fines maliciosos causantes de provocar estragos en los sistemas que vulneran necesitan mantener el anonimato para no ser descubiertos mediante el rastreo de sus acciones y direcciones ip, para lo cual eliminan el contenido de los registros de eventos efectuados en los equipos que entre otras cosas detallan las direcciones ip de las sesiones remotas establecidas a los servicios.

3.5 Sistema operativo para pruebas de penetración

La evaluación de la seguridad de los sistemas involucra la utilización de diversas herramientas, técnicas y conocimientos, a nivel de seguridad informática los profesionales en la identificación, evaluación y explotación de las vulnerabilidades reúnen las herramientas más eficientes y potentes.

La evolución de la tecnología y el desarrollo de aplicaciones en todas las áreas de la informática, ha permitido que los hackers o cualquier profesional relacionado con la seguridad informática pueda adquirir las herramientas necesarias para el objetivo que desea alcanzar, por tal razón actualmente existen la más diversa variedad de herramientas y software utilizados para las diversas etapas para el proceso de hacking ético.

Las aplicaciones utilizadas para la actividad hacker son fáciles de adquirir, descargar e instalar, básicamente cualquier sistemas operativo puede ser utilizado para realizar estas tareas, cada profesional adquiere las herramientas que necesita sin embargo existen varios sistemas operativos creados específicamente para pruebas de intrusión basados en Linux.

Los sistemas operativos Linux son más seguros porque el núcleo del sistema operativo llamado kernel[11] administra el sistema de archivos, datos e información diferente en comparación con otros sistemas operativos comerciales, otro punto a favor es la presencia mayoritaria de virus en sistema Windows, es decir no es posible la ejecución de virus o malware en Linux que fueron desarrollado para Windows por la estructura del archivo ejecutable el cual es (.exe) el cual no es admitido en Linux. Esta tendencia a desarrollar código malicioso contra sistemas Windows se debe a lo comercial que son y la gran cantidad de usuarios a nivel mundial, lo que se traduce como gran cantidad de víctimas a quien explotar.

Los sistemas operativos Linux al ser menos populares y comerciales existen menos virus o errores detectados que pueden afectar el equipo es decir en muchas ocasiones no se necesitan antivirus mejorando así el rendimiento de la máquina. El rendimiento tan importante en este tipo de actividades muchas veces se ve enormemente afectado en sistemas Windows por la cantidad de recursos que consume para su funcionamiento tanto del sistema operativo como tal y de las aplicaciones que en muchos de los casos no son utilizados.

Se puede armar un sistema operativo como Ubuntu con las herramientas que necesita un hacker, sin embargo es mucho mejor utilizar otras distribuciones diseñadas exclusivamente para ello lo que facilita la obtención de herramientas y la configuración.

Las herramientas pre-instaladas en este tipo de distribuciones funcionan y trabajan mejor de lo que podrían ser en Windows. Quienes son hackers controlan la pc, en Windows la pc controla al usuario al ser dependiente de las limitaciones que representa.

---

[11] **Kernel:** Es el núcleo de los sistemas operativos Linux encargado de gestionar el software y el hardware de un host.

Existe una gran variedad de distribuciones enfocadas a las pruebas de penetración entre las más populares encontramos las siguientes:

- **BackTrack5 R3:** Es una distribución GNU/Linux desarrollada para la auditoría de seguridad y relacionada con la seguridad informática en general. Ha sido por muchos años la favorita por los profesionales en esta área se encuentra basada en Ubuntu con una gran cantidad de herramientas, sin embargo debido a la re-estructuración que ha sufrido su arquitectura ha sido descontinuado por los desarrolladores.
- **WiFiSlax:** Es una distribución GNU/Linux con funcionalidades de Livecd[12] y Liveusb[13] desarrollada para auditorías de seguridad la cual incluye una larga lista de herramientas listas para ser utilizadas.
- **Matriux Krypton:** Es una distribución de seguridad conformado por un conjunto de herramientas de código abierto utilizado para penetration testing[14], hacking ético, administración de sistemas y redes, investigaciones forenses, pruebas de seguridad, análisis de seguridad, y mucho más.
- **Blackbuntu:** Es una distribución para pruebas de penetración basada en Ubuntu 10.10 que fue desarrollado para estudiantes y profesionales de la seguridad de la información.
- **Bugtrack:** Es una distribución GNU/Linux enfocada al pentesting y al análisis forense basada en openSUSE, Ubuntu y Debian. Cuenta con laboratorios de pruebas de malware, herramientas de auditoría para GSM, wifi, bluetooth y RFID integradas y herramientas de Windows, entre otras.

---

[12] **Livecd:** Funcionamiento del sistema operativo desde el Cd de instalación.
[13] **Liveusb:** Funcionamiento del sistema operativo desde la unidad de almacenamiento externo usb.
[14] **Penetration testing:** Traducido al español son pruebas de penetración o hacking.

- **BackBox Linux:** Es una distribución Linux basada en Ubuntu Lucid 11.04 enfocada para ser utilizada en pruebas de seguridad, se caracteriza por ser rápida y sencilla de utilizar en comparación con Back Track.
- **Kali Linux:** Es una distribución de Linux avanzada diseñada y desarrollada exclusivamente para pruebas de penetración y auditorías de seguridad, posee más de 300 herramientas de código abierto. Kali Linux está basada en Debian[15] sincronizando los repositorios hasta cuatro veces al día para mantenerlo actualizado. Kali Linux es la distribución seleccionada para el proceso de penetración y explotación de los servidores del Gobierno Provincial de Imbabura. Las razones de su elección son:

    - Todos los puertos cerrados desde la instalación.
    - Software de código abierto
    - Compatible con gran variedad de hardware inalámbrico y dispositivos usb.
    - Kernel modificado por los desarrolladores de Kali adaptado a las necesidades de hacking
    - Repositorios disponibles cuatro veces al día
    - Actualizaciones seguras de los paquetes.
    - Basado en Debian permite instalar paquetes y aplicaciones fácilmente tanto en 32 y 64 bits
    - Optimiza los recursos del equipo
    - Bajos requerimientos de instalación
    - Funcionamiento livecd, liveusb o en disco duro.
    - Instalación similar a cualquier distribución Linux

---

[15] **Debian:** Es una distribución o sistema operativo Linux desarrollada por miles de programadores.

- Opción de cifrado de la partición de la instalación
- Soporta multitud de lenguajes entre ellos español

3.6 Herramientas de recolección de información

En muchas ocasiones el evaluador desconoce características propias del equipo para el proceso de penetration testing. La etapa de recolección de información involucra utilizar una serie de herramientas y técnicas que servirán para interaccionar con el equipo objetivo y descubrir características, detalles, servicios, versiones de aplicaciones, es decir información en general que puedan ser utilizadas para detectar fallos o vulnerabilidades.

3.6.1 Motores de búsqueda

El primer paso consiste en investigar la información pública de la institución relacionada con la seguridad de la información y pistas de los sistemas utilizados. Los motores de búsqueda como google, bing, ask entre otros son en excelente medio de búsqueda de información. (Véase figura 10)

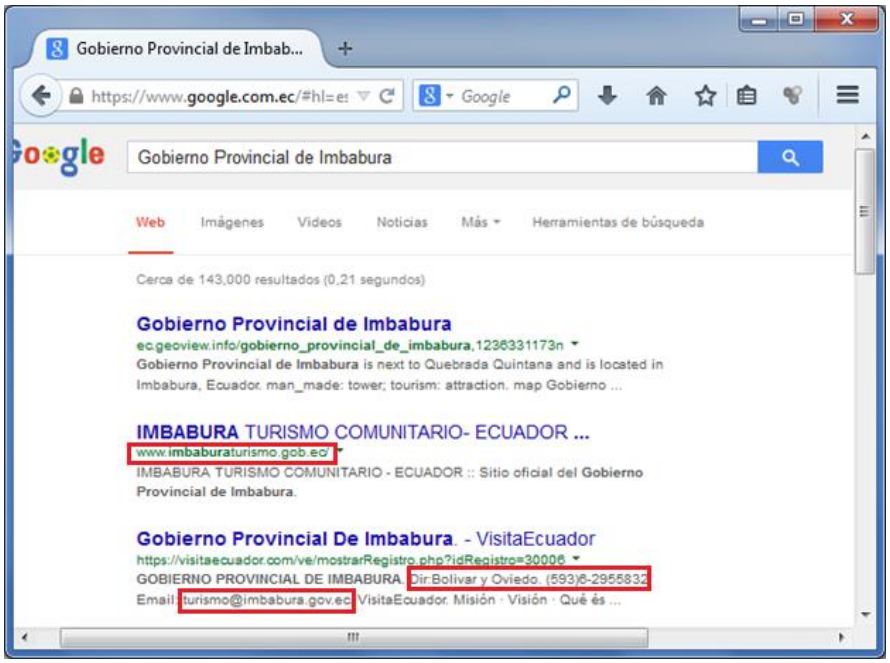

Figura 10: Búsqueda de información en los motores de búsqueda. Recuperado de: https://www.google.com/search?q=Gobierno+Provincial+de+Imbabura

De esta manera se recolecta información como nombres de dominio, enlaces a otros servidores relacionados con la institución entras, además durante todo el procedimiento de búsqueda de vulnerabilidades se utiliza los motores de búsqueda como se verá más adelante.

3.6.2 Detección de IP pública

La identificación de la dirección IP pública del servidor es vital para la continuación del análisis, para ello una vez conseguido el nombre de dominio la identificación de la dirección IP se lo puede realizar de varias manera. La primera opción es mediante la herramienta ping disponible tanto en sistemas Windows como Linux.

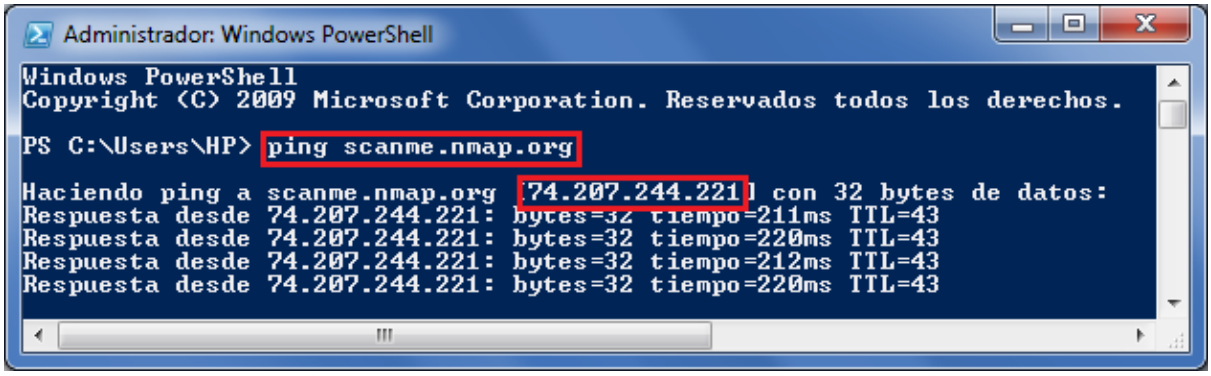

Figura 11: Uso de la herramienta ping al dominio scanme.nmap.org

Otra herramienta muy útil es nslookup la cual entrega como resultado el nombre del servidor de dominio por el cual se establece la traducción de la dirección IP, junto con la IP pública en formato IPv4 e IPv6.

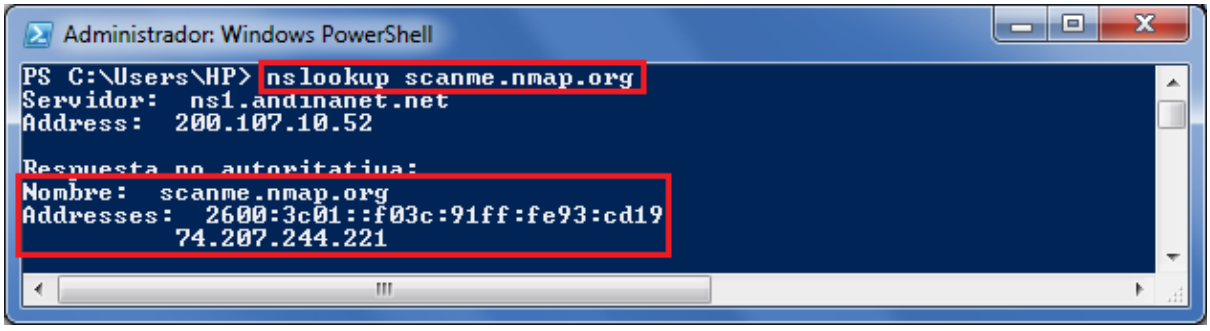

Figura 12: Uso de la herramienta nslookup al dominio scanme.nmap.org

3.6.3 Localización geográfica del servidor

Una vez detectada la dirección IP pública del servidor se procede con la investigación de la ubicación geográfica o el país de alojamiento. La ventaja de utilizar esta técnica es la identificación del hosting que aloja la página web o los servicios, y conocer el proveedor de servicio de internet.

Es importante conocer esta característica debido a que si la dirección IP pública revela que el servidor utiliza un hosting o empresa para alojar la página web, la estrategia de ataque cambia porque usualmente este tipo de empresas protegen muy bien sus servidores brindando seguridad a los clientes.

Por el contrario si el resultado permite identificar que el servidor se encuentra alojado en las instalaciones propias de la institución, es decir en la ciudad donde se presume su funcionamiento, quiere decir que la institución se encarga de la protección de sus propios equipos. Algunas de los servicios web respecto a detalles en la localización geográfica son los siguientes:

- http://www.ipaddresslocation.org/
- http://whatismyipaddress.com/
- http://www.ip2location.com/demo.aspx
- http://www.ip-adress.com/

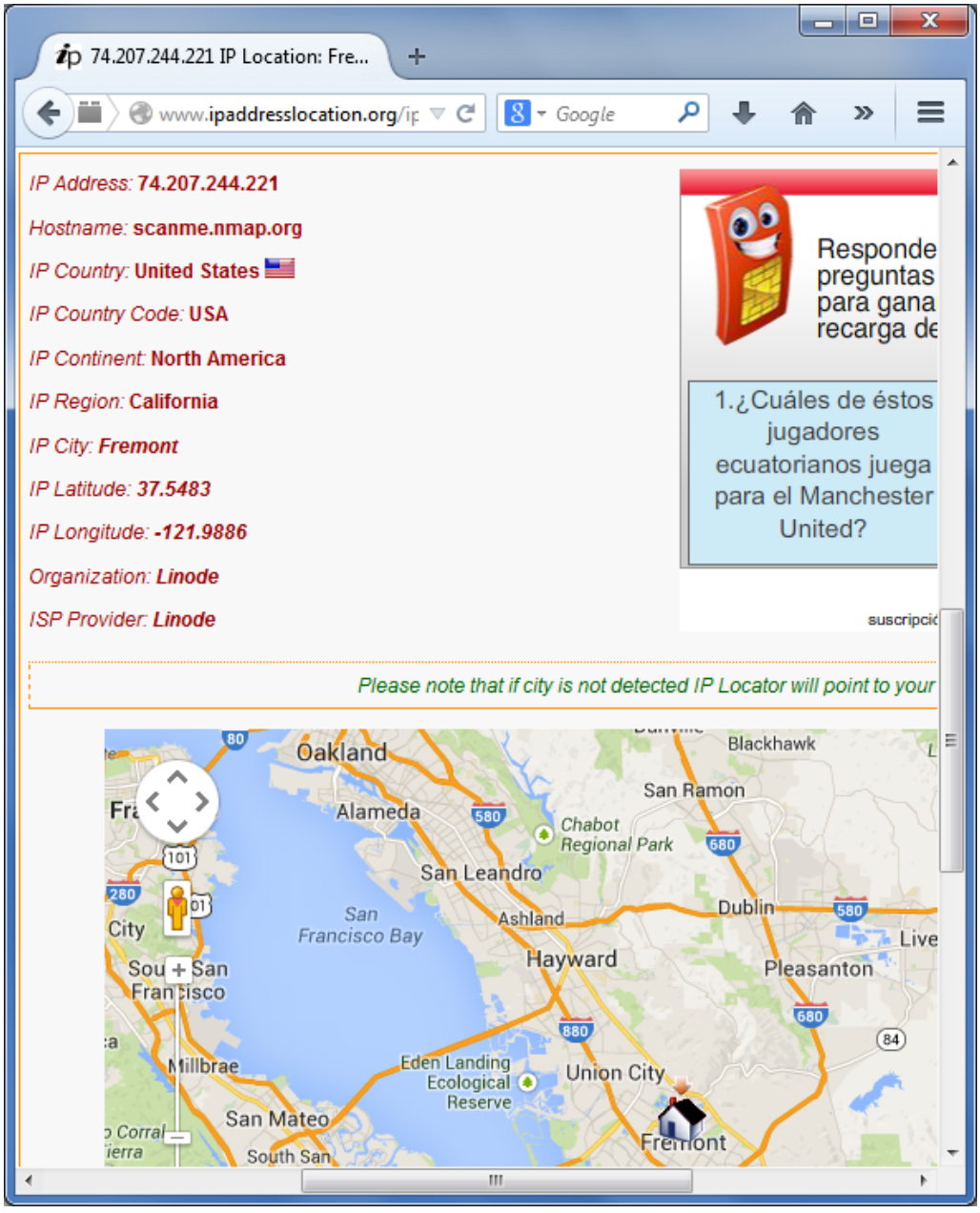

Figura 13: Detalles del posicionamiento geográfico en base a la dirección IP pública.

Como se observa en la figura 13 se ha tomado como ejemplo la dirección IP del dominio www.google.com obteniendo como resultados el nombre del equipo, el país de origen, la provincia o estado, la ciudad, el proveedor de servicio de internet y las coordenadas geográficas. En la sección inferior de la pantalla se presente un mapa para conocer visualmente la ubicación del servidor.

3.6.3 Técnicas de recolección de información

Existen varias técnicas que no se limitan solamente al uso de herramientas de software para descubrir detalles o pistas del servidor que puedan ser útiles. Una de ellas es forzar al error es decir se ingresa valores no existentes en formularios, entradas, direcciones incorrectas obligando al servidor a devolver detalles del servidor como se aprecia en la figura 14.

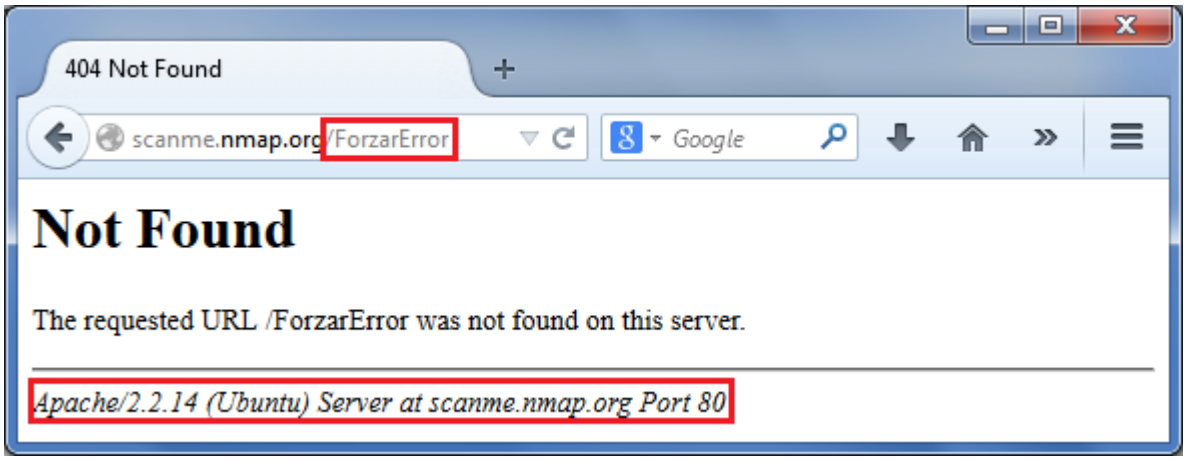

Figura 14: Error forzado en una página web inexistente en http://scanme.nmap.org/

Otra técnica simple pero efectiva es la utilización de aplicaciones de conexión remotas como telnet o netcat[16], los cuales permiten establecer la conexión especificando la dirección IP destino y el puerto, lo cual no permitirá el establecimiento de la conexión pero en muchos de los casos se obtiene las versiones de las aplicaciones del servidor como se ilustra en la figura 15.

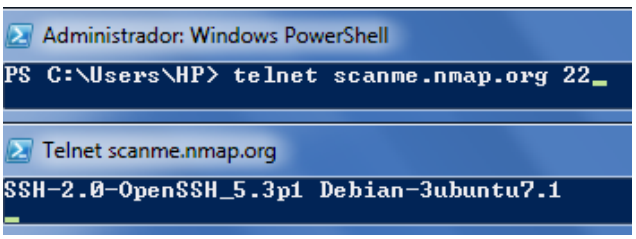

Figura 15: Identificación de la versión de la aplicación utilizando telnet.

[16] **Netcat:** Es una herramienta de red la cual permite abrir y conectar puertos tcp/udp en un host.

Visitar la página web del servidor evaluado es una tarea preliminar y de mucha importancia. El reconocimiento visual de todas las páginas, formularios, aplicaciones permite brindar una idea más clara del funcionamiento del servidor e identificar posible vectores de ataque la interacción con la base de datos (Inyección SQL), modificación de la página web (XSS-Código para sitios cruzados), directorios web accesibles, acceso a archivos de configuración entre otras. La figura 16 demuestra la posibilidad de conseguir otros cinco nombres de dominios de los servidores sin dificultad.

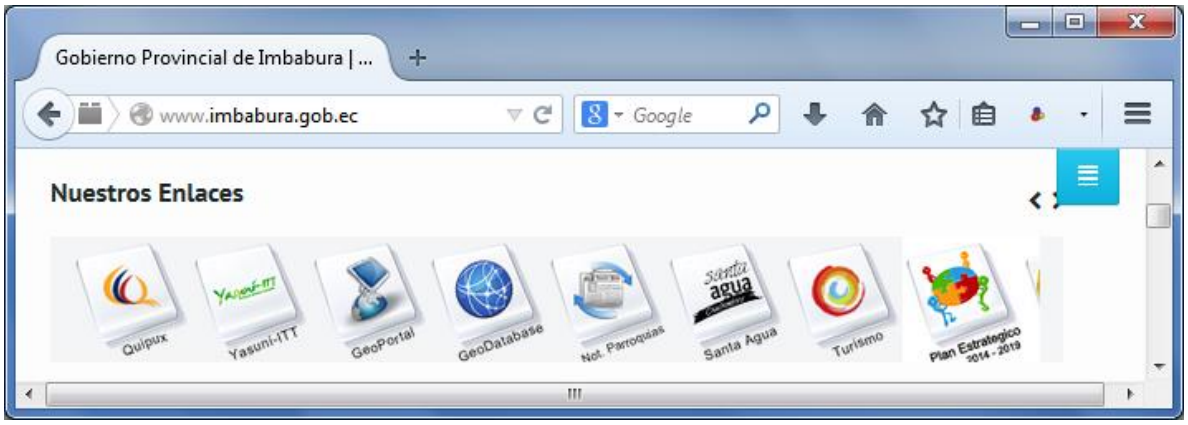

Figura 16: Recolección de información visitando la página web principal.

Otra técnica es revisar los metadatos de todo tipo de documentos encontrados y recolectados en busca de información como nombres de usuario, contraseñas, versiones de aplicaciones utilizadas por los usuarios, correos electrónicos, impresoras, versiones de sistemas operativos y muchas más. Los metadatos es información añadida en todo tipo de archivos digitales utilizados por las respectivas aplicaciones y sistemas operativos para identificar cada archivo. Tanto en sistemas Windows como Linux existen herramientas para realizar estas tareas sin embargo la mejor de todas es Focapro disponible sólo en Windows.

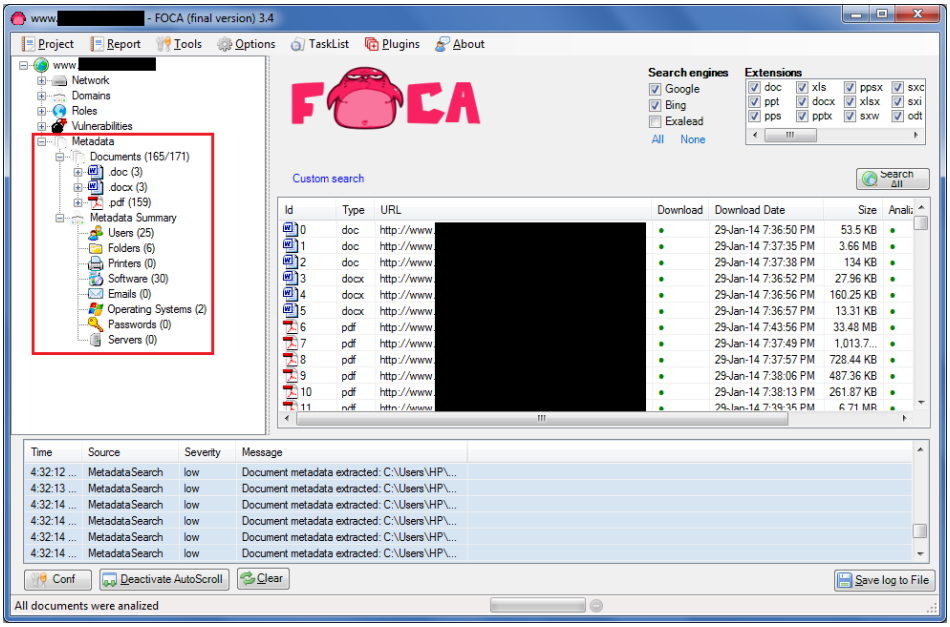

Figura 17: Extracción de metadatos de los archivos con el software Foca pro.

3.7 Escaneo de puertos y servicios

Una vez recolectada la información mediante medios públicos se procede con el reconocimiento activo, es decir interactuar con el servidor para descubrir detalles específicos del equipo para posteriormente investigar vulnerabilidades. En esta sección se intenta descubrir los puertos y servicios que presta el servidor, para ello existen gran cantidad de herramientas disponibles entre ellas la más popular y utilizada es nmap.

Nmap permite personalizar el escaneo utilizando varios comandos dependiendo de las necesidades, en primera instancia es importante conocer los puertos abiertos, cerrados y filtrados. Nmap por defecto solo analiza los primeros 1000 puertos conocidos, sin embargo es importante seleccionar todos los 65535 puertos porque algunos de ellos pueden brindar servicios conocidos en puertos no habituales para ello. El comando es el siguiente:

```
root@kali:~# nmap –p 1-65535 [Dirección_ip o dominio]
```

Sin embargo existen servicios que funcionan bajo el protocolo TCP (Protocolo de Control de Transmisión) y otros UDP (Protocolo datagrama de usuario). El primero establece una conexión de tres vías conocido con el nombre de (handshake) es decir, el cliente solicita el servicio al servidor enviando un paquete SYN, el cual responde con un paquete SYN/ACK como respuesta a la primera solicitud, finalmente el host envía el paquete ACK al servidor y se establece la sincronización entre las máquinas.

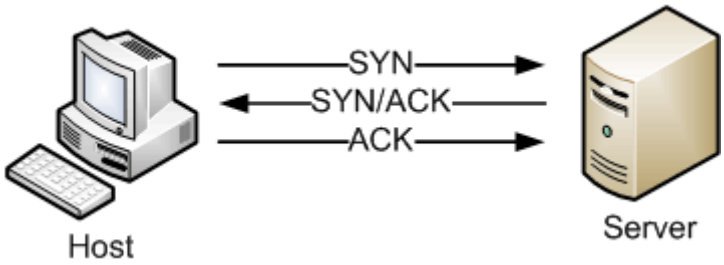

Figura 18: Esquema de establecimiento de conexiones bajo el protocolo TCP
Fuente: System & Code Recuperado de: http://www.georgecoding.com /wp-content/uploads/2013/04/handshake.gif

Por el contrario la transmisión de paquetes UDP se lo realiza desde un equipo a otro sin establecer una conexión previa lo cual no garantiza la presencia de todo los paquetes transmitidos en el host destino.

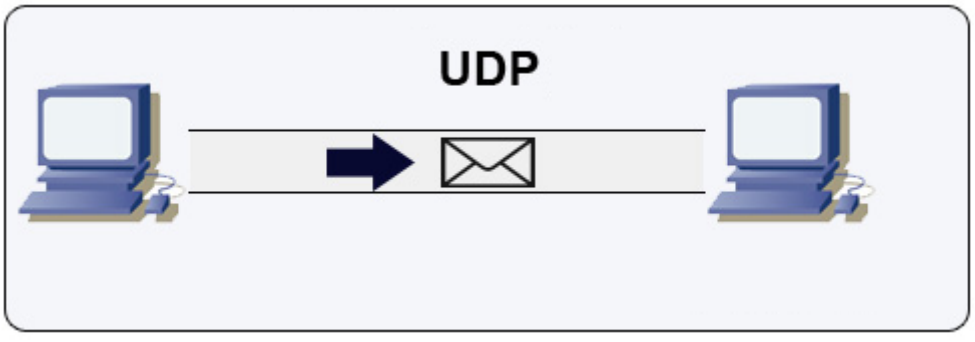

Figura 19: Esquema de conexiones bajo el protocolo UDP
Fuente: Informática 1ln. Recuperado de http://lombardoanabellaln.blogspot.com/2011/06/ udp-son-las-siglas-de-protocolo-de.html

La importancia de conocer las características de cada protocolo de transporte según el modelo OSI, radica en el tipo de escaneo de puertos y la seguridad que representa, porque si

no se especifica adecuadamente las opciones de escaneo, nmap puede devolver los puertos abiertos solo aquellos bajo el protocolo TCP porque nmap verificó mediante el establecimiento de la conexión al finalizar el handshake, esto quiere decir como los puertos bajo el protocolo UDP no existe la respuesta del servidor por medio de un paquete de respuesta, nmap asume que se encuentran cerrados lo cual puede no ser cierto. Para solventar esta escenario se debe indicar a nmap mediante otro escaneo la verificación de puertos abiertos únicamente bajo el protocolo UDP con el comando (-sU)

El siguiente comando especifica la evaluación de los 65535 puertos (-p 1-65535) bajo el protocolo TCP (-sT) con un nivel alto de detalle (-A -v)

```
nmap -p 1-65535 -sT -A -v DIRECCION_IP
```

El siguiente comando realiza un escaneo a los puertos UDP (-sU) con un nivel alto de detalle (-A -v)

```
nmap -sU -A -v DIRECCION_IP
```

En los sistemas protegidos por firewall o dispositivos de análisis de tráfico donde se bloquea o se impide el establecimiento de conexiones a los puertos de los servidores desde redes no autorizadas, es muy difícil realizar el escaneo de puertos porque la herramienta no puede verificar con certeza el estado del puerto. Para ello existen varias alternativas representadas en los siguientes comandos:

- -sS: Conocido como escaneo sigiloso puede realizar el sondeo de miles de miles de puertos rápidamente con la particularidad de que no llega a completar las conexiones TCP.
- -f: Opción utilizada para fragmentar en paquetes de ocho bytes.

La importancia de evitar completar las conexiones TCP radica en la seguridad del atacante, porque los servidores reciben gran cantidad de peticiones de muchos clientes (SYN) y cuando culmina el handshake (Envío de ACK), el servidor registra las conexiones establecidas almacenando la dirección IP perjudicando el anonimato del atacante.

Como se aprecia en la figura 20 nmap presenta los resultados detallando los puertos abiertos, el estado del puerto, el servicio y la versión de la aplicación e incluso información adicional como sistema operativo, distancia con el servidor a nivel de saltos y otros.

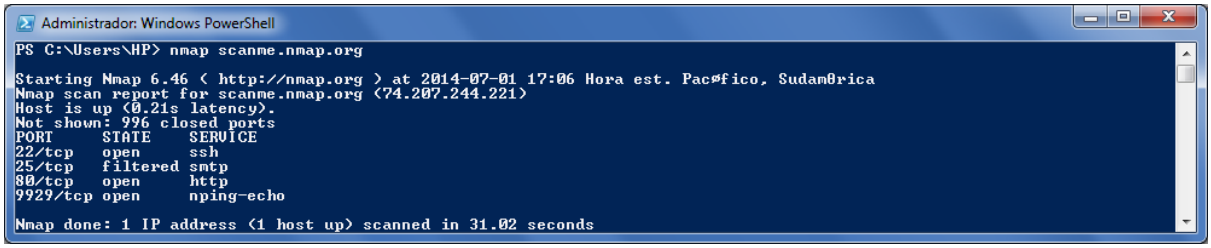

Figura 20: Resultado de nmap hacia el dominio scanme.nmap.org

Como se ha manifestado hasta el momento en esta etapa no solamente se puede identificar las versiones de las aplicaciones por cada puerto abierto como es versión del servidor web, bases de datos, servidores ftp, conexiones remotas telnet, ssh, vnc entre otras, también brinda una idea clara de la función principal del servidor y planificar vectores de ataque.

3.8 Bases de datos de exploits

Un exploit en una porción de código desarrollado en cualquier lenguaje de programación para quebrantar una vulnerabilidad específica de alguna aplicación en particular. En el campo de las vulnerabilidades informáticas existe lo que se conoce como bases de datos de vulnerabilidades en las cuales se recopila todos los exploits o vulnerabilidades diferenciados por identificadores únicos como son CVE y OSVDB.

- **CVE:** son las siglas de vulnerabilidades y exposiciones comunes, es una lista de vulnerabilidades y exposiciones de seguridad de la información, es decir a cada vulnerabilidad reportada se le asigna un identificador único con el siguiente formato (CVE: 2014-3805) el cual se encuentra formado por el año de descubrimiento y el número de la vulnerabilidad.
- **OSVDB (Open Source Vulnerability Database):** es una base de datos de vulnerabilidades de libre distribución, similar a la anterior clasificación se asigna un número de cinco dígitos a cada vulnerabilidad reportada.
- **Exploit Database:** Es una base de datos de exploits en la que se recopila todos los exploits publicados a nivel mundial disponibles de manera gratuita para la descarga o consulta. Esta base de datos es la utilizada por Kali Linux para actualizar la lista de exploits localizada en la dirección www.exploit-db.com.
- **Inj3ct0r:** Considerada la mayor base de datos de exploits del mundo alberga todos los exploits libres y comercializa muchos otros catalogados como eficientes y letales. Alrededor del mundo hackers profesionales desarrollan exploits para explotar nuevas vulnerabilidades encontradas o conocidas pero los autores cobran una cierta cantidad de dinero por la descarga del código. La dirección web es http://es.1337day.com/.

Existen otras bases de datos en varios idiomas prácticamente con la misma información, sin embargo las citadas anteriormente son las más populares y referenciadas por los profesionales de la seguridad informática.

3.9 Búsqueda de vulnerabilidades

Durante la evaluación de los servidores se sondea los puertos abiertos y los servicios en ejecución en cada uno mediante la herramienta "nmap". Conocidas las aplicaciones y versiones de los servicios del servidor, se busca agujeros de seguridad mediante consultas en bases de datos de exploits existentes como es (www.exploit-db.com).

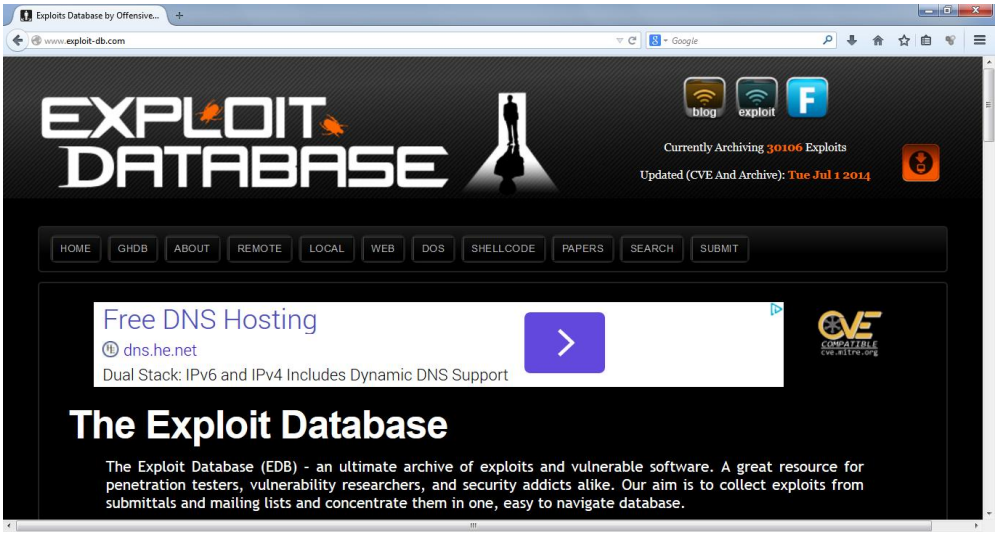

Figura 21: Base de datos de exploits www.exploit-db.com

Por ejemplo si se identificó un servicio FTP cuya versión es vsftpd 2.0.5 se procede a buscar los exploits disponibles para esta aplicación específica en la página www.exploit-db.com en la pestaña (Search). Este formulario facilita la búsqueda de exploits mediante varias opciones como la descripción de la aplicación, el autor del exploit, el sistema operativo, por tipo, por lenguaje, exploits por puerto o por identificadores como OSVDB o CVE.

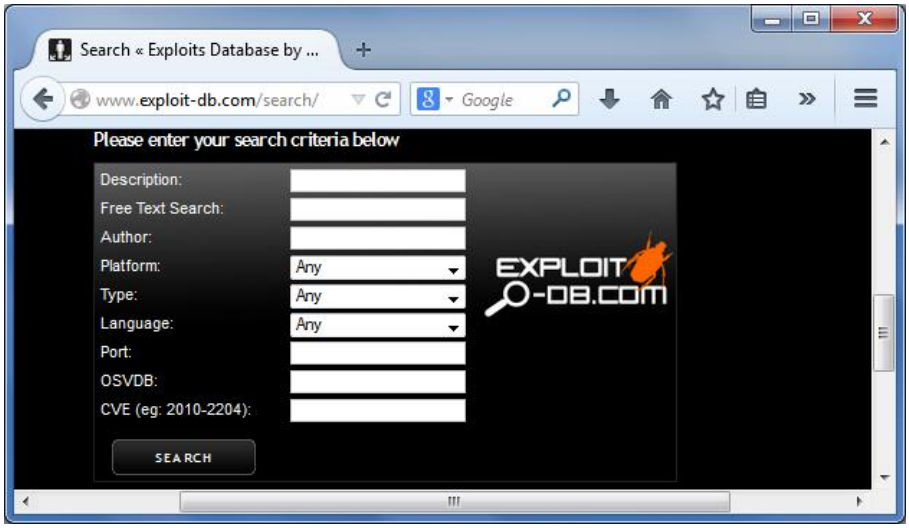

Figura 22: Formulario de búsqueda de exploits en exploit-db.

Una vez encontrado el exploit se puede acceder a información mucho más detallada como una descripción de las capacidades del código, el autor, los identificadores y el código propiamente dicho disponible para la descarga.

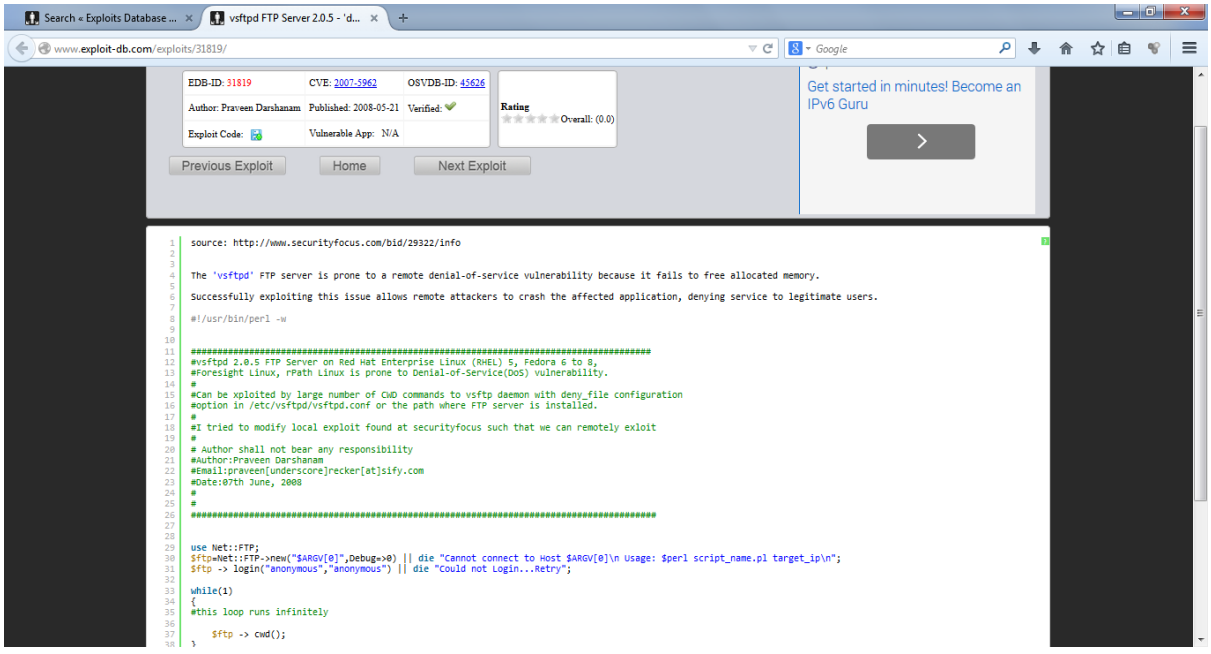

Figura 23: Código del exploit y detalles adicionales en explot-db.com

Otra forma de investigar las vulnerabilidades es utilizando los motores de búsqueda simplemente ingresando la versión de la aplicación a evaluar, esta técnica es muy

recomendable porque algo importante a conocer es que no todas las vulnerabilidades poseen exploits, por el contrario muchas de ellas pueden ser explotadas manualmente como también lo es la identificación de la vulnerabilidad.

Un ejemplo práctico de ello son las vulnerabilidades en php (Lenguaje de programación para el desarrollo de páginas web dinámicas) las cuales son explotadas añadiendo un símbolo como (~ ó -s dependiendo de la versión) al final de la dirección web en la barra de na navegación, lo cual permite acceder al código fuente de la aplicación (php). Como se ilustra en la figura 24 mediante esta vulnerabilidad es posible acceder al código de un archivo (.php) el cual se conecta a la base de datos la información encontrada corresponde al nombre de usuario y contraseña de la base de datos, información considerada de suma importancia y confidencial cuyo conocimiento por atacantes maliciosos puede desencadenar el borrado total de la información contenida en la base de datos o subir un malware el cual permita apoderarse del servidor o muchas otras opciones. Este caso corresponde la explotación manual de la vulnerabilidad.

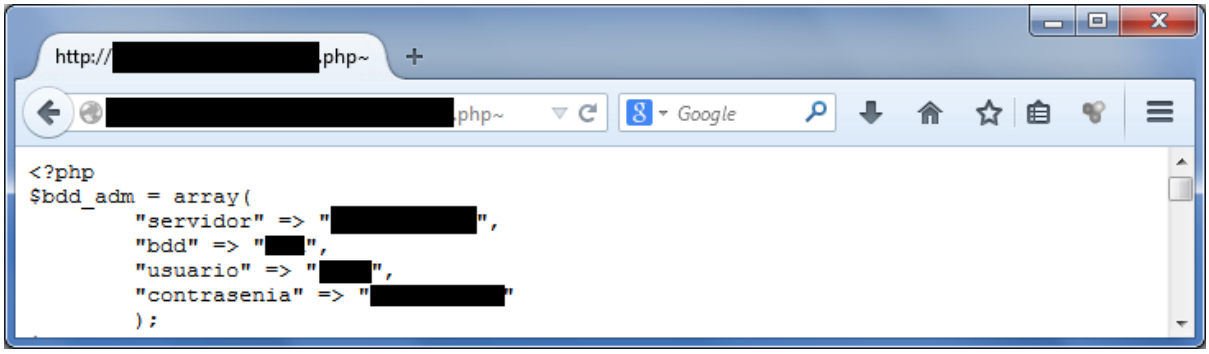

Figura 24: Nombre de usuario y la contraseña de la base de datos revelada en un archivo del servidor.

3.10 Escaneo de Vulnerabilidades

Las aplicaciones dedicadas a la identificación de vulnerabilidades son muy demandantes en el área de seguridad de la información, su funcionamiento se basa en la identificación de los banners de las aplicaciones por cada puerto y las versiones de los sistemas operativos. Dichas aplicaciones trabajan en primera instancia recolectando información de cada puerto abierto, principalmente las versiones de las aplicaciones. Con esta información buscan las vulnerabilidades reportadas por cada versión de la aplicación y son presentados mediante reportes al usuario. En otras palabras automatizan las actividades descritas hasta el momento en recolección de información e identificación de vulnerabilidades.

El escáner de vulnerabilidades más utilizado a nivel mundial es Nessus por las capacidades en la eficiencia en este campo, debido a la gran cantidad de plugins[17] que posee gracias a sus desarrolladores. La desventaja principal es que Nessus es un software comercial para grandes corporaciones constituidas por numerosas computadoras y servidores, sin embargo la versión gratuita admite es escaneo de quince (15) direcciones IP, lo cual puede ser suficiente para una empresa de mediano tamaño.

Nessus no se encuentra instalado en Kali Linux pero la instalación es relativamente fácil, solamente se accede a la página web oficial de nessus y se descarga el paquete con extensión (.deb) para plataforma debían. Una vez instalado el paquete se procede con el ingreso de la clave de activación de la aplicación enviada al correo electrónico y se continúa con los pasos indicados por la aplicación.

---

[17] **Plugin:** Es una pequeña aplicación que funciona en otra para añadir funciones adicionales.

La interfaz de administración de Nessus es una aplicación web muy sencilla de utilizar basta con seleccionar la pestaña (New Scan) e ingresar la dirección IP del equipo a evaluar o el nombre de dominio como se demuestra en la figura 25.

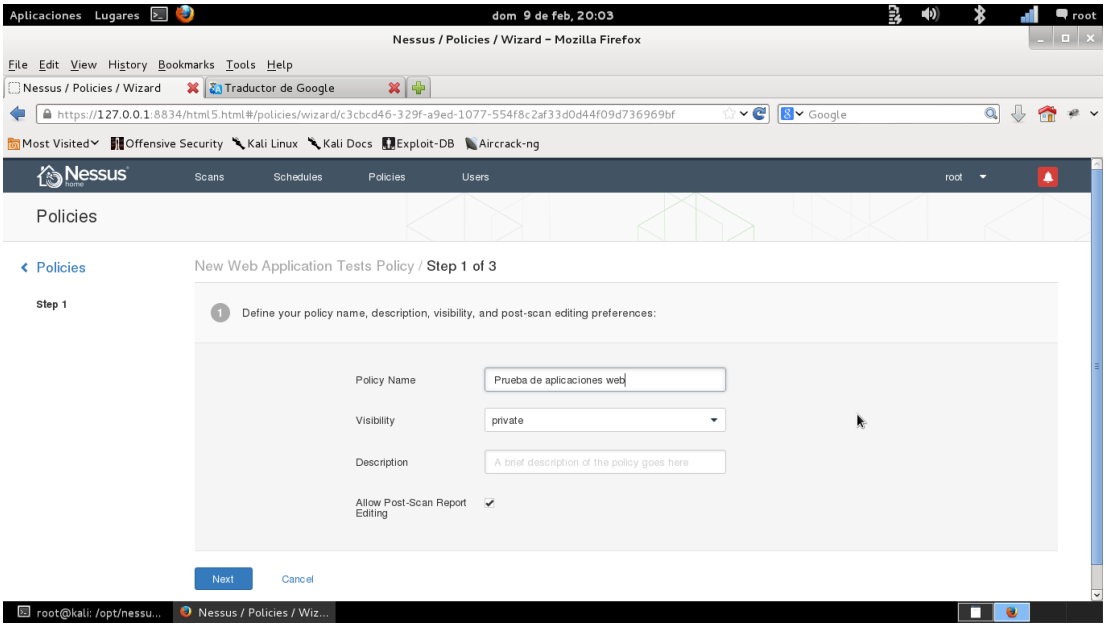

Figura 25: Nuevo escaneo de vulnerabilidades mediante Nessus.

Nessus reporta las vulnerabilidades encontradas clasificándolas en base a la criticidad, sin embargo no es capaz de evaluar la veracidad de la vulnerabilidad, es decir se reporta muchos falsos positivos, por lo tanto esta herramienta es una ayuda más pero se debe verificar todos los resultados entregado por Nessus y descartar las falsas vulnerabilidades.

3.11 Explotación de vulnerabilidades.

Una vez identificadas las vulnerabilidades y los códigos de explotación muchas veces es necesario la utilización de software especializado para explotar las vulnerabilidades sin embargo es importante aclarar que se requiere de una vulnerabilidad real para que la herramienta sea efectiva, no se puede lanzar una herramienta al azar y esperar resultados favorables, por esta razón las etapas de recolección de información e identificación de

vulnerabilidades representan un gran aporte en el proceso de hacking ético y usualmente involucra mucho tiempo de investigación.

A nivel mundial existe una organización enfocada a la seguridad en aplicaciones web llamada OWASP la cual centra sus esfuerzos en dar a conocer las mejores prácticas en el desarrollo, adquisición y mantenimiento de aplicaciones con un alto grado de seguridad. Esta organización posee un proyecto llamado OWASP TOP 10 el cual cada año describe las diez vulnerabilidades más comunes detectadas por los servidores a nivel mundial, la siguiente tabla representa dicha información en el año 2013.

Tabla 1 Top ten riesgos de seguridad en aplicaciones

OWASP TOP 10 DE RIESGOS DE SEGURIDAD EN APLICACIONES
1 - Inyección SQL
2 - Pérdida de autenticación y gestión de sesiones
3 - Secuencias de comandos en sitios cruzados (XSS)
4 - Referencia directa insegura a objetos
5 - Configuración de seguridad incorrecta
6 - Exposición de datos sensible
7 - Ausencia de control de acceso a funciones
8 - Falsificación de peticiones de sitios cruzados
9 -Utilización de componentes con vulnerabilidades conocidas
10 - Redirecciones y reenvíos no válidos

Nota: Fuente: Reporte OWAP. Recuperado de: https://www.owasp.org/images /5/5f/OWASP_Top_10_-_2013_Final_-_Espa%C3%B1ol.pdf

3.11.1 Inyección SQL

Esta técnica consiste en comunicarse con la base de datos mediante el ingreso de código SQL[18] por medio del navegador web con la finalidad de extraer toda la información contenida en la base de datos. El éxito de la explotación es posible gracias a la identificación de la aplicación que consulta con a base de datos para presentar al usuario la información solicitada.

[18] **SQL:** Es un lenguaje de acceso a la base de datos o creación de base de datos por medio de código.

Por lo tanto en la fase de identificación de vulnerabilidades se identificó alguna variable que admita únicamente valores numéricos de entrada, los cuales son enviados a la base de datos para el retorno de la información solicitada la identificación.

La detección de la variable vulnerable es realizada añadiendo el símbolo de comilla simple (‘) en la dirección web, en reemplazo del valor numérico lo cual deberá cambiarse la página web por otra en blanco o con un valor diferente al original.

El punto débil de esta técnica es el desconocimiento de las características de la base de datos como el nombre de las bases de datos, nombres de las tablas, las columnas, tipo de datos, por lo tanto dicha tarea se facilita utilizando herramientas de inyección SQL.

En sistemas Windows la mejor herramienta y la más utilizada por la facilidad de uso es Havij. Como se aprecia en la figura 26 en el campo de “Target” se debe ingresar la dirección web que contenga la variable vulnerable y solamente se interactúa con las opciones señaladas por la herramienta.

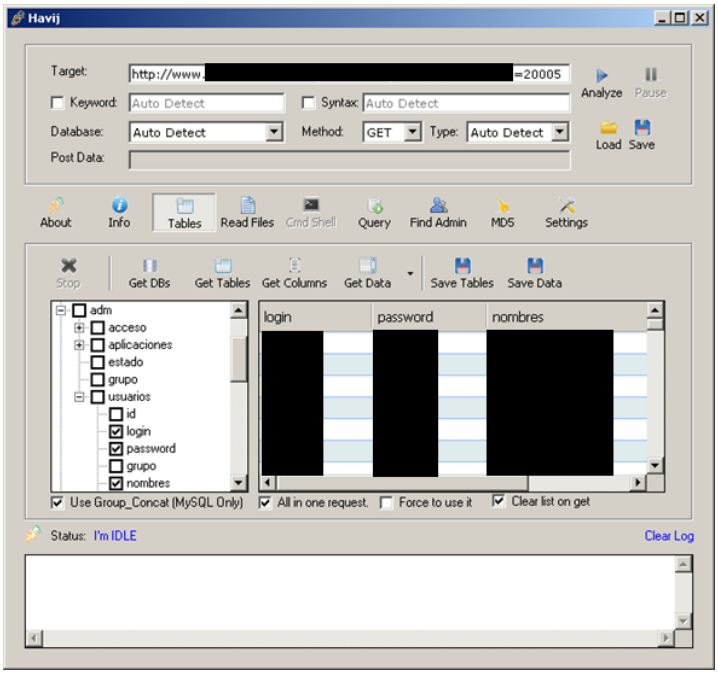

Figura 26: Extracción de información confidencial de la base de datos como nombres de usuario y contraseñas.

En Kali Linux la herramienta por excelencia es sqlmap permitiendo el uso únicamente por consola de comandos siendo fácil la utilización. Las opciones básicas utilizadas son las siguientes:

- -u [Dirección web]: Especifica la dirección web vulnerable con la variable de tipo numérica.
- --dbs: Búsqueda de todas las bases de datos del servidor.
- -D [Nombre de la base de datos]: Especifica la base de datos.
- --tables: Búsqueda de todas las tablas de una base de datos.
- -T [Nombre de la tabla]: Especifica el nombre de la tabla
- --columns: Búsqueda de todas las columnas de una tabla
- -C [Nombre de columna]: Especifica el nombre de la columna de una tabla.
- --dump: Extrae todos los datos de las columnas seleccionadas.

Como ejemplo de la usabilidad de la herramienta se tiene el siguiente comando el cual permite detectar las bases de datos disponibles en por medio de la dirección web vulnerable.

```
root@kali:~# sqlmap -u http://dirección_web_vulnerable --dbs
```

Una vez identificada la base de dato, la tabla y las columnas se ingresa el siguiente comando de ejemplo para extraer los datos de las columnas seleccionadas de la siguiente manera.

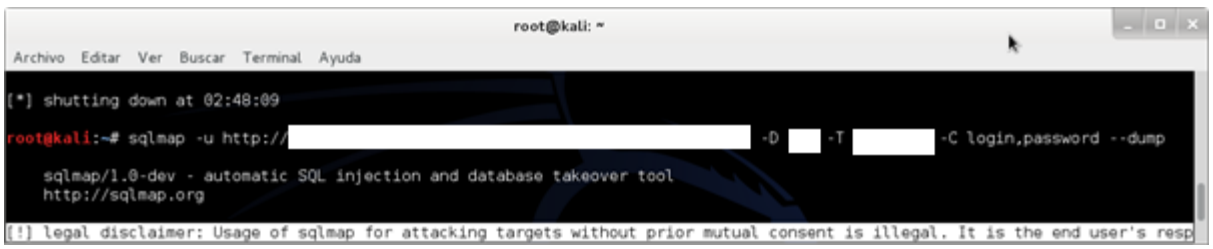

Figura 27: Uso de sqlmap para extraer datos de la base de datos.

3.11.2 Secuencias de comandos en sitios cruzados (XSS)

Conocida en el campo de la seguridad informática como “Cross site scipting” las vulnerabilidades de este tipo permite al atacante ingresar código malicioso en las páginas web visitadas por el usuario modificando la página web original y presentando otro contenido al usuario, el cual estará confiado que es la página pertenece a la institución la cual visita pero en realidad no lo es y es posible engañar al usuario con varios fines maliciosos.

La vulnerabilidad es posible debido a un mal filtrado de las variables de entrada la cual perite ejecutar en el servidor web el código ingresado por medio del navegador. La detección de la variable vulnerable se detecta interactuando con ella ingresando valores de texto y descubrir la ejecución del código ingresado. Un ejemplo práctico de ello se representa en la figura 28 en la cual se observa que ha sido eliminado el contenido original de la página web y fue reemplazado por otro texto demostrativo.

Figura 28: Verificación de la vulnerabilidad XSS

3.11.3 Metasploit y Exploits

Kali Linux incorpora en su arsenal de herramientas a “Metasploit”, una poderosa aplicación que posee un conjunto de módulos con el fin de explotar las vulnerabilidades de los servidores. Su campo de acción se basa en la ejecución de exploits escritos en lenguaje de programación ruby.

Metasploit utiliza gran cantidad de datos para la ejecución de los ataques porque almacena en el sistema operativo todos los exploits conocidos hasta la fecha, por lo tanto Metasploit para gestionar todos los exploits, módulos y auxiliares utiliza una base de datos en postgresql, no solamente para realizar estas actividades, también para almacenar los ataques y escaneos por el tiempo que dura el proceso de explotación.

Para utilizar la herramienta se debe iniciar el servicio ingresando el siguiente comando en la consola de comandos: (#service metasploit start) o también (#/etc/init.d/metasploit start), de esta manera se inicia la base de datos y metasploit. Solo resta ingresar (#msfconsole) y se habilita la aplicación como se ilustra en la figura 29.

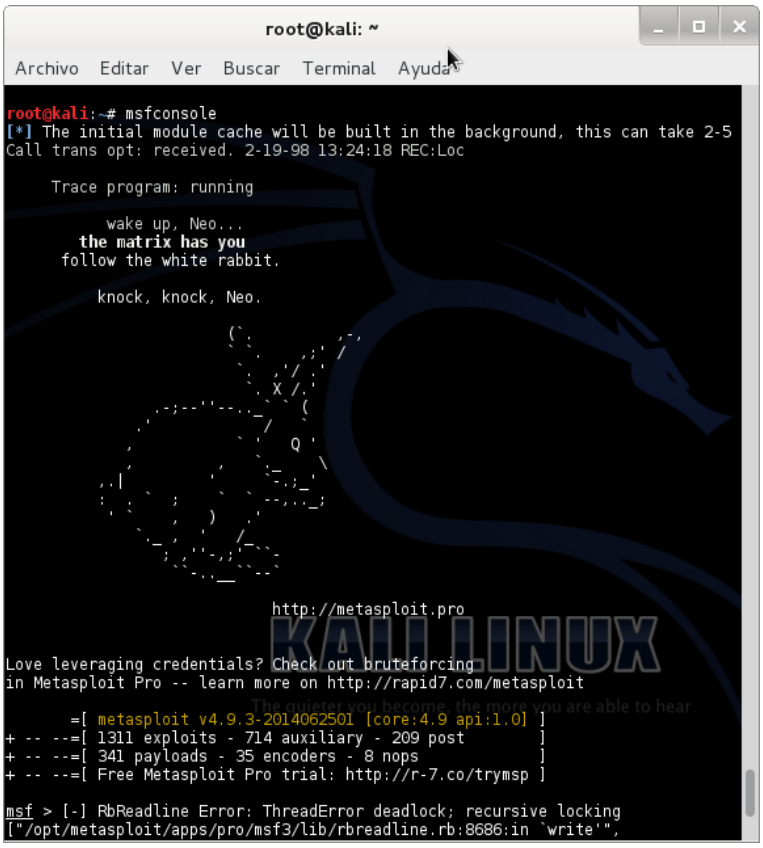

Figura 29: Presentación de la herramienta de explotación Metasploit

La forma como Metasploit trabaja es mediante el uso de dos tipos de códigos, el primero son los exploits exclusivos para cada vulnerabilidad y plataforma, el segundo código son los payloads utilizados después de que el exploit tuvo éxito en quebrantar la

vulnerabilidad el cual realiza la tarea de penetrar en el sistema afectado, es decir el exploit lo único que realiza es aprovecharse de la vulnerabilidad y quebranta la seguridad pero deja un camino abierto, el cual es utilizado por el payload para ingresar al sistema operativo con el fin de ejecutar comandos o acciones en la máquina vulnerada bajo el control del atacante informático.

Metasploit utiliza comandos propios para la configuración de las opciones de los exploits, los comandos clave son los siguientes:

- search: Búsqueda de exploit en la base de datos.
- use: Selecciona el exploit a utilizar
- set: Establece los valores a cada una de las opciones que el exploit requiere para operar.
- exploit: Inicialización del ataque.

Un ejemplo práctico de la facilidad de la utilización de la herramienta se encuentra representado en la figura 30. En esta ocasión el exploit utilizado es “php_cgi_arg_injection” que explota una vulnerabilidad en php mediante el protocolo http en un servidor Windows Server 2008, las opciones de configuración del exploit son las siguientes:

- set RHOST: Ingresa la dirección IP del servidor remoto o víctima.
- set LHOST: Ingresa la dirección IP de la máquina del atacante.
- set TARGETURI: Ingresa la dirección web donde se aloja la vulnerabilidad.
- set PAYLOAD: Ingresa el código de a ejecutarse en el servidor remoto o víctima.
- exploit: empieza el ataque.

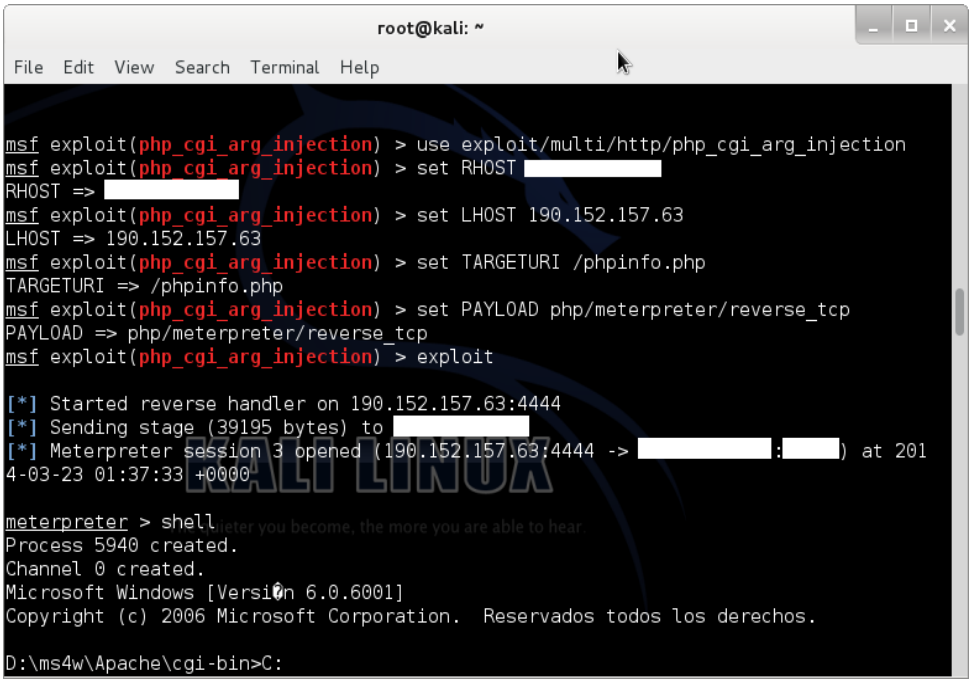

Figura 30: Ejeccución del exploit php_cgi_arg_injection mediante metasploit

El payload seleccionado en esta ocasión es conocido como "meterpreter[19]" el cual ejecuta comandos en la máquina vulnerada a elección del atacante, el comando "shell" permite conseguir una consola de comandos de Windows "CMD" lo cual comprueba la versión del sistema operativo Windows.

3.11.4 Software cliente

Para la explotación de las vulnerabilidades también es posible realizarlo utilizando el software cliente de las aplicaciones, en algunos de los casos se podrá acceder a los servicios por fallas en la configuración o ausencia de controles de acceso como se demuestra en la figura 31.

[19] **Meterpreter:** Es una herramienta utilizada como payload, utiliza inyección de código ensamblador en el proceso vulnerable permitiendo obtener al atacante una consola de comandos.

Figura 31: Acceso al servidor VNC y FTP sin restricciones al no solicitar credenciales de acceso.

El software cliente también es utilizado en la fase de explotación como medio para verificar credenciales de acceso conseguidas. En la figura 32 se aprecia el acceso a la base de datos postgresql por medio de la aplicación cliente utilizando las credenciales de autenticación detectadas previamente.

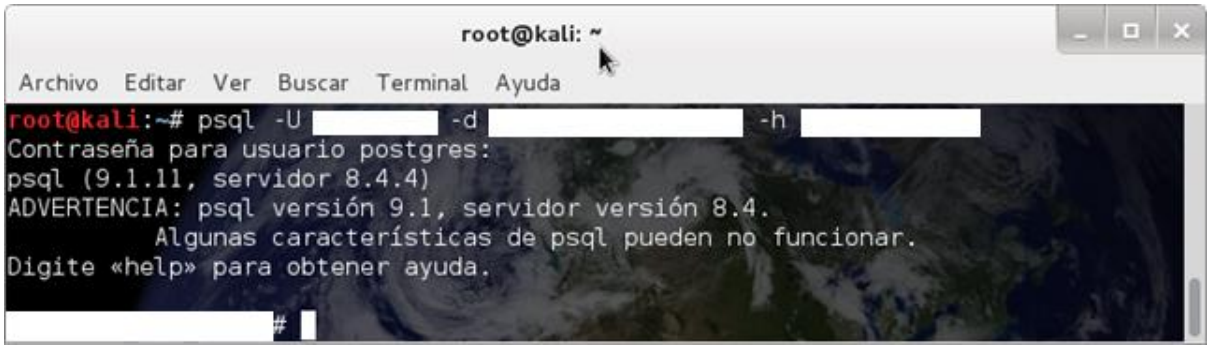

Figura 32: Verificación de la contraseña conseguida por medio de software cliente a la base de datos postgresql

Otros ejemplos prácticos referentes a este tema es la utilización de aplicaciones clientes para verificación de servicios como putty, phpMyAdmin, pgAdmin.php, escritorio remoto, navegadores web y muchos más.

3.11.5 Comunicaciones inseguras

El análisis de los medios para establecer comunicaciones remotas con los servidores es un área importante de investigación el cual puede revelar las prácticas utilizadas para la gestión de bases de datos, conexiones ssh, telnet, ftp inseguro entre otras.

La evaluación de canales sin cifrado permite el envió de información sensible como las credenciales de autenticación a los sistemas en texto plano sin encriptar, brindando gran

facilidad en la interceptación mediante herramientas de sniffing[20], man in the middle[21] entre otras.

Existe una inclinación por parte de los desarrolladores de sitios web a utilizar la combinación de paquetes informáticos como Apache, Mysql y PHP en aplicaciones como xampp server, wamp server, permitiendo ser consumidores de dichos productos sin considerar las múltiples vulnerabilidades de las que son sujetas.

Como ejemplo una aplicación que presenta una falencia de importancia en la transmisión de nombres de usuario y contraseñas sin cifrar es “phpMyAdmin.php” el cual permite comunicarse con la base de datos. En la figura 33 se ilustra la herramienta web utilizada para acceder a la base de datos del servidor local, para ello se ha ingresado dos credenciales de prueba.

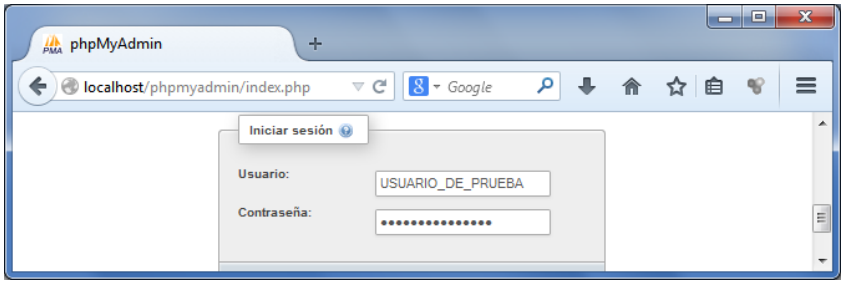

Figura 33: Envió de credenciales de autenticación a través de “phpMyAdmin.php”.

El procedimiento para interceptar o capturar el tráfico de los paquetes desde navegador web hacia el servidor se lo realiza mediante la herramienta “wireshark”. Wireshark es el software más utilizado a nivel mundial disponible tanto para sistemas operativos Windows y Linux, Kali Linux posee dicha herramienta por defecto desde la

[20] **Sniffing:** Técnica de captura de paquetes que circulan por una interfaz de red.
[21] **Man in the middle:** Es un tipo de ataque en el cual se intercepta las comunicaciones de la víctima y los envía al destino original pero el atacante posee el control de las comunicaciones y accede a la información de la víctima.

instalación. El uso de esta herramienta se facilita debido a que posee una interfaz gráfica muy amigable con el usuario permitiendo auditar cada paquete si es necesario.

En esta ocasión wireshark capturó el paquete que contiene el método POST el cual contiene la información ingresada en el formulario. Al acceder al contenido del paquete se identificó el nombre de usuario y la contraseña de prueba como se demuestra en la figura 34.

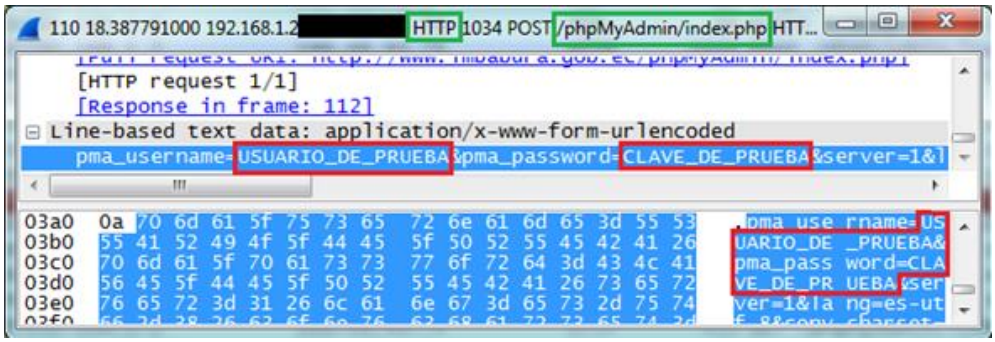

Figura 34: Captura del paquete con el contenido ingresado en el formulario de phpMyAdmin.php

Los métodos para el envío de información utilizados en portales web son POST y GET, los cuales presentan características de funcionamiento propias y el uso de uno de ellos depende de la aplicación. La siguiente tabla resume las diferencias entre POST y GET.

Tabla 2 Diferencias entre los métodos POST y GET

MÉTODO	POST	GET
DEFINICIÓN	Envía los datos de forma oculta para los usuario por medio de un paquete.	Envía los datos por medio de la URL del navegador web, es decir son visibles los datos.
CARACTERÍSTICAS	Los datos enviados no son visibles por el usuario y la URL no se modifica.	Los datos on visibles y enviador por la URL. www.dominio.com/action.php?username=juan &pass=juan123
DESVENTAJAS	La información es transmitida en texto plano, siendo fácilmente capturada por cualquier snnifer.	El usuario podría modificar la URL modificando el contenido de las variables en el navegador web.

CAPÍTULO IV

DISEÑO DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN

Como parte de los requerimientos previos a la selección de los controles de la norma ISO/IEC 27001, el tercer documento consiste en el análisis de riesgos de los activos de información del Gobierno Provincial de Imbabura. Como punto de partida para la elaboración del informe, se toma el inventario de activos previamente establecido y se procede con el análisis de varios criterios descritos en la metodología Magerit e interrelacionarnos entre ellos con el fin de determinar los riesgos a los que dichos activos se encuentran sometidos.

Todo el análisis de riesgos se basa en la metodología Magerit dedicada especialmente al análisis y gestión de riesgos de los sistemas de información. Se ha consultado esta herramienta para la identificación, clasificación y valoración de los activos, como también la identificación y valoración de las amenazas a las que están expuestos los activos del GPI.

4.1 Identificación de los activos de información

Los activos que formarán parte del proceso del sistema de gestión de seguridad de la información, han sido seleccionados en base a la importancia para la institución en cuanto se refiere al cumplimiento de las propiedades de la seguridad de la información como son la confidencialidad, la integridad, la disponibilidad, la autenticidad y la trazabilidad, es decir los dispositivos y elementos encargados del almacenamiento, modificación y transportación de la información.

De acuerdo a la recomendación de la metodología Magerit cada activos de información debe ser asignado un código identificativo entre corchetes [] para trabajar de

mejor manera a través de todo el proceso. A continuación se listan los activos de información más importantes de la institución los cuales se detallan en el capítulo dos.

- Atención al público [At_pub]
- Quipux[Gest_doc]
- Zimbra_email [email]
- Web [web]
- Proxy [proxy]
- Elastix [serv_voz_ip]
- Gis [Gis]
- Olympo [Olympo]
- Servidor blade [serv_blade]
- Switch de core [SW_C]
- Switch de acceso [SW_A]
- Firewall [FW]
- Packet Shaper [AB]
- Router CNT [R_CNT]
- PC[PC]
- Cableado estructurado [Cabling_estr]
- Backbon [backbon]
- Sistema de aire acondicionado [Sist_aire_acond]
- UPS [UPS]
- Sistema de energía eléctrica [EE]
- Control de Acceso[ctl_access]
- Cámaras de seguridad [Cam_seg]

- Sistema de monitoreo ambiental [Sist_Mon_Amb]
- Sistema de control de detección y extinción de incendio [Sist_fuego]
- Teléfono IP [Fono_ip]
- Internet [Internet]

4.2 Tipificación de los activos

La clasificación de los activos en una categoría se encuentra determinada por la importancia del mismo en la institución, la jerarquía en las operaciones y las características propias del activo. La identificación del tipo de activo establece las amenazas a las que el activo se encuentra expuesto sin embargo en base a los servicios que presta en la institución un activo puede pertenecer a varios tipos de activos.

La clasificación de los activos según la metodología Magerit ha diferenciado en 12 categorías generales resumidas en la sección 1.6.3 del presente proyecto, a su vez cada una de ellas diferencia muchos tipos de activos descritos en el documento conocido como “Catálogo de elementos” de la metodología Magerit.

En las siguientes tablas se clasifica los activos de información en base a las características propias de los elementos y a los diferentes tipos descritos en el catálogo de elementos de la Magerit.

Tabla 3 Caracterización de activos esenciales [ESENCIAL] del GPI

No	NOMBRE Y CÓDIGO	TIPO DE ACTIVOS
1	Atención al público [At_pub]	[essential][info][biz] datos de interés para el negocio [essential][info][per] datos de carácter personal nivel medio [essential][info][com] datos de interés comercial [essential][info][per][M] datos de carácter personal nivel medio [arch][sap] punto de acceso al servicio [D][password] credenciales
2	Quipux[Gest_doc]	[S][ext] a usuarios externos [S][int] interno [SW][std][www] servidor de presentación [HW][data] que almacena datos [Media][electronic][disk] discos

Tabla 4 Caracterización de servicios internos [IS] del GPI

No	NOMBRE Y CÓDIGO	TIPO DE ACTIVOS
1	zimbra_email [email]	[arch][sap] punto de acceso al servicio [D][conf] Datos de configuración [D][password] credenciales, contraseñas [S][int] interno (usuarios y medios de la propia organización) [S][email] correo electrónico [S][file] almacenamiento de ficheros
2	Web [web]	[arch][sap] punto de acceso al servicio [S][pub] al público en general
3	Proxy [proxy]	[arch][sap] punto de acceso al servicio [D][conf] datos de configuración [D][log] registro de actividad [S][int] interno (usuarios y medios de la propia organización)
4	Elastix [serv_voz_ip]	[arch][sap] punto de acceso al servicio [D][conf] datos de configuración [S][voip] voz sobre ip
5	Gis [Gis]	[arch][sap] punto de acceso al servicio [D][files] ficheros de datos [S][pub] al público en general [S][int] interno
6	Olympo [Olympo]	[arch][sap] punto de acceso al servicio [D][int] datos de gestión interna [D][password] credenciales [S][int] interno [SW][std][app] servidor de aplicaciones [HW][data] que almacena datos [Media][electronic][disk] discos

Tabla 5 Caracterización de equipos hardware [HW] del GPI

No	NOMBRE Y CÓDIGO	TIPO DE ACTIVOS
1	Servidor blade [serv_blade]	[arch][ip]punto de interconexión [D][files] ficheros de datos [D][backup] copias de respaldo [D][conf] datos de configuración [D][password] credenciales [D][int] datos de gestión interna [D][log] registro de actividad [SW][std][www] servidor de presentación [SW][std][email_server] servidor de correo electrónico [SW][std][file] servidor de ficheros [SW][std][os][windows][server_2003] [SW][std][os][linux] [SW][std][hypervisor] hypervisor [HW][mid] equipos medios [HW][data] que almacena datos [Media][electronic][disk] discos [Media][electronic][dvd] DVD
2	Switch de core [SW_C]	[arch][ip] punto de interconexión [D][conf] datos de configuración [D][password] credenciales [S][int] interno [S][telnet] acceso remoto a cuenta local [HW][network][switch] switch [COM][LAN] red local [COM][VLAN] Lan virtual

3	Switch de acceso [SW_A]	[arch][ip] punto de interconexión [HW][network][switch] switch
4	Firewall [FW]	[arch][ip] punto de interconexión [HW][network][firewall] cortafuegos
5	Packet Shaper [AB]	[arch][ip] punto de interconexión [HW][network][bridge] puente [COM][WAN] red de area amplia
6	Router CNT [R_CNT]	[arch][ip] punto de interconexión [S][www]world wide web [HW][bd] dispositivo de frontera [COM][WAN] red de área amplia [COM][Internet] Internet
7	PC[PC]	[availability][easy] fácilmente reemplazable [SW][std][browse] navegador web [SW][std][email_client] cliente de correo electrónico [SW][std][office]ofimática [SW][std][av] antivirus [SW][std][os][windows] windows [HW][pc] informática personal [Media][electronic][disk]discos [Media][electronic][cd] cederrón (CD-ROM) [Media][electronic][usb] memorias usb [Media][electronic][dvd] DVD

Tabla 6 Caracterización de activos de comunicaciones [COM] del GPI

No	NOMBRE Y CÓDIGO	TIPO DE ACTIVOS
1	Cableado estructurado [Cabling_estr]	[COM][LAN] red local [AUX][cabling] cableado de datos
2	Backbon [backbon]	[COM][LAN] red local [AUX][cabling][fiber] fibra óptica

Tabla 7 Caracterización de activos auxiliares [AUX] del GPI

No	NOMBRE Y CÓDIGO	TIPO DE ACTIVOS
1	Sistema de aire acondicionado [Sist_aire_acond]	[AUX][ac] equipos de climatización
2	UPS [UPS]	[AUX][ups] sai-sistema de alimentación ininterrumpida
3	Sistema de energía eléctrica [EE]	[AUX][power] fuentes de alimentación [AUX][gen] generadores eléctricos [AUX][cabling][wire] cable eléctrico
4	Control de Acceso[ctl_access]	[AUX][other] otros
5	Cámaras de seguridad [Cam_seg]	[AUX][other] otros
6	Sistema de monitoreo ambiental [Sist_Mon_Amb]	[AUX][other] otros
7	Sistema de control de detección y extinción de incendio [Sist_fuego]	[AUX][other] otros
8	Teléfono IP [Fono_ip]	[HW][ipphone]

Tabla 8 Caracterización de servicios subcontratados [SS] del GPI

No	NOMBRE Y CÓDIGO	TIPO DE ACTIVOS
1	Internet [Internet]	[COM][Internet] Internet

4.3 Dependencias entre activos

El análisis de los activos permite realizar un árbol de dependencias en el que se puede observar la relación entre todos los activos, como también los niveles en los cuales se han categorizado a los activos desde el de mayor importancia al menor. Los activos dependen de otros para continuar con las operaciones, dicha dependencia puede ser a uno o varios activos. En la siguiente tabla se resume las dependencias de los activos del Gobierno Provincial de Imbabura.

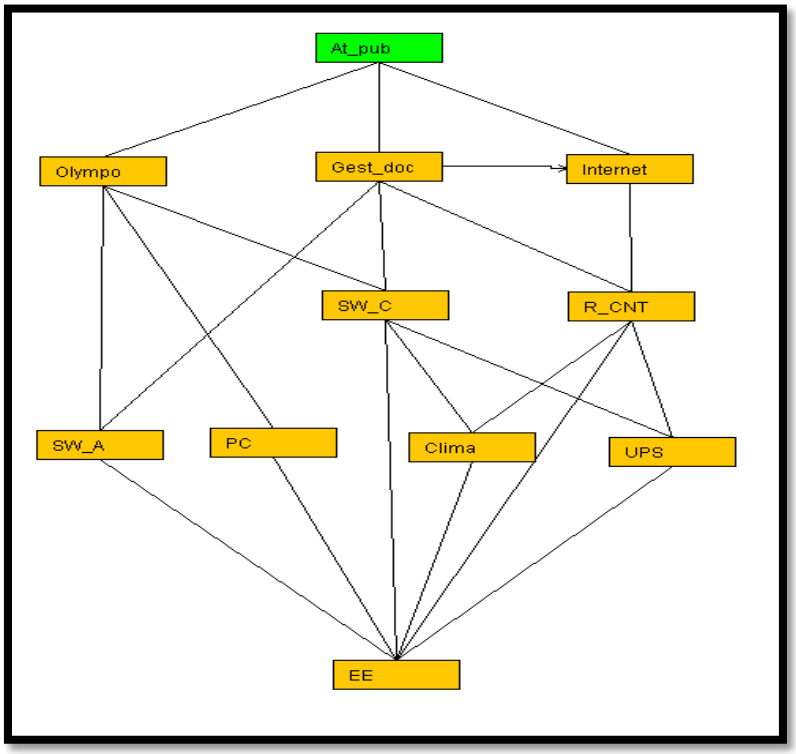

Figura 35: Primer esquema dependencias entre activos.

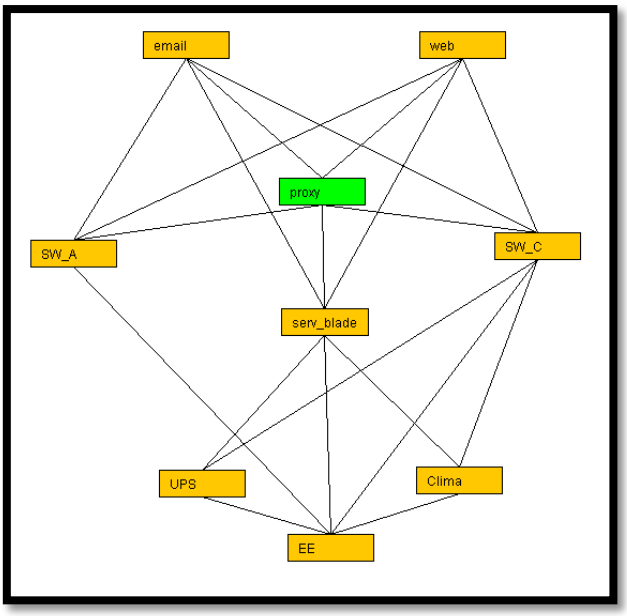

Figura 36: Segundo esquema dependencias entre activos.

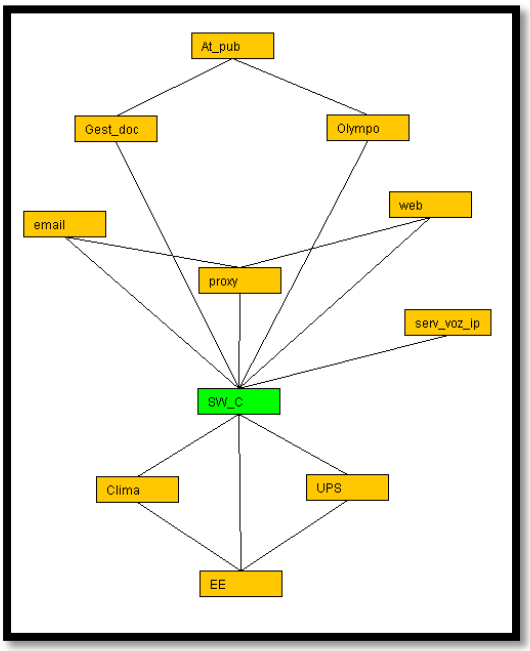

Figura 37: Dependencias en base al switch de core.

En la tabla 9 se enumeran los activos de información del GPI junto con los correspondientes activos superiores a los cuales prestan servicios, y otros inferiores de los cuales depende su funcionamiento.

Tabla 9 Dependencia entre activos

No	ACTIVO	SUPERIORES	INFERIORES
1	Atención al público [At_pub]		Quipux[Gest_doc] Olympo [Olympo] Internet [Internet]
2	Quipux[Gest_doc]	Atención al público [At_pub]	Switch de core [SW_C] Switch de acceso [SW_A] Router CNT [R_CNT] Internet [Internet]
3	zimbra_email [email]		Proxy [proxy] Servidor blade [serv_blade] Switch de core [SW_C] Switch de acceso [SW_A]
4	Web [web]		Proxy [proxy] Servidor blade [serv_blade] Switch de core [SW_C] Switch de acceso [SW_A]
5	Proxy [proxy]	zimbra_email [email] Web [web]	Servidor blade [serv_blade] Switch de core [SW_C] Switch de acceso [SW_A]
6	Elastix [serv_voz_ip]		Switch de core [SW_C] Switch de acceso [SW_A] Teléfono IP [Fono_ip]
7	Gis [Gis]		Internet [Internet]
8	Olympo [Olympo]	Atención al público [At_pub]	Switch de core [SW_C] Switch de acceso [SW_A] PC[PC]
9	Servidor blade [serv_blade]	zimbra_email [email] Web [web] Proxy [proxy]	Sistema de aire acondicionado [Sist_aire_acond] UPS [UPS] Sistema de energía eléctrica [EE]
10	Switch de core [SW_C]	Quipux[Gest_doc] zimbra_email [email] Web [web] Proxy [proxy] Elastix [serv_voz_ip] Olympo [Olympo]	Sistema de aire acondicionado [Sist_aire_acond] UPS [UPS] Sistema de energía eléctrica [EE]
11	Switch de acceso [SW_A]	Quipux[Gest_doc] zimbra_email [email] Web [web] Proxy [proxy] Elastix [serv_voz_ip] Olympo [Olympo]	Sistema de energía eléctrica [EE]
12	Firewall [FW]	Packet Shaper [AB]	Sistema de aire acondicionado [Sist_aire_acond] UPS [UPS] Sistema de energía eléctrica [EE] Router CNT [R_CNT] Firewall [FW]
13	Packet Shaper [AB]		Sistema de aire acondicionado [Sist_aire_acond] UPS [UPS] Sistema de energía eléctrica [EE]
14	Router CNT [R_CNT]	Quipux[Gest_doc] Firewall [FW] Internet [Internet]	Sistema de aire acondicionado [Sist_aire_acond] UPS [UPS] Sistema de energía eléctrica [EE]
15	PC[PC]	Olympo [Olympo]	Sistema de energía eléctrica [EE]

16	Cableado estructurado [Cabling_estr]		
17	Backbon [backbon]		
18	Sistema de aire acondicionado [Sist_aire_acond]	Servidor blade [serv_blade] Switch de core [SW_C] Firewall [FW] Packet Shaper [AB] Router CNT [R_CNT]	Sistema de energía eléctrica [EE]
19	UPS [UPS]	Servidor blade [serv_blade] Switch de core [SW_C] Firewall [FW] Packet Shaper [AB] Router CNT [R_CNT]	Sistema de energía eléctrica [EE]
20	Sistema de energía eléctrica [EE]	Servidor blade [serv_blade] Switch de core [SW_C] Switch de acceso [SW_A] Firewall [FW] Packet Shaper [AB] Router CNT [R_CNT] PC[PC] Sistema de aire acondicionado [Sist_aire_acond] UPS [UPS] Control de Acceso[ctl_access] Sistema de monitoreo ambiental [Sist_Mon_Amb] Sistema de control de detección y extinción de incendio [Sist_fuego]	
21	Control de Acceso[ctl_access]		Sistema de energía eléctrica [EE]
22	Cámaras de seguridad [Cam_seg]		
23	Sistema de monitoreo ambiental [Sist_Mon_Amb]		Sistema de energía eléctrica [EE]
24	Sistema de control de detección y extinción de incendio [Sist_fuego]		Sistema de energía eléctrica [EE]
25	Teléfono IP [Fono_ip]	Elastix [serv_voz_ip]	
26	Internet [Internet]	Gis [Gis]	Router CNT [R_CNT]

4.4 Valoración por activo de información

La valoración de los activos recomendado por la metodología Magerit es una escala del cero al diez, de esta manera una calificación de cero supondría que el activo no tiene mucha importancia y su pérdida o daño no afectaría a las actividades de la organización, todo lo contrario si la valoración es diez demostrando la enorme importancia del activo.

La valoración es realizada en base a la importancia para las operaciones de la organización evaluando las cinco propiedades de la seguridad de la información como son la

confidencialidad de la información [C], la integridad de los datos [I], la disponibilidad [D], autenticidad [A] y trazabilidad [T].

Tabla 10 Niveles de criticidad en una escala de valores del cero al 10.

CRITERIO	VALOR
10	Daño extremadamente grave
9	Daño muy grave
6-8	Daño grave
3-5	Daño importante
1-2	Daño menor
0	Irrelevante a efectos prácticos

Nota: Tomado del catálogo de elementos de la Metodología de análisis y gestión de riesgos de los sistemas de información.

4.4.1 Resumen del valor propio de los activos

Cada uno de los activos es sometido al análisis de las cinco propiedades de la información en base a 13 categorías generales que describen cuales serían las posibles consecuencias si los activos fueran sometidos a diferentes motivos. Este criterio de valoración busca ser lo más homogéneo posible entre todos los tipos de activos.

Son muchos criterios utilizados en esta parte del proyecto para determinar el valor de cada propiedad de la información por activo de información, los cuales son descritos en el capítulo cuatro del libro “Catálogo de elementos” de la metodología Magerit. La siguiente tabla concentra el resultado final de la valoración de las propiedades de la información.

Tabla 11 Valor propio de activos en base a criterios de confidencialidad de la información [C], la integridad de los datos [I], la disponibilidad [D], autenticidad [A] y trazabilidad [T].

ACTIVO	[D]	[I]	[C]	[A]	[T]
Atención al público [At_pub]	10	7	7	9	4
Quipux[Gest_doc]	1	7	7	7	4
Zimbra_email [email]	3	7	4	9	8
Web [web]	4	7			
Proxy [proxy]	7	9	7	9	5
Elastix [serv_voz_ip]	3	7	7	7	9
Gis [Gis]	5	7			
Olympo [Olympo]	4	7	7	7	4
Servidor blade [serv_blade]	7	7		5	8
Switch de core [SW_C]	9	7	9	9	7
Switch de acceso [SW_A]	5	7		7	4
Firewall [FW]	7	7	7	7	8
Packet Shaper [AB]	3	7	3	7	7

Router CNT [R_CNT]	7	7	9	9	7
PC[PC]	3	7	7	6	5
Cableado estructurado [Cabling_estr]	3				
Backbon [backbon]	4				
Sistema de aire acondicionado [Sist_aire_acond]	4				
UPS [UPS]	3				
Sistema de energía eléctrica [EE]	9				
Control de Acceso[ctl_access]	7	7	5	7	4
Cámaras de seguridad [Cam_seg]	3	3	3	1	
Sistema de monitoreo ambiental [Sist_Mon_Amb]	7	3			
Sistema de control de detección y extinción de incendio [Sist_fuego]	7	7			
Teléfono IP [Fono_ip]	1	0	3	1	
Internet [Internet]	4	7	3		

4.4.2 Resumen del valor acumulado de los activos

El valor acumulado de un activo en una relación de dependencia constituye la herencia del máximo valor de los activos superiores a los cuales el activo presta servicio, es decir un activo adquiere el valor de cada propiedad de la información heredando el máximo valor de los activos a los cuales presta servicio.

Tabla 12 Valor acumulado de activos en base a criterios de confidencialidad de la información [C], la integridad de los datos [I], la disponibilidad [D], autenticidad [A] y trazabilidad [T].

ACTIVO	[D]	[I]	[C]	[A]	[T]
Atención al público [At_pub]	10	7	7	9	4
Quipux[Gest_doc]	10	7	9	9	4
Zimbra_email [email]	3	7	4	9	8
Web [web]	4	7			
Proxy [proxy]	7	9	7	9	8
Elastix [serv_voz_ip]	3	7	7	7	9
Gis [Gis]	5	7			
Olympo [Olympo]	10	7	9	9	4
Servidor blade [serv_blade]	7	9	9	9	8
Switch de core [SW_C]	10	9	9	9	9
Switch de acceso [SW_A]	10	9	9	9	9
Firewall [FW]	7	7	7	7	8
Packet Shaper [AB]	3	7		3	
Router CNT [R_CNT]	10	7	9	9	8
PC[PC]	10	7	9	9	5
Cableado estructurado [Cabling_estr]	10	9	9	9	9
Backbon [backbon]	10	9	9	9	9
Sistema de aire acondicionado [Sist_aire_acond]	10				

UPS [UPS]	10				
Sistema de energía eléctrica [EE]	10	9	9	9	9
Control de Acceso[ctl_access]	10	7	5	5	4
Cámaras de seguridad [Cam_seg]	3	3	3	1	
Sistema de monitoreo ambiental [Sist_Mon_Amb]	7	3			
Sistema de control de detección y extinción de incendio [Sist_fuego]	7	7			
Teléfono IP [Fono_ip]	3	7	7	7	9
Internet [Internet]	10	7	9	9	4

4.5 Amenazas de los activos

De acuerdo a lo descrito en la sección 1.6.6 del presente proyecto, la metodología Magerit clasifica a las amenazas en 12 categorías generales de las cuales se derivan otras más específicas. La selección de las amenazas de los activos es realizada en función del tipo o tipos de activos en los que se ha clasificado a cada uno de los elementos inmersos en el análisis de riesgos. Magerit facilita esta tarea debido a que cada amenaza sólo puede afectar a determinados tipos de activos, por lo tanto para el caso de este proyecto al utilizar la herramienta “PILAR”, la selección de las amenazas de cada uno de los activos es un proceso automático y la valoración del riesgo también lo es.

4.6 Informe de análisis de riesgos

Una vez identificados los activos, la clasificación a la que pertenece, las relaciones de dependencia y la valoración de cada una de las propiedades de la información según los lineamientos de la metodología Magerit, se procede con la elaboración del informe de análisis de riesgos el cual consiste en la identificación expresa de las amenazas por cada activo de información y el valor de cada propiedad de la información. El informe de análisis de riesgos se encuentra en el anexo A.

4.7 Diseño del SGSI

En base al análisis de riesgos de los activos de información y el informe de vulnerabilidades se procede a seleccionar los controles recomendados en el anexo A de la norma ISO/IEC 27001:2005 a ser implementados para gestionar el riesgo en los activos de información del Gobierno Provincial de Imbabura

4.7.1 Actividades realizadas

Los controles son seleccionados en base a las amenazas a los que se encuentran expuestos y las vulnerabilidades que poseen. Ambos requisitos obedecen al análisis de riesgos de los activos de la información y el informe de vulnerabilidades.

A continuación se enumeran los activos de información sometidos al análisis de riesgos ordenados en base al tipo de activo al que pertenece y al nivel de importancia del activo.

Tabla 13 Activos de información del Gobierno Provincial de Imbabura

GRUPOS DE ACTIVOS	ACTIVOS DE INFORMACIÓN	
ESENCIALES **SERVICIOS INTERNOS**	• Atención al público • Servidor de correo • Servidores web • Servidor proxy	• Quipux • Servidor Elastix • Servidor GIS • Plataforma Olympo
EQUIPOS	• Servidor Blade • Switch de Core • Switch de Accesos	• Packet Shaper • Router CNT • Firewall
COMUNICACIONES	• Cableado Estructurado	• Backbone
ELEMENTOS AUXILIARES	• Sistema de aire acondicionado • Sistema de energía eléctrica • Control de Accesos • UPS • Cámaras de seguridad	• Sistema de monitoreo ambiental • Sistema de control de detección y extinción de incendio • Teléfono IP
SERVICIOS SUBCONTRATADOS	• Internet	

4.7.2 Procedimiento

Los activos cuyo nivel de riesgo sobrepasan los valores aceptables por la organización y no sea posible eliminarlos o transferirlos, se procede a seleccionar los controles descritos en el anexo A de la norma ISO/IEC 27001 con el fin de reducir la probabilidad de la materialización de una amenaza sobre el activo de información.

Una vez identificados los riesgos a los que están expuestos los activos de información se procede a seleccionar una de las opciones de tratamiento del riesgo. Las opciones son las siguientes.

- **Aceptación del riesgo:** La institución acepta el riesgo existente sobre un activo y continuará funcionando como lo ha estado haciendo hasta la fecha.
- **Evasión del riesgo:** Es posible evitar el riesgo mediante la eliminación del activo. Al no existir el activo no existe riego alguno.
- **Transferencia del riesgo:** Transferir el riesgo potencial de un activo a otros sistemas como son aseguradoras, pólizas de seguros u otros organismos que se encarguen de la operación y mantenimiento del activo.
- **Mitigación del riesgo:** Es la eliminación o reducción del riesgo al mínimo probable mediante la implementación de los controles necesarios que eviten, que una vulnerabilidad sea explotada por una amenaza.

4.7.3 Resultados del tratamiento de riesgos

A continuación se describen los controles seleccionados por cada amenaza y vulnerabilidad de los activos de información del Gobierno Provincial de Imbabura. El tratamiento de riesgos se ha ordenado en base a grupos de activos según menciona la metodología Magerit.

GRUPO ESENCIALES.

Tabla 14 Selección de controles del grupo de activos esenciales

AMENAZA / VULNERABILIDAD	RIESGO NO ACEPTABLE C, I o D	CONTROLES SELECCIONADOS
[N.1] Fuego	D	A.9.1.4
[N.2] Daños por agua	D	A.9.1.4
[N.*] Desastres naturales	D	A.9.1.4
[I.1] Fuego	D	A.9.1.4
[I.2] Daños por agua	D	A.9.1.4
[I.*] Desastres industriales	D	A.9.1.4, A.13.2.1
[I.3] Contaminación medioambiental	D	A.9.1.4
[I.5] Avería de origen físico o lógico	D	A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2
[I.6] Corte del suministro eléctrico	D	A.9.2.2
[I.7] Condiciones inadecuadas de temperatura o humedad	D	A.9.2.1
[I.10] Degradación de los soportes de almacenamiento de la información	D	A.10.5.1, A.13.1.2, A.15.1.3, A.10.7.2
[E.1] Errores de los usuarios	I,C,D	A.8.2.1, A.8.2.2, A.10.7.3, A.10.10.5,
[E.2] Errores del administrador	D,I,C	A.10.10.4
[E.8] Difusión de software dañino	D,I,C	A.10.4.1
[E.9] Errores de [re-]encaminamiento	C	A.11.4.7
[E.10] Errores de secuencia	I	A.8.2.2
[E.15] Alteración accidental de la información	I	A.10.10.5, A.13.1.1, A.8.1.1, A.8.2.2
[E.18] Destrucción de información	D	A.8.1.1, A.8.2.2
[E.19] Fugas de información	C	A.11.3.3, A.12.5.4
[E.20] Vulnerabilidades de los programas (software)	I,D,C	A.10.10.5, A.12.6.1, A.13.1.1
[E.21] Errores de mantenimiento / actualización de programas (software)	I,D	A.12.5.2, A.12.5.3, A.13.1.1
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	D	A.9.2.4, A.13.1.1
[E.24] Caída del sistema por agotamiento de recursos	D	A.12.6.1
[E.25] Pérdida de equipos	D,C	A.13.1.1, A.8.1.1. A.8.3.2
[A.5] Suplantación de la identidad del usuario	C,A,I	A.11.3.1
[A.6] Abuso de privilegios de acceso	C,I,D	A.11.2.2
[A.7] Uso no previsto	D.C.I	A.8.2.1, A.8.2.2, A.8.2.3
[A.8] Difusión de software dañino	D,I,C	A.10.4.1, A.10.8.1
[A.9] [Re-] encaminamiento de mensajes	C	A.10.8.4
[A.10] Alteración de secuencia	I	A.11.4.7
[A.11] Acceso no autorizado	C,I	A.9.2.1, A.10.7.4, A.11.3.1, A.11.3.3, A.11.6.1, A.11.5.2, A.11.5.5, A.8.3.3
[A.13] Repudio	I	A.11.4.7, A.11.4.3, A.8.2.3
[A.15] Modificación deliberada de la información	I	A.12.2.2
[A.18] Destrucción de información	D	A.8.2.3, A.8.3.2, A.15.1.3
[A.19] Divulgación de información	C	A.10.7.3, A.11.5.5
[A.22] Manipulación de programas	C,I,D	A.12.4.1, A.12.4.3, A.12.5.3, A.13.1.1
[A.23] Manipulación de los equipos	C,D	A.11.5.5, A.13.1.1

[A.24] Denegación de servicio	D	A.12.6.1
[A.25] Robo	D,C	A.13.2.1
[A.26] Ataque destructivo	D	A.13.1.1

GRUPO SERVICIOS INTERNOS

Tabla 15 Selección de controles del grupo servicios internos

AMENAZA / VULNERABILIDAD	RIESGO NO ACEPTABLE C, I O D	CONTROLES SELECCIONADOS
[N.1] Fuego	D	A.9.1.4, A.14.1.3
[N.2] Daños por agua	D	A.9.1.4, A.14.1.3
[N.*] Desastres naturales	D	A.9.1.4, A.14.1.3
[I.1] Fuego	D	A.9.1.4, A.14.1.3
[I.2] Daños por agua	D	A.9.1.4, A.14.1.3
[I.*] Desastres industriales	D	A.9.1.4, A.13.2.1, A.14.1.3
[I.3] Contaminación medioambiental	D	A.9.1.4
[I.5] Avería de origen físico o lógico	D	A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2
[I.6] Corte del suministro eléctrico	D	A.9.2.2, A.14.1.3
[I.7] Condiciones inadecuadas de temperatura o humedad	D	A.9.2.1
[I.10] Degradación de los soportes de almacenamiento de la información	D	A.10.5.1, A.13.1.2, A.15.1.3, A.10.7.2
[E.1] Errores de los usuarios	I,C,D	A.10.7.3, A.10.10.5
[E.2] Errores del administrador	D,I,C	A.10.10.4
[E.8] Difusión de software dañino	D,I,C	A.10.4.1
[E.9] Errores de [re-]encaminamiento	C	A.10.8.1
[E.10] Errores de secuencia	I	A.10.8.1
[E.15] Alteración accidental de la información	I	A.10.10.5, A.13.1.1, A.8.1.1, A.8.2.2
[E.18] Destrucción de información	D	A.8.1.1, A.8.2.2, A.15.1.3, A.8.3.2, A.7.2.2
[E.19] Fugas de información	C	A.12.5.4
[E.20] Vulnerabilidades de los programas (software)	I,D,C	A.10.9.3, A.12.4.1, A.12.4.3, A.12.6.1
[E.21] Errores de mantenimiento / actualización de programas (software)	I,D	A.12.5.2, A.13.1.1
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	D	A.9.2.4
[E.24] Caída del sistema por agotamiento de recursos	D	A.12.6.1, A.14.1.3
[E.25] Pérdida de equipos	D,C	A.13.1.1, A.8.1.1
[A.5] Suplantación de la identidad del usuario	C,A,I	A.11.3.1
[A.6] Abuso de privilegios de acceso	C,I,D	A.11.2.2
[A.7] Uso no previsto	D,C,I	A.8.2.1, A.8.2.2, A.8.2.3
[A.9] [Re-] encaminamiento de mensajes	C	A.10.8.1
[A.10] Alteración de secuencia	I	A.11.4.7
[A.11] Acceso no autorizado	C,I	A.9.2.1, A.10.7.4, A.11.3.1C, A.11.6.1, A.11.5.2, A.11.5.5, A.8.3.3
[A.13] Repudio	I	A.11.4.7, A.11.4.3, A.8.2.3

[A.15] Modificación deliberada de la información	I	A.12.2.2, A.8.2.3
[A.18] Destrucción de información	D	A.8.2.3, A.15.1.3
[A.19] Divulgación de información	C	A.10.7.3, A.11.5.5
[A.22] Manipulación de programas	C,I,D	A.12.4.1, A.12.4.3, A.12.5.3, A.13.1.1
[A.23] Manipulación de los equipos	C,D	A.11.5.5, A.13.1.1
[A.24] Denegación de servicio	D	A.13.1.1, A.14.1.3
[A.25] Robo	D,C	A.13.1.1
[A.26] Ataque destructive	D	A.13.1.1, A.13.2.1, A.14.1.3

GRUPO EQUIPOS

Tabla 16 Selección de controles del grupo equipos

AMENAZA / VULNERABILIDAD	RIESGO NO ACEPTABLE C, I O D	CONTROLES SELECCIONADOS
[N.1] Fuego	D	A.9.1.4, A.14.1.3
[N.2] Daños por agua	D	A.9.1.4, A.14.1.3
[N.*] Desastres naturales	D	A.9.1.4, A.14.1.3
[I.1] Fuego	D	A.9.1.4, A.14.1.3
[I.2] Daños por agua	D	A.9.1.4, A.14.1.3
[I.*] Desastres industriales	D	A.9.1.4, A.14.1.3
[I.3] Contaminación medioambiental	D	A.9.1.4, A.14.1.3
[I.5] Avería de origen físico o lógico	D	A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2
[I.6] Corte del suministro eléctrico	D	A.9.2.2, A.14.1.3
[I.7] Condiciones inadecuadas de temperatura o humedad	D	A.9.2.1
[I.8] Fallo de servicios de comunicaciones	D	A.13.1.1, A.14.1.3
[I.10] Degradación de los soportes de almacenamiento de la información.	D	A.10.5.1, A.13.1.2, A.15.1.3, A.10.7.2
[E.1] Errores de los usuarios	I,C,D	A.10.7.3, A.10.10.5
[E.2] Errores del administrador	D,I,C	A.10.10.4
[E.4] Errores de configuración	I	A.7.1.1, A.12.4.1, A,12,4,3
[E.8] Difusión de software dañino	D,I,C	A.10.4.1
[E.9] Errores de [re-]encaminamiento	C	A.11.4.7
[E.10] Errores de secuencia	I	A.10.8.1
[E.15] Alteración accidental de la información	I	A.10.10.5, A.13.1.1, A.8.1.1, A.8.2.2
[E.18] Destrucción de información	D	A.8.1.1, A.8.2.2, A.15.1.3, A.8.3.2, A.7.2.2
[E.19] Fugas de información	C	A.11.3.3, A.12.5.4
[E.20] Vulnerabilidades de los programas (software)	I,D,C	A.12.5.3
[E.21] Errores de mantenimiento / actualización de programas (software)	I,D	A.12.5.2, A.12.5.3
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	D	A.9.2.4,
[E.24] Caída del sistema por agotamiento de recursos	D	A.12.6.1
[E.25] Pérdida de equipos	D,C	A.13.1.1, A.8.1.1
[A.3] Manipulación de los registros de actividad	I	A.10.7.4

(log)		
[A.4] Manipulación de la configuración	I,C,A	A.10.7.3, A.14.1.3, A.10.5.1
[A.5] Suplantación de la identidad del usuario	C,A,I	A.11.3.1
[A.6] Abuso de privilegios de acceso	C,I,D	A.11.2.2
[A.7] Uso no previsto	D,C,I	A.8.2.1, A.8.2.2, A.8.2.3
[A.8] Difusión de software dañino	D,I,C	A.10.4.1
[A.9] [Re-] encaminamiento de mensajes	C	A.10.8.1
[A.10] Alteración de secuencia	I	A.11.4.7
[A.11] Acceso no autorizado	C,I	A.9.2.1, A.10.7.4, A.11.3.1, A.11.3.3, A.11.6.1, A.11.5.2, A.11.5.5, A.8.3.3
[A.12] Análisis de tráfico	C	A.10.6.1, A.10.6.2
[A.13] Repudio	I	A.11.4.7, A.11.4.3, A.8.2.3
[A.15] Modificación deliberada de la información	I	A.12.2.2, A.8.2.3
[A.18] Destrucción de información	D	A.8.2.3, A.8.3.2, A.15.1.3
[A.19] Divulgación de información	C	A.10.7.3, A.11.5.5
[A.22] Manipulación de programas	C,I,D	A.12.4.1, A.12.4.3, A.12.5.3, A.13.1.1
[A.23] Manipulación de los equipos	C,D	A.11.5.5, A.13.1.1
[A.24] Denegación de servicio	D	A.13.1.1, A.14.1.3
[A.25] Robo	D,C	A.13.1.1
[A.26] Ataque destructivo	D	A.13.1.1, A.14.1.3

GRUPO COMUNICACIONES

Tabla 17 Selección de controles del grupo comunicaciones

AMENAZA / VULNERABILIDAD	RIESGO NO ACEPTABLE C, I O D	CONTROLES SELECCIONADOS
[N.1] Fuego	D	A.9.1.4, A.14.1.3
[N.2] Daños por agua	D	A.9.1.4, A.14.1.3
[N.*] Desastres naturales	D	A.9.1.4, A.14.1.3
[I.1] Fuego	D	A.9.1.4, A.14.1.3
[I.2] Daños por agua	D	A.9.1.4, A.14.1.3
[I.*] Desastres industriales	D	A.9.1.4, A.14.1.3
[I.3] Contaminación medioambiental	D	A.9.1.4, A.14.1.3
[I.5] Avería de origen físico o lógico	D	A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2, A.9.2.3, A.10.5.1
[I.8] Fallo de servicios de comunicaciones	D	A.13.1.1, A.9.2.3
[E.2] Errores del administrador	D,I,C	A.10.10.4
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	D	A.9.2.4
[E.24] Caída del sistema por agotamiento de recursos	D	A.12.6.1
[A.7] Uso no previsto	D,C,I	A.8.2.1, A.8.2.2, A.8.2.3
[A.23] Manipulación de los equipos	C,D	A.13.1.1
[A.24] Denegación de servicio	D	A.13.1.1
[A.25] Robo	D,C	A.13.1.1
[A.26] Ataque destructivo	D	A.13.1.1, A.9.2.3

GRUPO ELEMENTOS AUXILIARES

Tabla 18 Selección de controles del grupo elementos auxiliares

AMENAZA / VULNERABILIDAD	RIESGO NO ACEPTABLE C, I O D	CONTROLES SELECCIONADOS
[N.1] Fuego	D	A.9.1.4
[N.2] Daños por agua	D	A.9.1.4
[N.*] Desastres naturales	D	A.9.1.4
[I.1] Fuego	D	A.9.1.4
[I.2] Daños por agua	D	A.9.1.4
[I.*] Desastres industriales	D	A.9.1.4
[I.3] Contaminación medioambiental	D	A.9.1.4
[I.5] Avería de origen físico o lógico	D	A.13.1.1, A.13.1.2, A.13.2.1, A.13.2.2, A.9.2.3
[I.6] Corte del suministro eléctrico	D	A.9.2.2, A.14.1.3
[I.7] Condiciones inadecuadas de temperatura o humedad	D	A.9.2.1
[I.9] Interrupción de otros servicios y suministros esenciales	D	A.14.1.3, A.8.1.1, A.9.2.4, A.13.2.1
[E.2] Errores del administrador del sistema / de la seguridad	D,I,C	A.10.10.4
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	D	A.9.2.4
[E.24] Caída del sistema por agotamiento de recursos.	D	A.12.6.1
[E.25] Pérdida de equipos	D,C	A.13.1.1
[A.6] Abuso de privilegios de acceso	C,I,D	A.11.2.2
[A.7] Uso no previsto	D,C,I	A.8.2.1, A.8.2.2, A.8.2.3
[A.11] Acceso no autorizado	C,I	A.9.2.1, A.11.3.1, A.11.6.1, A.11.5.2, A.8.3.3
[A.23] Manipulación de los equipos	C,D	A.13.1.1
[A.24] Denegación de servicio	D	A.13.1.1
[A.25] Robo	D,C	A.13.1.1
[A.26] Ataque destructivo	D	A.13.1.1, A.9.2.3

SERVICIOS SUBCONTRATADOS

Tabla 19 Selección de controles del grupo servicios subcontratados

AMENAZA / VULNERABILIDAD	RIESGO NO ACEPTABLE C, I O D	CONTROLES SELECCIONADOS
[I.8] Fallo de servicios de comunicaciones	D	A.13.1.1
[E.2] Errores del administrador	D,I,C	A.10.10.4
[E.9] Errores de [re-]encaminamiento	C	A.11.4.7, A.8.1.1
[E.10] Errores de secuencia	I	A.8.2.1
[E.15] Alteración accidental de la información	I	A.10.10.5, A.13.1.1, A.8.1.1, A.8.2.2
[E.18] Destrucción de información	D	A.8.1.1, A.8.2.2, A.15.1.3, A.8.3.2, A.7.2.2
[E.19] Fugas de información	C	A.12.5.4
[E.24] Caída del sistema por agotamiento de recursos	D	A.12.6.1

[A.5] Suplantación de la identidad del usuario	C,A,I	A.11.3.1
[A.6] Abuso de privilegios de acceso	C,I,D	A.11.2.2
[A.7] Uso no previsto	D,C,I	A.8.2.1, A.8.2.2, A.8.2.3
[A.9] [Re-] encaminamiento de mensajes	C	A.10.8.1
[A.10] Alteración de secuencia	I	A.14.1.3
[A.11] Acceso no autorizado	C,I	A.9.2.1, A.11.3.1, A.11.6.1, A.11.5.2
[A.12] Análisis de tráfico	C	A.11.4.6
[A.15] Modificación deliberada de la información	I	A.12.2.2, A.8.2.3
[A.18] Destrucción de información	D	A.8.1.1, A.8.1.3
[A.19] Divulgación de información	C	A.10.7.3
[A.24] Denegación de servicio	D	A.13.1.1, A.14.1.3
[A.26] Ataque destructivo	D	A.13.1.1, A.14.1.3

CAPÍTULO V

IMPLEMENTACIÓN DEL SISTEMA DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN (SGSI)

Como parte del proceso de implementación del sistema de gestión de seguridad de la información y por recomendación de la norma ISO/IEC 27001:2005 se redactan los documentos concernientes a la aplicación de los controles selección en el diseño del SGSI.

El documento más importante son las políticas de seguridad que sientan las bases de la seguridad en términos generales, seguido de las normativas y procedimientos que desarrollan mediante detalles más técnicos la forma de cumplir los objetivos citados en las políticas; finalmente todos los procedimientos, cambios y acciones en el SGSI quedarán registrados y documentados como evidencia del cumplimiento de los requerimientos de seguridad.

5.1 Antecedentes

La adecuada gestión de la información del Gobierno Provincial de Imbabura obedece al cumplimiento de los siguientes procesos, garantizando la confidencialidad, integridad y disponibilidad de la información en base a los requisitos de seguridad obtenidos hasta el momento y respetando las directrices de operación de la institución.

La política de seguridad de la información proporciona los principios por medio de los cuales se dirige todos los mecanismos concernientes con la implementación del SGSI. Ninguna normativa o procedimiento está sobre la política de seguridad de la información.

5.2. Procedimiento

Los criterios a seguir como referencia para la implementación, mantenimiento y mejora del Sistema de Gestión de Seguridad de la Información es la norma ISO/IEC 27001:2005.

Los procedimientos a desarrollarse deben respetar los principios de seguridad estipulados en la política de seguridad de la información, marcados en las siguientes clausulas:

- **Organización de la seguridad de la información:** Establece las bases que rigen la gestión de la seguridad de la información dentro y fuera de la institución, junto con los miembros responsables encargados de velar el fiel cumplimiento de las normas establecidas.
- **Gestión de activos de información:** Cubre la gestión de los activos de información mediante la identificación y clasificación de los activos junto con la responsabilidad y propiedad de los mismos. Del mismo modo abarca la identificación, evaluación y tratamiento de los riesgos relacionados con los activos de la información.
- **Seguridad del Recurso Humano:** Establece roles y responsabilidades de los empleados, contratistas y terceros acerca de la seguridad de la información que manejen ya sea antes, durante y después del ejercicio laboral.
- **Seguridad Física y Ambiental:** Asegura la protección física de las instalaciones, equipos y dispositivos auxiliares relacionados con la operación y funcionamiento del sistema.
- **Gestión de comunicaciones y operaciones:** Especifica los procedimientos operacionales para la protección de la información en su transporte, modificación y

almacenamiento tomando medidas de seguridad como antivirus, respaldo, almacenamiento, intercambio de información, gestión de redes entre otras.

- **Control de acceso:** Regula al usuario autenticado el acceso únicamente a los activos de información, redes, sistemas operativos, aplicaciones, internet, es decir los recursos a los que se le ha otorgado permisos.
- **Adquisición mantenimiento y desarrollo de sistemas de información:** Menciona los requisitos de seguridad necesarios en la adquisición, desarrollo y mantenimiento de los sistemas de información.
- **Gestión de incidentes y mejoras en la seguridad de la información:** Define los procedimientos a emprender para la generación, monitoreo y seguimiento que reflejen eventos de seguridad y debilidades de los sistemas.
- **Gestión de continuidad del negocio:** Establecer acciones y mecanismos a emprender que respondan rápida y eficientemente ante la materialización de un incidente de seguridad que atente contra la confidencialidad, integridad y disponibilidad de los sistemas de información solucionando los problemas suscitados y poniendo en marcha los sistemas afectados en el menor tiempo posible, permitiendo la continuidad de las actividades de la organización.
- **Cumplimiento:** Asegurar el cumplimiento de la política de seguridad de la información, requerimientos legales y regulatorios que la institución adopte para el aseguramiento de la información, así como los mecanismos de control y detección ante la violación de cualquiera de los principio estipulados en la política de seguridad de la información y las sanciones a emprender a quienes incumplan con los reglamentos y pongan en peligro la operación de los sistemas.

5.3 Documentos del SGSI

La implementación del SGSI corresponde al desarrollo de los documentos exigidos por la Norma ISO/IEC 27001:2005. En primera instancia la política de la seguridad dictamina los lineamientos a seguir para el desarrollo de los otros documentos los cuales implementan los controles seleccionados. El nivel de jerarquía viene dado de la siguiente manera.

- Política de la seguridad de la información
- Normativas y procedimientos de seguridad de la información.
- Estándares.
- Registros de seguridad

5.3.1 Política de seguridad de la información:

Establece los lineamientos generales, necesidades y requisitos de seguridad de la información como medidas a adoptar para mantener a salvo la información y los activos que lo procesan, transportan o almacenan para garantizar las actividades de negocio de la institución. La política de seguridad de la información del GPI se encuentra en la sección 5.3.

5.3.2 Las Normativas

También conocido como normas de seguridad se sustentan en la política de seguridad las cuales se concentran en un tema o área específica, implementando uno o varios controles semejantes. La normativa define las condiciones y los activos de información a proteger bajo escenarios concretos previamente definidos en la política de seguridad de la información. Las normativas desarrolladas como parte de la implementación de los controles seleccionados son los siguientes:

- Normativa de acuerdos con terceras partes
- Normativa de administración de incidentes de seguridad de la información

- Normativa de administración de seguridad de la red
- Normativa de buenas prácticas de seguridad de la información
- Normativa de control de acceso
- Normativa de control de cambios
- Normativa de gestión de continuidad del negocio
- Normativa de mantenimiento de equipos e instalaciones
- Normativa de protección contra software malicioso
- Normativa de requisitos de seguridad de la información para nuevas instalaciones y adquisición de software
- Normativa de roles y responsabilidades de seguridad de la información
- Normativa de segregación de funciones
- Normativa de seguridad de la información para la gestión del recurso humano
- Normativa de seguridad de la información
- Normativa de software licenciado
- Normativa de suministro eléctrico
- Normativa de uso de internet

El detalle de cada una de las normativas del SGSI del Gobierno Provincial de Imbabura se encuentra en el Anexo E.

5.3.3 Procedimientos

Son las acciones o actividades a realizar describiendo el procedimiento a ejecutar relacionado con la seguridad de la información y los funcionarios responsables de su vigilancia, actualización y cumplimiento. Los procedimientos desarrollados son los siguientes:

- Procedimiento de contacto con grupos de interés en materia de seguridad de la información
- Procedimiento de disposición de medios de almacenamiento y equipos de cómputo
- Procedimiento de generación y almacenamiento de backups
- Procedimiento de protección y revisión de registros de auditoria
- Procedimiento de seguridad física y ambiental del data center
- Procedimiento para la creación, modificación y eliminación de acceso de usuarios en sistemas
- Procedimiento para la identificación y clasificación de activos de información

El detalle de cada uno de los procedimientos del SGSI del Gobierno Provincial de Imbabura se encuentra en el Anexo F.

5.3.4 Estándares

Determina las acciones necesarias para completar el proceso de un procedimiento específico para ser considerado como estándar o común para todos los usuarios de un servicio, es decir debe ser el mismo esquema para todos. Para el desarrollo del presente proyecto SGSI se ha desarrollado dos estándares:

- Estándar de contraseñas para usuarios y administradores
- Estándar de etiquetado de activos de información

El detalle de los estándares de seguridad del SGSI del Gobierno Provincial de Imbabura se encuentra en el Anexo G.

5.3.5 Registros

Los registros son los documentos en donde se asienta por escrito un resumen de las actividades realizadas en el Sistema de Gestión de Seguridad de la Información, como la hora y fecha del trabajo realizado, los activos de información intervenidos, Personal a cargo de las tareas, eventos de seguridad, observaciones, entre otra información considerada importante con el objetivo de llevar un registro de las actividades en materia de seguridad de la información.

Es importante aclarar que todo documento del sistema de gestión de seguridad de la información debe ser redactado con lenguaje claro, sencillo de interpretar y no debe prestarse para confusiones. Los procedimientos son considerados pasos a seguir para ejecutar un proceso en base al cumplimiento de lo establecido en la política. El procedimiento al indicar las acciones a desarrollar no debe ser extenso pero si preciso.

5.3 Política de seguridad de la información del Gobierno Provincial de Imbabura

La información es el activo de mayor valor para una organización independientemente del medio electrónico o físico donde se transmita o encuentre almacenada, debe ser primordial la protección de dicha información y de los sistemas que la procesan de amenazas internas y externas, minimizando los daños y restableciendo las operaciones en el menor tiempo posible.

5.3.1 Objetivos:

Los objetivos globales que rigen la seguridad de la información son los siguientes:

- Controlar el adecuado uso de la información junto con la protección y gestión de los activos de información encargados del almacenamiento, transporte y procesamiento de la información garantizando su confidencialidad, integridad y disponibilidad.

- Asegurar el correcto funcionamiento de los servicios mediante la asignación de responsabilidades del mantenimiento y respuesta ante incidentes de seguridad.
- Establecer mecanismos para la identificación, evaluación y tratamiento de las amenazas y vulnerabilidades que pongan en riesgo la seguridad de la información.
- Modificaciones o actualizaciones del presente documento deben basarse conforme lo estipula la norma ISO/IEC 27001:2005.

5.3.2 Importancia

La importancia de implementar un sistema que garantice la seguridad de la información radica en la existencia de las más diversas amenazas que ponen en riesgo a los sistemas que procesan la información con el fin de lograr conseguir este recurso potenciando aún más el daño, perjudicando el normal funcionamiento de las actividades de la organización y afectando la imagen, prestigio y reputación del Gobierno Provincial de Imbabura ante la sociedad y autoridades gubernamentales nacionales.

5.3.3 Apoyo gerencial

Según lo acordado por la Contraloría General de Estado a través de su autoridad el Dr. Carlos Pólit Faggioni el 16 de noviembre de 2009 determina expedir las Normas de Control Interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos para que desarrollen, expidan y apliquen los controles internos que provean una seguridad razonable en salvaguarda de su patrimonio.

5.3.4 Evaluación del riesgo

La selección de los controles a ser implementados para proteger la información se basa en metodologías definidas de identificación, clasificación y dependencia de los activos involucrados con la manipulación de información, por medio de los cuales se investigan,

identifican y evalúan las amenazas y vulnerabilidades que pondrían en riesgo la disponibilidad de los sistemas y la confidencialidad e integridad de la información.

Los controles se obtienen de la norma ISO/IEC 27001:2005, norma internacional dedicada exclusivamente con la gestión de la seguridad de la información.

5.3.5 Principio de la política de seguridad de la información

La política de la seguridad de la información está orientada a ser un soporte en la correcta administración de los activos de información, controlar el acceso a los sistemas, aplicaciones y servicios, fomentar la seguridad en instalaciones y equipos, capacitar al personal interno, contratistas y terceros en temas de seguridad de la información, coordinación entre los propietarios y responsable de los activos para actuar frente a incidentes de seguridad y establecer el cumplimiento del SGSI concienciando que el incumplimiento de lo estipulado en la política de seguridad será objeto de sanciones conforme lo dictamine el reglamento interno.

5.3.6 Responsabilidades generales

La dirección de gestión de tecnologías de información y comunicaciones TIC´s del Gobierno Provincial de Imbabura conformará un comité de seguridad informático el cual será responsable del desarrollo, mantenimiento y actualización del SGSI.

El comité de seguridad informático nombrará a un responsable de la seguridad informática el cual velará por el cumplimiento de la seguridad de la información, el cumplimiento de la presente política, e impulsará todo lo relacionado con la seguridad de la información.

La autoridad del área de recursos humanos será la responsable de capacitar al personal que ingrese a la institución acerca de la política de seguridad de la información, las buenas

prácticas en la jornada laboral en materia de seguridad de la información, protección de equipos como las sanciones administrativas a las que está sujeto si incumple con las medidas adoptadas hasta el momento.

El responsable del departamento jurídico asesorará en materia legal a la institución sobre cambios en la legislación nacional acerca de la seguridad de la información, como también será un soporte en lo que necesite el comité de seguridad informático.

Todos los funcionarios del Gobierno Provincial de Imbabura poseen las siguientes responsabilidades generales acerca de la seguridad de la información:

- Respetar sus roles y funciones no abusando de los privilegios de acceso, deben utilizar adecuadamente los activos de información, proteger la información de modificaciones con mala intención así como la no divulgar información calificada como confidencial.
- Reportar los incidentes de seguridad detectados a lo largo de la jornada laboral a los miembros responsables del resguardo de la seguridad de la información.
- Todo el personal tiene la responsabilidad y obligación de conocer la política de seguridad de la información y aplicarla en todas las funciones diarias.
- El personal debe ejecutar sus acciones en base a la ética y la moral.

5.3.7 Alcance

La política de la seguridad de la información cubre lo siguiente:

- Es de cumplimiento obligatorio para todo el personal del Gobierno Provincial de Imbabura, junto con los contratistas y colaboradores sin importar su nivel jerárquico.
- La información al ser el activo más importante de la institución debe protegerse en todo momento desde la creación, procesamiento, transporte y eliminación sin importar en el medio físico o electrónico en el que se encuentre.

- La presente política abarca la gestión de la seguridad de la información en donde se concentra el procesamiento, almacenamiento y prestación de servicios como son los servidores en el data center.

5.3.8 Vigencia de la política de seguridad

El Sistema de Gestión de Seguridad de la Información está sujeto a la publicación de nuevas versiones cuando exista un proceso de implementación, modificación o actualización de nuevas aplicaciones o servicios, cambios en la infraestructura o equipos, y ante la ocurrencia de incidentes de seguridad que pongan en peligro la información, sus procesos y activos involucrados en el procesamiento, transporte o almacenamiento de la misma.

La política de seguridad junto con el SGSI debe evaluarse cada año por el comité de seguridad informático, si se considera necesario deberá actualizarse o cambiar conforme sucedan los eventos de seguridad o implementación de nuevos equipos, servicio y sistemas.

5.3.9 Sanciones

En base a la gravedad de la violación de la política de la seguridad de la información sea con mala intención o por desconocimiento será sancionada administrativa o penalmente de acuerdo a la legislación vigente.

5.3.10 Organización de la seguridad de la información

Los equipos informáticos así como la información son propiedad del Gobierno Provincial de Imbabura y por ende del Estado Ecuatoriano, debido aquello los funcionarios quienes posean dichos elementos son los responsables de protegerlos contra ataques sobre la disponibilidad e integridad de los mismos, como también de la confidencialidad de la información, siempre cumpliendo con lo estipulado en la política de seguridad de la información.

Los miembros responsables de los activos de información también serán conocidos como los propietarios de los activos, entendiéndose como propietarios los funcionarios responsables de su cuidado, más no de ser los dueños de los bienes.

Tanto los recursos y la información consideradas vitales tendrán un propietario que será el responsable de gestionar el activo y la seguridad en el marco de la política de seguridad de la información. Si el funcionario detecta alguna anomalía en el bien protegido deberá notificar la novedad al responsable de la seguridad informática para que establezca las acciones pertinentes.

La adquisición de nuevos recursos de procesamiento de la información deberán estar inclinados con los objetivos de la organización, calidad de servicio y ser aprobados por el responsable de cada área de la institución conjuntamente con el responsable de seguridad informático, justificando su propósito y uso. Del mismo modo en la adquisición de nuevos recursos deberá constar información técnica del producto, las garantías del proveedor y el personal de contacto con quien solicitar soporte o hacer efectivas las garantías.

Los funcionarios quienes tengan contacto o manipulen información clasificada como confidencial o secreta deberán suscribir un acuerdo con la institución y firmar un acuerdo de no divulgación de la información o también llamado acuerdo de confidencialidad.

Es obligación de todo el personal respetar las funciones por las cuales fueron contratados y deberán respetarse los permisos de acceso a los sistemas. Se establecerán mecanismos pare el control de accesos de los usuarios y administradores.

Si se violan los acuerdos de confidencialidad o se coloca en peligro la estabilidad de las operaciones de la institución mediante ataques intencionados, se entablará las sanciones

administrativas, civiles y/o penales conforme a la legislación interna y nacional vigente y de acuerdo a la magnitud del delito.

Si el funcionario habiendo detectado alguna alteración en el sistema que produzca un gran daño posterior en los activos de información y no proceda a notificar a tiempo, será sancionado administrativamente conforme lo dictamine el reglamento interno.

El responsable de seguridad informática y el propietario del activo deberán realizar un análisis de riesgos y vulnerabilidades del activo de información con el fin de establecer los controles necesarios a implementar para la protección de la información.

Cuando el acceso sea físicamente a los activos de información más importantes de la institución, se deberá cumplir a cabalidad con los controles de acceso, restricción y registro exigidos por la institución como parte del de la política de seguridad de la información.

5.3.11 Gestión de activos

Cada uno de los departamentos del Gobierno Provincial de Imbabura deberá elaborar un inventario de los activos asociados con el procesamiento de la información, en el que constarán detalles como el propietario del activo, características técnicas específicas y una descripción del bien.

El inventario de activos deberá ser actualizado cuando existan cambios en el personal, cambios en los equipos o después de cualquier incidente de seguridad.

Según la metodología de análisis y gestión de riegos de los sistemas de información (Magerit) el procedimiento a seguir para clasificar un activo es el siguiente:

- Identificar el tipo de activo de activo al que pertenece.

- Valorar en términos de las propiedades de la información como son la confidencialidad, integridad y disponibilidad en base a la importancia del activo o el nivel de daño ante la materialización de una amenaza.
- Un análisis de dependencia del activo, es decir cuáles son los activos de información a los que presta servicio y de acules depende para su funcionamiento.

5.3.12 Responsabilidad de los recursos humanos

Las funciones, permisos y responsabilidades en materia de seguridad de la información serán claramente definidos para cada uno de los puestos de trabajo en los términos y condiciones de empleo.

Los funcionarios deben cumplir con las responsabilidades generales (Sección 5.3.6), como también el cumplimiento de la presente política de seguridad y velar por la protección de cada uno de los activos de información que utilicen diariamente para sus actividades, o de los que son propietarios.

Establecer acuerdos de confidencialidad conforme se estipula en la sección 5.3.10 organización de la seguridad de la información. Tanto el funcionario como la institución deben respetar lo estipulado en los acuerdos de confidencialidad, evitando la divulgación, fuga o sustracción de la información.

Todos los funcionarios del GPI junto con los contratistas y terceros con acceso a información de la institución deberán ser capacitados en materia de política, normas y procedimientos organizacionales.

La capacitación en seguridad informática comprende las responsabilidades generales y legales, el uso correcto de las instalaciones y los equipos de procesamiento, almacenamiento y trasportación de la información y sobre todo concientizar que el

departamento de tecnologías de la información y comunicación realiza lo necesario en materia de seguridad de la información, pero sin embargo la seguridad total no existe y el punto más débil en la cadena de la seguridad es el error humano.

Del mismo modo el personal que ingrese a la institución será capacitado acerca de las obligaciones contraídas con la institución en materia de seguridad de la información, uso correcto de privilegios de acceso, acciones legales y procedimientos disciplinarios.

Oportunamente el personal deberá ser capacitado al existir nuevas actualizaciones o cambios realizados tanto en las normativas internas y la política de seguridad de la información.

La finalización de las relaciones laborales de un funcionario de la institución, contratista o tercero corresponde la entrega de los activos de información de los cuales ha utilizado o es propietario. Si los activos de información gestionados hasta el momento son críticos también se debe entregar las credenciales de acceso y se deberá proceder con el cambio o eliminación de la cuenta de usuario del funcionario saliente.

La información como documentos corporativos, equipos, software, manuales, tarjetas de acceso, e información almacenada en medios digitales deberá ser entregada al responsable del área de recursos humanos.

Ante cualquier violación a la política de seguridad, acuerdos de confidencialidad, ataques en contra de la disponibilidad de las operaciones de la institución, o modificación intencionales de la información con fines destructivos por parte del personal excluido de la organización, se establecerán las acciones legales correspondientes de acuerdo a las leyes vigentes en el país.

El cambio de puestos debe tratarse como la terminación de las relaciones laborales y el ingreso del funcionario al nuevo cargo con los requisitos de seguridad establecidos en el inciso.

5.3.13 Seguridad física y ambiental

Las áreas donde se ubiquen los activos de información más importante deberán ser protegidas mediante controles de acceso físicos recomendados por el responsable de la seguridad informático y el responsable del departamento de tecnologías de la información y comunicación, permitiendo el acceso sólo al personal autorizado.

Establecer los mecanismos necesarios de acceso a la información confidencial y a los medios de procesamiento de la información sólo al personal autorizado, registrando todos los accesos. Los visitantes a las áreas seguras deberán ser supervisados registrando la hora de entrada y salida. El acceso está permitido únicamente a los sitios y dispositivos autorizados previamente y se capacitará al visitante sobre procedimientos de emergencia y seguridad en el área.

Todo el personal en el interior del departamento de tecnologías de la información y comunicación debe llevar colocado en todo momento la credencial de identificación en un lugar visible de su vestimenta. Cualquier persona desconocida que no se encuentre acompañada de algún funcionario autorizado debe identificarse de alguna manera, de lo contrario deberá abandonar el sitio.

El acceso de terceros por cuestiones de soporte hacia áreas restringidas debe ser autorizado y controlado en tiempo y desarrollo de actividades. Las acciones desarrolladas por terceros deben ser aprobadas previamente y monitoreadas en todo momento.

El área física donde exista almacenamiento o procesamiento de la información como es el data center, debe ser protegido contra posibles daños producidos por desastres industriales como el fuego, inundaciones, desastres en la infraestructura, desastres producidos por el hombre, robo, y desastres naturales como fenómenos sísmicos, meteorológicos, entre otros.

El incremento de la seguridad en áreas protegidas se establece incluyendo controles para el personal y terceros como las citadas a continuación:

- Si las autoridades lo consideran necesario, dar a conocer al personal la ubicación del área protegida.
- Terceras personas no deben laborar sin supervisión.
- El personal se servicio de limpieza deberá tener acceso limitado a las áreas seguras o al data center. El acceso deberá ser autorizado y supervisado.
- Mantener cerrado el acceso físico al data center e inspeccionar periódicamente infraestructura y equipos.
- Se prohíbe el ingreso de equipos que registre información de video, audio, fotografía, computadoras portátiles u otros elementos similares sin la debida autorización del responsable de seguridad informática y el responsable de la dirección de gestión de tecnologías de información y comunicaciones.
- No se permite fumar, comer, beber o ingresar con animales al data center.

La ubicación de los equipos inherentes al procesamiento de la información deberán ser ubicados y protegidos contra amenazas ambientales y reducir la oportunidad de acceso no autorizado. La selección del lugar de los activos de información permitirá otorgar un control visual y supervisión en todo momento. De ser el caso se deberá separar los activos de

información de suma importancia a lugares mucho más seguros y establecer el nivel de seguridad requerida.

Establecer mecanismos contra variaciones de voltaje adoptando la protección necesaria ante anomalías o fallos eléctricos que afecten la disponibilidad de los equipos, suministrando el voltaje requerido de acuerdo a especificaciones técnicas de los equipos.

Equipos considerados esenciales para el correcto funcionamiento de las actividades de la institución deberán asegurar su operación con el continuo suministro de energía eléctrica adoptando los siguientes controles:

- No sobrecargar un punto de suministro de energía eléctrica, los funcionarios deben disponer de varios puntos de conexión para conectar los equipos.
- Adoptar sistemas de suministro de energía eléctrica continua (U.P.S) para evitar el cierre de los equipos informáticos como servidores u otros activos críticos, evitando alteraciones en las configuraciones, pérdidas de información o indisponibilidad de servicios.
- Si se desea brindar los servicios institucionales ininterrumpidamente, es necesario montar un generador de respaldo para el suministro de energía eléctrica cuando fallen los servicios públicos disponiendo del suficiente combustible. El mantenimiento del generador y su correcto funcionamiento deberán ser revisados periódicamente.

El cableado de energía y comunicaciones estarán protegidos contra interceptaciones o daños, ubicándolos en zonas no disponibles al público mediante la utilización de conductos o canaletas, separar líneas de energía eléctrica del cable de datos evitando interferencias, facilidad en la identificación del cableado de datos.

Asegurar la disponibilidad e integridad de los equipos mediante planes de mantenimiento preventivos y reparación de daños sólo del personal de mantenimiento autorizado, asegurando en primera instancia la información importante del equipo, documentar anomalías y respetar las condiciones para hacer efectivas las garantías del equipo.

Los dispositivos de almacenamiento de datos de equipos desatendidos o no utilizados deberán atravesar por un proceso de borrado o sobre escritura de los datos a fin de evitar fuga o sustracción vital de información hacia personas no autorizadas.

Cualquier equipo de procesamiento de la información no debe salir de las instalaciones de la institución a menos que sea autorizado por el responsable de seguridad informático y el propietario del activo. El funcionario encargado del bien informático será responsable de su cuidado y utilización de acuerdo a las especificaciones técnicas.

5.3.14 Gestión de las comunicaciones y operaciones

Se documentará y mantendrá actualizados los procedimientos relacionados con el procesamiento de la información respecto de los siguientes temas:

- Procedimiento a seguir ante un incidente de seguridad en la jornada laboral.
- Personal a contactar para soluciones técnicas u operativas.
- Recuperación de información al producirse fallas en el sistema.
- Procedimiento a seguir para modificar la configuración de servidores o dispositivos de red.
- Copias de respaldo de las configuraciones de los servidores y dispositivos de red y actualizar la información en caso de producirse cambios.

- Procedimientos ante la migración, mantenimiento o configuraciones de equipos sin afectar las operaciones de la institución.

La asignación de funciones y responsabilidades garantiza la adecuada segregación de funciones para controlar el mal uso intencional o accidental de los sistemas, permitiendo también la monitorización de los activos de información de accesos no autorizados o accesos no detectados.

La dirección de gestión de tecnologías de información y comunicaciones TIC´s revisará el dimensionamiento de la red y los sistemas de operación y gestionará proyectos de aumento de la capacidad para nuevos usuarios si es el caso. Del mismo modo se identificarán congestiones en los servicios o cuellos de botella e informarán a las autoridades correspondientes la amenaza y planificar una acción correctiva.

Ante la implementación de nuevos sistemas de información o actualizaciones se realizarán las pruebas correspondientes sobre el funcionamiento en los sistemas actuales y serán aprobados si el impacto de su desempeño no afecte a las computadoras o los sistemas de procesamiento de la información.

La dirección de gestión de tecnologías de información y comunicaciones TIC´s en conjunto con el responsable de seguridad informático establecerá los controles necesarios para la detección y eliminación del código malicioso.

Ningún funcionario puede instalar cualquier software si no está debidamente autorizado o realizado por el responsable de la seguridad informática.

El personal del departamento de TIC´s encargado del mantenimiento del software actualizar periódicamente el software antivirus de los equipos de los usuarios, como también

software utilitario y actualizaciones de sistemas operativos bajo ciertas restricciones citadas en la sección de mantenimiento de los sistemas de información.

Analizar archivos digitales provenientes de redes externas la presencia de virus o software malicioso antes de proceder a trabajar en el archivo sospechoso.

Capacitar al personal el uso correcto del software antivirus al analizar archivos digitales, dispositivos de almacenamiento masivo portátil, forma de operación del código malicioso, ataques a través del correo electrónico, entre otros.

El responsable de seguridad informático y los propietarios de la información determinarán la información o software importante para la institución y los detalles para el respaldo de la información como también el tiempo máximo de almacenamiento.

Se realizarán las pruebas concernientes con la restauración de la información al usuario origen, verificando que la información no esté modificada y completa.

Todo respaldo remoto de la información será registrado con detalles de fecha y tamaño del archivo. El lugar donde reposa las copias de seguridad debe estar protegido contra amenazas ambientales, humanas e industriales para asegurar su permanente disponibilidad, confidencialidad e integridad de la información y todos los controles concernientes a la protección de la información citada en este documento.

La dirección de gestión de tecnologías de información y comunicaciones TIC´s establecerá los controles necesarios en el aseguramiento de las comunicaciones con redes públicas, permitiendo así la disponibilidad de los servicios de red sin anomalías.

El acceso remoto a los equipos que así lo ameriten deberá ser realizarse mediante enlaces ssh, siendo los propietarios de los activos los responsables de su administración, por lo tanto se prohíbe la habilitación del servicio telnet o escritorio remoto vnc en los servidores.

Se debe poseer una copia de seguridad de la configuración de los dispositivos de red y servidores con el fin de restablecer los servicios en el menor tiempo posible.

El responsable de seguridad informática se encargará de eliminar totalmente la información que no sea útil para la institución en cualquier formato en que se encuentre, incluso de las copias de respaldo no importantes.

El procedimiento de eliminación de activos de información corresponde al responsable de seguridad de la información, asegurándose el borrado correcto de la información almacenada en el equipo, siendo registrado y documentado dicho proceso.

El uso del correo electrónico como medio de comunicación debe ser normado siguiendo los siguientes lineamientos:

- Protección de la información de modificaciones no autorizadas, accesos no permitidos, interceptación de la información, código malicioso en los mensajes.
- Almacenamiento de los mensajes para casos de repudio.
- Requisitos funcionales del uso del medio como tamaño máximo de la información almacenada en los buzones de entrada, salida y papelería, etc.
- Alcance del uso del correo electrónico sin usar el medio para cometer actos delictivos, de ser así la institución podrá auditar los mensajes de los servidores.

Es de vital importancia para la imagen y reputación de la institución que los servicios de libre acceso al público como páginas web y consulta de documentos electrónicos no sean vulnerables a modificaciones de la información o afecten la disponibilidad del servicio.

Antes de publicar nueva información o cambios en la configuración se debe realizar un análisis de riesgos y vulnerabilidades para asegurar la no vulnerabilidad del servicio y evitar el acceso al sistema, la configuración o la base de datos del servidor.

El administrador del sistema deberá registrar sus actividades con detalles como la actividad realizada, la causa de la intervención, fecha y hora.

5.3.15 Control de accesos

La política de control de accesos lógico y físico establece los siguientes lineamientos:

- Se identificarán los requisitos de seguridad de cada aplicación independientemente.
- Se asigna a cada usuario un identificador único para el respectivo control y seguimiento de acciones.
- No debe proveerse acceso a un funcionario hasta completar el procedimiento de autorización, de la misma manera se retira los derechos de acceso al tiempo que deja de poseer cualquier obligación laboral con la institución.
- Los responsables de recursos humanos y el director de cada área otorgarán el acceso a la información de cada empleado en base a sus funciones. Informarle de los privilegios de acceso, confidencialidad de la información y las sanciones por incumplimiento de la política de control de accesos. Asimismo los responsables de ambas áreas podrán retirar privilegios de accesos.
- Los usuarios deberán mantener en secreto las contraseñas personales evitando la divulgación de la clave a los compañeros o anotando en lugares visibles.
- Cambiar las contraseñas por defecto de los sistemas y equipos al empezar el uso de los dispositivos.
- A cada usuario se le otorgará una cuenta de correo electrónico, la cual cada funcionario deberá gestionarla conforme la política de seguridad de la información y la gestión de claves.
- El acceso físico al data center deberá ser sólo del personal autorizado mediante el uso de tarjetas magnéticas de control de acceso.

Las responsabilidades de los usuarios ante el resguardo de la seguridad de la información evitando el acceso a personas no autorizadas a los sistemas por medio de sus cuentas obedecen a respetar lo siguiente:

- Las contraseñas deben ser confidenciales y personales, evitando guardar en papeles, dispositivos de almacenamiento portátiles, teléfonos celulares o similares.
- Ante la sospecha de vulnerabilidad de la contraseña proceder a cambiarla como procedimiento ante un incidente de seguridad.
- Evitar el almacenamiento automático de las contraseñas en las aplicaciones.

En los escritorios de trabajo no deben reposar documentos impresos, dispositivos de almacenamiento portátiles, el escritorio de las computadoras no deben tener documentos.

Si el funcionario abandona temporalmente su puesto de trabajo deberá cerrar la sesión del computador antes de retirarse. Al finalizar la jornada laboral el funcionario apagará el equipo guardando previamente los documentos.

Los responsables de cada área autorizarán el acceso a las redes y servicios permitidos de cada funcionario mediante una solicitud formal al departamento de gestión de seguridad de la información TIC’s de la institución.

Las computadoras de los usuarios deberán conectarse al cableado horizontal en cada una de las áreas en las que trabaja, así mismo la identificación y el control lógico se establece asignando una dirección ip de acuerdo al departamento/vlan del área de trabajo.

Debido a la cantidad de usuarios del GPI se subdivide las redes en dominios lógicos separados por cada uno de los departamentos de la institución.

5.3.16 Adquisición, desarrollo y mantenimiento de los sistemas de información

La dirección de gestión de tecnologías de información y comunicaciones TIC´s será el encargado de regular la adquisición de software respetando los siguientes aspectos:

- La adquisición de nuevo software deberá ser justificado estableciendo las necesidades reales de los usuarios considerando las políticas públicas, caso contrario la máxima autoridad autorizará la adquisición en base a la justificación técnica.
- El nuevo software deberá adaptarse sin problemas a los equipos actuales del GPI, además se verificará si el nuevo software permite cumplir con lo establecido en la política de seguridad de la información.
- Al contratar a terceros el desarrollo del software se acordará los derechos de autor al gobierno provincial de Imbabura como los derechos de propiedad intelectual. La empresa contratada deberá entregar el código fuente junto con la documentación técnica.
- Las garantías por mantenimiento, soporte cambio o reparación del software adquirido debe estar definido como también información del personal de soporte a comunicarse para solicitar atención.
- Entre la documentación requerida del nuevo software debe constar manuales técnicos de instalación, configuración y de usuarios, los cuales serán difundidos a quienes utilicen el software.

Se debe archivar una copia de las versiones antiguas del software junto con información técnica, manuales de instalación, configuración y uso durante un tiempo como medida de precaución para contingencias.

Debe existir un conjunto de programas de computación permitidos en la instalación de los equipos de la institución como medida de control ante cambios en los sistemas por parte de los usuarios o terceros.

Controlar estrictamente el acceso al código fuente de los programas y documentación relacionada con el diseño y las especificaciones con el fin de evitar la eliminación de parte del código o modificación con nuevas funcionalidades.

Estar al tanto de nuevas actualizaciones, parches o vulnerabilidades del software como de los sistemas operativos por parte del fabricante. Antes de proceder a modificar el software de los usuarios se puede probar y validar el correcto funcionamiento de las aplicaciones.

La actualización del software debe ser restringida y estrictamente controlada, ante todo no se recomienda modificar los paquetes de software del fabricante, pero de ser el caso los cambios deben asegurar el perfecto funcionamiento de las aplicaciones y no poner en riesgo tanto la información como los activos de información.

Después del cambio o actualización del sistema operativo se debe revisar y probar si no han sido comprometidas las funcionalidades del software o la forma de operación y trabajo.

La información constituye un bien del gobierno provincial de Imbabura y por ende del estado ecuatoriano, por lo tanto se prohíbe sustraer la información clandestinamente por cualquier fin o medio. Como medida de control no está permitido utilizar canales cubiertos, software de monitoreo remoto, redes privadas virtuales, software troyano de extracción de información o similar.

Utilizar los medios necesarios en la identificación oportuna de las vulnerabilidades de los sistemas en especial de los servidores. Como requisito esencial se debe poseer el inventario de activos de información como medio para conocer lo que se desea proteger.

Identificar los riesgos asociados con las vulnerabilidades encontradas y establecer las acciones correctivas como la aplicación o no de parches de seguridad, actualizaciones software vulnerable u otros controles.

Si existe un parche de solución a la vulnerabilidad, se debe tratar los riegos inherentes con la implementación mediante pruebas controladas verificando la existencia de efectos secundarios o funcionamiento anómalo de la aplicación.

Por el contrario si no existe un parche disponible se recomienda las siguientes acciones preventivas a un desastre:

- Suspender los servicios vulnerables temporalmente.
- Restringir los controles de acceso.
- Monitoreo específico en la detección y prevención de ataques.
- Solucionar las vulnerabilidades tomando en cuenta los procesos más críticos.
- Gestionar la vulnerabilidad con aplicaciones o procesos alternos con el fin de reducir el riesgo y el impacto en la organización.

5.3.17 Gestión de incidentes en la seguridad de información

Todos los funcionarios, contratistas y terceros tienen la responsabilidad de reportar cualquier evento en la seguridad de la información o debilidad sospechosa al tiempo de detección del incidente en la dirección de gestión de tecnologías de información y comunicaciones TIC´s cuya ubicación debe ser conocida por toda la organización.

La recepción del reporte debe ser documentada con detalles de la persona quien notifica, cargo desempeñado, los sistemas posiblemente afectados, hora del incidente, mensajes en pantalla u otros detalles relevantes.

Por ninguna circunstancia los individuos que detecten las fallas o los eventos de seguridad deben tratar de explotar las debilidades o intentar solucionar los problemas. Estas acciones serán interpretadas como mal uso de los sistemas y puede ocasionar daño severo a los servicios y sistemas acarreando responsabilidades legales.

Proveer una respuesta adecuada y a tiempo mediante un diagnóstico previo y determinar si se trata de un incidente aislado, mal funcionamiento, negligencia o mal uso de los activos. De ser así solucionar el problema, capacitar al funcionario sobre el adecuado uso de los recursos y realizar el seguimiento del punto de falla.

Como medida preventiva ante los incidentes y vulnerabilidades de la seguridad de la información deberá monitorearse los sistemas y las vulnerabilidades con el fin de detectar los incidentes de seguridad como intermitencia en los servicios, código malicioso, ataques de negación de servicio, mal usos de los sistemas, violación en la confidencialidad e integridad de la información.

Una vez solucionado los incidentes de seguridad es importante analizar las causas que produjeron dichos acontecimientos, analizando las causas, consecuencias y la forma de prepararse y evitar similares sucesos en el futuro sin olvidar actualizar la política del SGSI.

5.3.18 Gestión de continuidad de las operaciones de la dirección de gestión de tecnologías de información y comunicaciones TIC's

El comité de seguridad informático coordinará las acciones de administración de la continuidad de las operaciones de los activos de información ante interrupciones imprevistas considerando los siguientes requisitos:

- Identificación de los activos de información críticos en los cuales reposa o procesa la información y la operación de las actividades del GPI.
- Realizar un análisis de riesgos de los activos anteriormente identificados.
- Para cada activo de información determinar las vulnerabilidades que pondrían en peligro la información o los equipos.
- Comprender las dimensiones del impacto ante la interrupción de los servicios por cualquier causa.
- Solucionar las fallas encontradas hasta el momento.
- El plan de continuidad debe ser entendible para los funcionarios del GPI.
- Asegurar la protección del personal, las instalaciones de procesamiento de la información y los activos críticos de la información.
- Procedimientos de recuperación, respaldo y restauración de la información y las operaciones de negocio en un tiempo aceptable.
- Capacitación adecuada del personal en las acciones y procedimientos de emergencia aclarando las responsabilidades de los usuarios o propietarios de los bienes las responsabilidades con los bienes y la información que manejan.

Cada uno de los miembros involucrados en los planes de restauración de los servicios debe conocer las tareas y responsabilidades a ejecutar cuando exista un incidente de seguridad y se aplique el plan de contingencias.

Los planes de continuidad de negocio deben ser revisados regularmente y aprobados por el comité de seguridad informático como también cambios en el personal, el directorio, infraestructura, legislación, terceros, servicios y aplicaciones.

5.3.19 Cumplimiento de los requisitos legales

Los funcionarios del GPI, contratistas y terceros vinculados con el procesamiento de la información deben acatar las disposiciones estipuladas en la política de la seguridad de la información actuando respetando la ley, la institución y la moral.

La adquisición de software será adquirida respectando lo estipulado en la sección adquisición, desarrollo y mantenimiento de los sistemas de información del presente documento, sin embargo si el software es licenciado, será adquirido de manera lícita junto con la documentación técnica necesaria y respetando los requerimientos del fabricante, por lo tanto está prohibido el uso de software desconocido, craqueado o poco confiable.

Los derechos de propiedad intelectual debe ser un tema en las capacitaciones al personal del GPI como también la prohibición de instalar cualquier software sin autorización del responsable de la seguridad de la información.

Los miembros encargados del mantenimiento de los equipos informáticos administrarán los instaladores, drivers originales, manuales del software tanto para el proceso de mantenimiento de equipos y evidencia de la existencia de las licencias.

Todo bien informático incluido el software es de propiedad del GPI y por ende del Estado Ecuatoriano, por lo tanto está prohibido la instalación de los programas en equipos particulares o dispositivos ubicados fuera de las dependencias del GPI.

Registrar a los usuarios quienes utilicen el software con licencia para controlar el número máximo de conexiones o equipos usuarios.

Está totalmente prohibida la copia parcial o total de cualquier software o información del software, licencias, o información confidencial propiedad del GPI por cualquier medio si no está autorizado por la ley.

El personal que realiza algún procedimiento en los medios de procesamiento de la información deberán cumplir con sus roles y responsabilidades, registrando las actividades realizadas y entregando los datos al responsable de seguridad informático.

Proteger los registros de gestión, administración y configuración de los activos y servicios ante modificaciones o destrucción. El cuidado y almacenamiento de los registros debe asegurar su disponibilidad e integridad cuando sea necesario.

Se debe considerar respaldar los registros en medios distintos ya sea en documentos impresos o almacenados digitalmente mediante procedimientos de backup. Si el respaldo o almacenamiento es digital se debe establecer medidas de seguridad como contraseñas en al acceso o modificación del documento, encriptar el documento.

El comité de seguridad informático analizará si amerita o no almacenar los registros por un período largo de tiempo, caso contrario si los registros no aportan utilidad alguna a la institución el comité autorizará la destrucción de la información tanto digital como física.

En todos los procesos de seguridad de la información debe asegurar la privacidad de la información tanto del personal como de los usuarios, estableciendo controles de acceso, verificación de identidad con la cédula de identidad o credencial respectiva y no revelar información personal de ninguna persona a individuos desconocidos.

Todo uso no autorizado de los servicios de procesamiento de la información en base a roles y responsabilidades, será sancionado administrativamente. Si las acciones ilegales del funcionario por no respetar los procedimientos de seguridad de los sistemas ponen en peligro

la imagen, prestigio, los servicios, la integridad, confidencialidad o disponibilidad de la información, será sancionado administrativa y penalmente de acuerdo a la legislación vigente.

Los responsables de la seguridad de la información deben verificar constantemente el correcto cumplimiento de las normas de seguridad, si se detecta alguna irregularidad es necesario evaluar las causas, corregir el problema, capacitar al funcionario responsable y documentar el incidente para posteriores revisiones o actualizaciones de los procedimientos operativos.

5.4 Declaración de aplicabilidad

La declaración de aplicabilidad también conocida como SOA (Statement of applicability) por sus iniciales en inglés, es el reporte de los controles de la norma ISO/IEC 27001:2005 que se han adoptado para ser implementados en la institución, por el contrario aquellos controles que no se implementen se debe justificar la no aplicabilidad de los mismos. La declaración de aplicabilidad se localiza en el Anexo D.

CAPÍTULO VI

CONCLUSIONES Y RECOMENDACIONES

6.1 CONCLUSIONES

- La norma ISO IEC/27001:29005 no menciona ninguna metodología de análisis y gestión de riesgos, más bien recomienda al responsable del proceso escoger una metodología con la que más se relaciona y este acorde con las necesidades y características de los activos de información, por lo cual la norma se considera flexible en este aspecto.

- Uno de los procesos del análisis de riesgos de los activos de la información es la identificación de los activos más importantes, suponiendo la idea que si un activo de información importante falla el impacto en la institución sería grave, sin embargo dicha apreciación es falsa debido a que si un activo menor que presta servicios a otros de nivel superior falla, es daño sería igual o tal vez mayor, sin embargo la diferencia radica en la solución de cada activo, debido a que la implementación de los controles debe ser menor al valor del activo para que la solución sea viable.

- Si como resultado del análisis de riesgos y vulnerabilidades se detectan fallas en la seguridad se procede a mitigar, eliminar o transferir el riesgo, sin embargo al existir dificultades que permitan la implementación de las soluciones ya sea por falta de apoyo de la dirigencia, falta de recursos económicos, disputas políticas entre otras, la institución deberá asumir el riesgo y será responsable si el activo falla hasta encontrar una solución definitiva.

- Según la norma ISO/IEC 27001:2005 el SGSI puede ser aplicado a una parte de la institución aclarando que el área a intervenir debe tener alguna relación directa con el procesamiento, almacenamiento o transporte de información como es el data center.

- La política de seguridad de la información es el documento más importante en el que se basan la toma de decisiones y acciones a emprender en temas de seguridad, ninguna normativa interna o procedimiento está sobre la política y cualquier violación a la misma deberá ser sancionada conforme al reglamento interno considerando el análisis que si el daño es muy grave adoptar medidas civiles o penales.

- Los funcionarios debe respetar sus roles, responsabilidades y privilegios de acceso hacia los sistemas de información y no intentar sobrepasar los sistemas los límites de acceso asignados o poner en peligro la integridad de la información o los equipos con acciones ilegales o negligentes.

- Es importante definir un procedimiento para el reporte de incidentes de seguridad que sea fácil tanto para los usuarios que necesiten reportar los inconvenientes encontrados, como para los funcionarios del departamento de Tic´s encargados de solucionarlos en el que se asignen responsabilidades de operación dependiendo de los activos fallidos, acortando así los tiempos de respuesta.

- En el Ecuador existe un retraso respecto a los países vecinos en materia de justicia, al no existir una ley dedicada exclusivamente a los sistemas de información y comunicación, sin embargo al entrar en vigencia el nuevo código penal se reduce esta brecha, debido a que contiene varios artículos en los que se cita las acciones

consideradas como delitos que atenten contra los activos de los sistemas de información y comunicación.

- El actual código penal aunque no utiliza términos sofisticados relacionados con la seguridad informática para ser referenciados como delitos tales como ingeniería social, sniffing de paquetes, cracker de contraseñas, inyecciones SQL a bases de datos o secuestro de sesiones entre otros, utiliza palabras sencillas en la redacción de los artículos abarcando prácticamente toda clase de delitos informáticos.

6.2 RECOMENDACIONES

- La adecuada selección de los controles de seguridad depende directamente del correcto análisis de riesgos de los activos de información y de la identificación de todas las vulnerabilidades leves o graves de los servidores ya que son los medios en los que se basan las operaciones de la organización.

- La norma ISO/IEC 27001:2005 claramente establece realizar un monitoreo periódico del funcionamiento de las medidas adoptadas en favor de la seguridad de la información, y actualizar o realizar cambios en base de la experiencia o falencias encontradas hasta el momento de la revisión.

- Es importante documentar los procedimientos que apoyan la implementación del SGSI como una forma de conocimiento y consulta oportuna de la forma de proceder por parte de los funcionarios hacia los sistemas que utilizan.

- La designación a un funcionario como responsable de seguridad informática supone una gran responsabilidad y gran trabajo, por lo que se recomienda contratar el personal para este cargo el cual se dedicará a estas funcione la totalidad de la jornada laboral.

- Es recomendable capacitar y practicar las acciones a emprender en caso de suscitarse una contingencias por parte del personal designado con esta tarea, así al momento de actuar cada uno sabrá las responsabilidades asignadas y los procesos en los que tendrá que intervenir.

- La protección de la información debe ser compromiso de todos los funcionarios del Gobierno Provincial de Imbabura, cada colaborador debe tomar conciencia acerca del daño potencial si se pone en peligro la seguridad de la información al cometen actos con malicia, beneficio propio o negligencia. Motivar al personal a tomar la iniciativa y capacitase en temas de seguridad de la información o preguntar cualquier duda o conocimiento que necesite aclararse.

- El capacitar al personal en materia de seguridad de la información es vital debido a que la mayor parte de incidente de seguridad e infiltraciones a los sistemas es producto de errores en los funcionarios, confirmando la apreciación que el eslabón más débil en la cadena de la seguridad informática es el error humano.

REFERENCIAS BIBLIOGRÁFICAS

Acunetix. (Abril de 2013). *Cross Site Scripting*. Obtenido de http://www.acunetix.com/vulnerabilities/cross-site-scripting/

Acunetix. (26 de Abril de 2013). *Directory Listing and Information Disclosure*. Obtenido de http://www.acunetix.com/blog/web-security-zone/directory-listing-information-disclosure/

Ali, S., & Heriyanto, T. (2011). *BackTrack 4: Assuring Security by Penetration Testing.* Birmingham: Packt Publishing Ltd.

Anonimous España. (7 de Marzo de 2012). *DDoS clientes botnet empezar a integrar el exploit Killer Apache*. Obtenido de http://anonhispano.foroactivo.com/t85-ddos-clientes-botnet-empezar-a-integrar-el-exploit-killer-apache

Apache http server project. (2006). *Apache http server project*. Obtenido de http://httpd.apache.org/security/vulnerabilities_22.html

Arango Serna, J. C. (2010). *El Atacante Informático.*

Calles García, J. A., & González Pérez, P. (24 de Octubre de 2011). *La Biblia del Footprinting.* Obtenido de Flu Project: Flu Project.com

Council of Europe. (23 de Noviembre de 2001). *Convention on Cybercrime.* Obtenido de http://conventions.coe.int/Treaty/en/Treaties/Html/185.htm

Código Orgánico Integral Penal de 2014, Obtenido de

http://www.asambleanacional.gob.ec/system/files/document.pdf

Exposures Common Vulnerabilities. (2008). Obtenido de http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2008-0005

Exposures Common Vulnerabilities and. (2006). Obtenido de http://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2006-5752

Golubchik, S. (Junio de 2012). *Security vulnerability in MySQL/MariaDB sql/password.c*. Obtenido de http://seclists.org/oss-sec/2012/q2/493

Gómez Fernández, L., & Andrés Álvarez, A. (2012). *Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes.* Madrid: AENOR.

González Rufino, M. E. (19 de Noviembre de 2002). *Departamento de Informática Universidad de Vigo.* Obtenido de Señales: Interrupciones software de Unix: http://trevinca.ei.uvigo.es/~nrufino/ep/Senales.doc

Graves, K. (2010). *CEH: Certified Ethical Hacker Study Guide.* Indianapolis: Wiley.

Hacktimes. (18 de Julio de 2005). *PHP - Configuración segura de PHP.INI*. Obtenido de http://www.hacktimes.com/php_-_configuraci_n_segura_de_php_ini/

Hernández Pliego, J. A. (2006). *Programa de Derecho Procesal Penal.* México: Porrúa.

ISO, & 27001, I. (2005). *Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos.*

López Betancourt, E. (2007). *Teoría del Delito.* México: Porrúa.

López Neira, A., & Ruiz Spoh, J. (14 de 10 de 2012). *El portal de ISO 27001 en Español*. Obtenido de http://www.iso27000.es/sgsi.html#section2a

National Vulnerability Database. (2007). *National Cyber Awareness System*. Obtenido de http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2007-3304

National Vulnerability Database. (2012). *National Cyber Awareness System*. Obtenido de http://web.nvd.nist.gov/view/vuln/detail?vulnId=CVE-2012-4000

Nieves, R. (2010). *Teoría del Delito y Práctica Penal – Reflexiones dogmáticas y mirada crítica.* Santo Domingo, D.N.: Editora Centenario, S. A.

OWASP, O. (Enero de 2013). *Cross-Site Request Forgery (CSRF)*. Obtenido de https://www.owasp.org/index.php/Cross-Site_Request_Forgery_%28CSRF%29

PHP security consortium. (2013). *PhpSecInfo Test Information*. Obtenido de http://phpsec.org/projects/phpsecinfo/tests/display_errors.html

Php.net. (3 de Mayo de 2013). *phpinfo*. Obtenido de http://php.net/manual/es/function.phpinfo.php

Pro Hack. (Mayo de 2013). *Most of Web Attacks*. Obtenido de http://www.theprohack.com/2008/05/most-of-web-attacks.html

Security Focus. (27 de Marzo de 2013). *Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability*. Obtenido de http://www.securityfocus.com/bid/51706/info

Sense of security. (2010). *Apache 2.2.14 mod_isapi Dangling Pointer*. Obtenido de http://www.senseofsecurity.com.au/advisories/SOS-10-002

The hacker news. (10 de Junio de 2012). *CVE-2012-2122 : Serious Mysql Authentication Bypass Vulnerability*. Obtenido de http://thehackernews.com/2012/06/cve-2012-2122-serious-mysql.html?m=1

The PHP Group. (Mayo de 2013). *Usando Register Globals*. Obtenido de http://php.net/manual/es/security.globals.php

Zapata, N. (14 de Mayo de 2012). Jefe de la Unidad de Investigación de delitos tecnológicos de la Policía Judicial del Ecuador. (http://www.interfutura.ec/blog/delitos-informaticos-en-ecuador-lo-que-vendria-en-la-nueva-legislacion/, Entrevistador)

ANEXOS