UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS

MAESTRÍA EN TELEMÁTICA,

MENCIÓN: CALIDAD EN EL SERVICIO

(Aprobado por: RPC-SO-19-No.300-2016-CES)

TRABAJO DE TITULACIÓN EN OPCIÓN AL GRADO DE MAGÍSTER

Título:
MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL SECTOR PÚBLICO *Explotación de vulnerabilidades y análisis brecha de implementación del Sistema de Gestión de Seguridad de la Información (SGSI) en un proceso estratégico.*
Autor:
Carlos David Rocha Cahueñas, Ing.
Tutor:
Ing. Pablo Recalde, MSc.

Quito – Ecuador

2019

CERTIFICADO DE RESPONSABILIDAD

Yo, Ing. Pablo Recalde, MSc. certifico que le Ing. Carlos David Rocha Cahueñas con C. C. № 172107884-6 realizó la presente tesis con título **MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL SECTOR PÚBLICO. Análisis de vulnerabilidades y brecha de implementación del Sistema de Gestión de Seguridad de la Información (SGSI),** y que es autor intelectual de la misma, que es original, auténtica y personal.

Quito, Febrero 2019

_____

Ing. Pablo Recalde, MSc.

CERTIFICADO DE AUTORÍA

El documento de tesis con título: **MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL SECTOR PÚBLICO. Análisis de vulnerabilidades y brecha de implementación del Sistema de Gestión de Seguridad de la Información (SGSI),** ha sido desarrollado por Ing. Carlos David Rocha Cahueñas con C. C. № 172107884-6 que posee los derechos de autoría y responsabilidad, restringiéndose la copia o utilización de la información de esta tesis sin previa autorización.

Ing. Carlos David Rocha Cahueñas

C. C. № 172107884-6

DEDICATORIA

A mi madre Esperanza (†) porque gracias a su forma de ser, me enseño valores de constancia y esfuerzo, haciendo en mi una persona de bien.

A mi padre y hermana, por confiar siempre en mí, convirtiéndose en mi soporte, brindándome su apoyo incondicional y siempre oportuno hasta culminar con éxito esta nueva de mi vida.

A mi esposa Juana Carolina, por su apoyo y comprensión que me brinda día a día para alcanzar nuevas metas y objetivos.

A mi familia, amigos y compañeros, por estar siempre presentes brindándome su respaldo, confianza y ánimo, hasta llegar a la meta propuesta.

A mi abuelito Alfonso (†) con mucho cariño y respeto.

AGRADECIMIENTO

Quiero agradecer a Dios por haberme dado la oportunidad de culminar una etapa más de estudios como este posgrado, al bendecirme con fortaleza, paciencia y sabiduría necesaria.

A mi familia y amigos parte fundamental en mi vida, quien me animaron brindándome apoyo moral para seguir y conseguir mi propósito trazado.

A mis profesores y compañeros con quienes compartí gratos momentos en el transcurso universitario. Mi eterna gratitud al PhD. Fidel Parra y MSc. Pablo Recalde por sus enseñanzas tanto en el campo académico como fuera de él.

RESUMEN

El desarrollo de un modelo de gestión de la seguridad de la información (SGSI) para las entidades del Sector Público basado en las normas NTE INEN-ISO/IEC 27000 permite dotar a las mismas de una herramienta de gestión para la seguridad de la información adaptable a sus objetivos estratégicos y requerimientos de seguridad, que permite garantizar su confidencialidad, integridad y disponibilidad, a través de un manejo adecuado de los riesgos a los cuales pueden estar expuestos los activos de información. La plataforma e-learning del Ministerio de Finanzas del Ecuador, al igual que todas las aplicaciones web está expuestas a amenazas e intrusiones. La presente investigación está basada en métricas simples, claras y objetivas, sobre vulnerabilidades del sistema y debilidades en la gestión de la seguridad de la información, con el fin de asegurar la selección de controles de seguridad, adecuados y proporcionados para procesos estratégicos riesgosos en el sector público, para que no sirvan de puerta para ataques informáticos de mayor envergadura y que protejan los activos de información de la Institución.

PALABRAS CLAVES: SGSI, proceso estratégico, pentesting, seguridad, ISO/IEC 27001

ABSTRACT

The development of an information security management model (ISMS) for public sector entities based on the NTE INEN-ISO / IEC 27000 standards allows them to provide a management tool for the security of adaptable information to its strategic objectives and security requirements, which allows guaranteeing its confidentiality, integrity and availability, through an adequate management of the risks to which the information assets may be exposed. The e-learning platform of the Ministry of Finance of Ecuador, like all web applications, is exposed to threats and intrusions. The present research is based on simple, clear and objective metrics, on system vulnerabilities and weaknesses in the management of information security, in order to ensure the selection of security controls, adequate and proportionate for risky strategic processes in the public sector, so that they do not serve as a gateway for larger computer attacks and that protect the information assets of the Institution.

KEYWORDS: ISMS, strategic process, pentesting, security, ISO / IEC 27001

ÍNDICE

CERTIFICADO DE RESPONSABILIDAD ..... **i**
CERTIFICADO DE AUTORÍA ..... **ii**
DEDICATORIA ..... **iii**
AGRADECIMIENTO ..... **iv**
RESUMEN ..... **v**
ABSTRACT ..... **vi**
ÍNDICE ..... **vii**
ÍNDICE DE TABLAS ..... **ix**
ÍNDICE DE FIGURAS ..... **x**
INTRODUCCIÓN **1**
PROBLEMA CIENTÍFICO 3
Delimitación del problema científico 3
a) Delimitación temporal 3
b) Delimitación espacial 3
c) Delimitación de contenido 3
Planteamiento del problema científico 4
Formulación del problema científico 5
OBJETIVOS DE LA INVESTIGACIÓN 5
Objetivo General 6
Objetivos Específicos 6
HIPÓTESIS 6
JUSTIFICACIÓN DE LA INVESTIGACIÓN 6
CAPÍTULO I. MARCO TEÓRICO **8**
1.1.- Ataques cibernéticos 8
a) Vulnerabilidad 9
1.2.- Ataques informáticos en Ecuador 11
1.3.- Gestión de Seguridad de la Información 12
1.4.- Metodología de Evaluación de Seguridad de la Información 13
a) Recopilación de Información 14
b) Objeto y Alcance de la Evaluación 14
c) Plan de la Evaluación 15
d) Establecimiento del Contexto 15
e) Análisis de Brecha de Seguridad de la Información 15

f) Proceso de Análisis 16
g) Proceso de Valoración y Evaluación 17
h) Procesos de Tratamiento 18
i) Emisión de Informes Finales: Brecha de Seguridad y Plan de Tratamiento de Riesgos 19
1.5.- Análisis de vulnerabilidades 19
a) Vulnerabilidad de la condición de carrera 20
b) Vulnerabilidad Cross Site Scripting (XSS) 20
c) Vulneración de denegación de servicio 21
d) Vulnerabilidad de ventanas de engañosas (Window ARP Spoofing) 21
1.6.- Software para análisis de vulnerabilidades 21
a) OWASP ZAP 21
1.7.- Pentesting o prueba de penetración o intrusión 22
a) Pentest de caja blanca 23
b) Pentest de caja negra 23
c) Pentest de caja gris 23
CAPÍTULO II. MARCO METODOLÓGICO 24
2.1.- Tipo de la investigación 24
2.2.- Unidad de análisis, población o muestra 24
2.3.- Técnica de recolección de datos 25
2.4.- Metodología del trabajo 26
CAPÍTULO III. RESULTADOS 28
3.1.- Identificación de la unidad de análisis 28
3.2.- Explotación de vulnerabilidades 29
3.3.- Análisis de brecha de implementación de SGSI 31
3.4.- Identificación de activos y valoración 35
3.5.- Análisis y valoración de riesgos 36
3.6.- Determinación de amenazas y vulnerabilidades 37
3.7.- Estado y aplicabilidad de controles ISO/IEC 27001 39
3.8.- Propuesta de modelo de gestión de seguridad de la información para procesos estratégicos 46
CONCLUSIONES 48
RECOMENDACIONES 50
BIBLIOGRAFÍA 52
ANEXOS 55

ÍNDICE DE TABLAS

Tabla 1.1. Clasificación de las Vulnerabilidades Según su Gravedad 10
Tabla 1.2. Escala de Cumplimiento..... 16
Tabla 2.1. Técnicas de recolección de datos por etapa de investigación y metodología 25
Tabla 2.2. Definición de la unidad de análisis y proceso 27
Tabla 3.1. Resumen de cursos y estudiantes. Ambiente de producción e-Learning 29
Tabla 3.2. Alertas según nivel de riesgo pentesting con OWASP ZAP..... 30
Tabla 3.3. Tipología de vulnerabilidades encontradas en aplicación Web 31
Tabla 3.4. Brecha de implementación de SGSI (I) 31
Tabla 3.5. Brecha de implementación de SGSI (II) 32
Tabla 3.6. Brecha de implementación de SGSI (III)..... 32
Tabla 3.7. Brecha de implementación de SGSI (IV)..... 33
Tabla 3.8. Brecha de implementación de SGSI (V) 33
Tabla 3.9. Brecha de implementación de SGSI (VI)..... 34
Tabla 3.10. Brecha de implementación de SGSI (VII) 34
Tabla 3.11. Identificación y valoración de activos según riesgo del CID de la información... 36
Tabla 3.12. Identificación y valoración de riesgos sobre activos..... 37
Tabla 3.13. Identificación de amenazas y vulnerabilidades por activos 38
Tabla 3.14. Aplicación controles ISO/IEC 27001-02 (I) 39
Tabla 3.15. Aplicación controles ISO/IEC 27001-02 (II)..... 40
Tabla 3.16. Aplicación controles ISO/IEC 27001-02 (III)..... 41
Tabla 3.17. Aplicación controles ISO/IEC 27001-02 (IV) 42
Tabla 3.18. Aplicación controles ISO/IEC 27001-02 (V)..... 43
Tabla 3.19. Aplicación controles ISO/IEC 27001-02 (VI) 44
Tabla 3.20. Aplicación controles ISO/IEC 27001-02 (VII)..... 46
Tabla 3.21. Esbozo de elementos constitutivos de modelo de gestión de seguridad de la información para procesos estratégicos del sector público 47

ÍNDICE DE FIGURAS

Figura 1.1. Riesgos en seguridad de aplicaciones 9
Figura 1.2. Tipo de vulnerabilidades 10
Figura 1.3. Las vulnerabilidades más comunes en las aplicaciones web 11
Figura 1.4. Tipo de ataques y sectores más vulnerables en Latinoamérica 12
Figura 1.5. Metodología de Evaluación de Seguridad de la Información 14
Figura 1.6. Matriz de Valoración Detallada de los Riesgos de Seguridad de la Información . 18
Figura 1.7. Top 10 OWASP 2017 22
Figura 2.1. Unidad de análisis 25
Figura 2.2. Metodología para análisis de vulnerabilidades 26
Figura 3.1. Aplicación Web e-Learning Ministerio de Finanzas 29
Figura 3.2. Prueba de penetración o intrusión con OWASP ZAP 30
Figura 3.3. Porcentaje de implementación de SGSI por actividad 35
Figura 3.4. Estado de aplicación porcentual de controles 45

INTRODUCCIÓN

Según la *Encuesta 2018 sobre tendencias de cyber-riesgos de seguridad de la información en Ecuador*, que toma información procedente el sector público, financiero, de consumo, telecomunicaciones y energía indica que 4 de cada 10 organizaciones sufrieron incidentes de seguridad en los últimos 24 meses y, el 70% de las organizaciones afirma no tener certeza de la efectividad de su proceso de respuesta ante incidentes de seguridad. El problema para la implementación de un proceso de seguridad ante ciberamenazas es el presupuesto, como consecuencia solamente una de cada diez organizaciones cuenta con un proceso de gobierno de seguridad para proteger sus activos frente a las ciberamenazas (Deloitte, 2018).

El problema es que con el pasar del tiempo, las organizaciones se van retrasando en la generación de procesos que permiten mitigar las amenazas cibernéticas, todo lo contrario para los atacantes. Para el sector público la implementación de un Sistema de Gestión de Seguridad Informática (SGSI), implica sobre todo garantizar la disponibilidad de los activos industriales y de infraestructura en los sectores estratégicos y por tanto la disponibilidad de los servicios públicos (ISOtools, 2016).

El Ministerio de Finanzas del Ecuador es la entidad rectora encargada de la política económica y financiera del Ecuador, administra plataformas transaccionales, aplicaciones web, y un sinnúmero de activos tecnológicos. La disponibilidad de la plataforma transaccional es de vital importancia para el aseguramiento de la disponibilidad de recursos para las entidades estatales. Administra aplicaciones Web, creadas por terceros o por su propio departamento de tecnología, que cumplen funciones específicas en el sistema de sostenimiento de la política económica del país.

En el presente trabajo se pretende realizar un análisis de las principales vulnerabilidades de la plataforma e-learning para formación permanente del talento humano y el análisis de la brecha de implementación del SGSI específicamente para aplicaciones web creadas por terceros, ajenos a la entidad. Para determinar el nivel de vulnerabilidad de la plataforma ante ataques que pudieran comprometer la disponibilidad, integridad y confidencialidad de la información, se realiza un *pentesting* de caja negra simulando el ataque de un hacker, con esto se extraerá el nivel de vulnerabilidad y riesgos a los que se expone la aplicación web, para

identificar la causalidad interna del riesgo debido a la brecha de implementación del SGSI. Se propondrá recomendaciones para mitigar las amenazas detectadas, con la finalidad de establecer un modelo de gestión de seguridad de la información para el sector público basado en la Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27000, principalmente con la aplicación de controles de seguridad de la norma NTE INEN-ISO/IEC 27002.

Un Modelo de Gestión de Seguridad de la Información para las entidades del sector público direcciona al conjunto de normas NTE INEN-ISO/IEC 27000 y de manera particular a la norma NTE INEN-ISO/IEC 27001 que proporciona un modelo para la creación, implementación, operación, supervisión, revisión, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información (SGSI).

De acuerdo a la Norma NTE INEN-ISO/IEC 27001 un Sistema de Gestión de Seguridad de la Información (SGSI) provee un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la protección de los activos de información, para alcanzar los objetivos del negocio basado en una evaluación del riesgo y los niveles de aceptación de riesgo de la organización diseñados para tratar y gestionar efectivamente los riesgos. El análisis de los requisitos para la protección de los activos de información y la aplicación de controles apropiados para asegurar la protección de estos activos de información, según sea requerido, contribuye a la implementación exitosa de un SGSI.

Los principios fundamentales que contribuyen a la implementación exitosa de un SGSI son los siguientes:

- Concientización de la necesidad de seguridad de la información.
- Asignación de responsabilidades para la seguridad de la información.
- Incorporación del compromiso de la dirección y de los intereses de las partes involucradas.
- Mejoramiento de los valores societarios.
- Evaluaciones de riesgos que determinan controles apropiados para alcanzar niveles aceptables de riesgo.
- Seguridad incorporada como un elemento esencial de las redes y sistemas de información.

- Prevención activa y detención de incidentes de seguridad de la información.
- Asegurar un enfoque completo de la gestión de seguridad de la información.
- Reevaluación continúa de la seguridad de la información y realización de modificaciones según se considere apropiado.

Un modelo de Gestión de Seguridad de la Información que se describe en esta norma anima a los usuarios a enfatizar la importancia de:

- Comprender los requisitos de seguridad de la información de una organización y la necesidad de establecer una política de seguridad de la información y sus objetivos.
- Implementar y operar los controles para administrar los riesgos de seguridad de la información de una organización en el marco de sus riesgos empresariales generales.
- Supervisar y revisar el rendimiento y la eficacia del SGSI.
- Asegurar la mejora continua sobre la base de la medición objetiva.

PROBLEMA CIENTÍFICO

Delimitación del problema científico

a) Delimitación temporal

Para esta investigación se considerarán los datos enmarcados en el período 2018-2019, considerando aquellos referentes a la Dirección de Tecnologías y Comunicación, la aplicación Web e-Learning, del Ministerio de Finanzas, de la ciudad de Quito.

b) Delimitación espacial

El proyecto de investigación propuesto se desarrollará en la ciudad de Quito, sobre la entidad Ministerio de Finanzas, Dirección de Tecnologías y Comunicación.

c) Delimitación de contenido

El proyecto planteado se encuadra en las normas exigidas por la Universidad Tecnológica Israel, sobre los trabajos de titulación, se sustentará a través de una revisión bibliográfica

de textos, que brindaran el marco de referencia teórico y conceptual. Para el diseño del piloto experimental y análisis de brecha de implementación la información se referirá al estudio de caso realizado, se basará en los estándares innovadores y normalizado por el Servicio Ecuatoriano de Normalización, específicamente la norma NTE INEN–ISO/IEC 27000, a fin de garantizar la Gestión de Seguridad de la Información para las entidades del sector público del Ecuador.

Planteamiento del problema científico

En la actualidad, existe un manejo masivo de recursos y datos dentro de las entidades del sector público, sin estar integrados a un modelo de Gestión de Seguridad de la Información (SGSI), lo cual atrae cada vez más a diferentes atacantes para lograr obtener información privilegiada conllevando perjuicios y convirtiéndose en riesgo eminente.

Existen organismos como OWASP, Deloitte o Kaspersky, que publican, cada año o regularmente, un análisis de los principales ataques que sufren las aplicaciones Web y las organizaciones en su infraestructura tecnológica. Según Deloitte, en su *Encuesta 2018* indica que de 10 organizaciones al menos 4 han sufrido incidentes de seguridad en los últimos 24 meses y el 70% de organizaciones no poseen procesos de respuesta ante incidentes y ciberseguridad. El incremento de las ciberamenazas supone un reto para las organizaciones en particular para el sector público debido a que deben garantizar la disponibilidad de los servicios públicos. Según ISOtools (2016), la aplicación de la norma 27001 en el ámbito público se ha centrado básicamente en la necesidad de preservar los activos industriales y de la infraestructura que son la base de la de los sectores estratégicos del funcionamiento de un país.

En los últimos años, los ataques a los sectores estratégicos de varios países han generado alertas significativas entre los diferentes gobiernos. De hecho, a partir del ataque ransomware WannaCry, que no fue dirigido específicamente hacia el sector público, sino que fue progresando a medida del contagio con otros sectores. Se evidenció grandes vulnerabilidades en los sistemas de informáticos públicos, que terminaron temporalmente apagados.

Luego de 34.200 intentos de infección en 97 países India, Estados Unidos y Rusia fueron los más afectados, los ataques fueron indiscriminados tanto para el sector público como para el

sector privado. Entre los afectados más representativos estuvieron la empresa Telefónica que brinda servicio de telecomunicación en España, el Servicio Nacional de Salud de Inglaterra y la empresa FedEx de entrega de paquetería en Estados Unidos (Kaspersky Lab, 2017).

El Ecuador no es ajeno a este fenómeno, según Kaspersky Lab (2017) empresa seguridad informática, al hacer un balance del ataque del ransomware señaló que WannaCry logró estar alrededor de 200 mil equipos en 150 países. En América Latina los más afectados fueron México, Brasil, Chile, Ecuador y Colombia.

La información representa un pilar fundamental dentro de cada organización por lo cual surge la necesidad de protegerla, sin importar el medio en el que se encuentre, por lo tanto es imprescindible que las entidades del sector público de Ecuador implementen, estrategias y controles para garantizar de forma permanente la protección de los datos.

La Seguridad de la Información busca establecer normas y políticas con la finalidad de mantener de confidencialidad, integridad y disponibilidad de la información (CID), puesto que la falta del cumplimiento de estos objetivos pondría a la organización en riesgo y por ende a su información.

Formulación del problema científico

¿Cómo contribuir a la protección de la información que generan las entidades del sector público con el fin de garantizar sus confidencialidad, integridad y disponibilidad, especificadamente en relación a los datos disponibles en plataformas e-Learning?

OBJETIVOS DE LA INVESTIGACIÓN

En la presente sección se detalle el objetivo general, que marca la meta hacia dónde se dirige el trabajo de investigación. También se han incluido objetivos específicos que determinan los pasos a seguir para la consecución de la meta final, para el caso de la investigación es la definición de un modelo de gestión de seguridad de la información para el sector público aplicado a procesos estratégicos.

Objetivo General

Establecer la necesidad de un modelo de Gestión de Seguridad de la Información para entidades del sector público ecuatoriano basado en las normas INEN NTE–ISO/IEC 27000 y en otras normas.

Objetivos Específicos

- Analizar las condiciones actuales para la Seguridad de la Información en las entidades del sector público de Ecuador.
- Establecer los elementos constitutivos para el modelo de Gestión de Seguridad de la Información.
- Realizar el análisis de brecha de la implementación del Esquema Gubernamental de Seguridad de la Información aplicando la metodología definida en el desarrollado para el sector público.
- Implementar un piloto de explotación de vulnerabilidades de aplicación Web.
- Esbozar un modelo de Gestión de Seguridad de la Información para el proceso estudiado en la entidad del sector público de Ecuador.
- Evaluar el modelo de Gestión de Seguridad de la Información actualmente vigente.

HIPÓTESIS

Con la aplicación de la metodología OWASP para análisis de vulnerabilidades informáticas, el análisis de brecha de implementación de SGSI y la aplicación de los controles de la norma NTE INEN–ISO/IEC 2700, se establece un proceso de reconfiguración del actual modelo de gestión de seguridad de la información, procurando la adecuada implementación de un SGSI para los diferentes procesos del sector público del Ecuador, para este caso de la plataforma e-Learning del Ministerio de Finanzas del Ecuador.

JUSTIFICACIÓN DE LA INVESTIGACIÓN

Actualmente la mayoría de entidades del sector público de Ecuador no tiene implementado un modelo de gestión para la seguridad de la información, sino solamente el

conjunto de controles basado en el Esquema Gubernamental de Seguridad de la Información expedido mediante Acuerdo Ministerial № 166 de la Secretaria Nacional de la Administración Pública, y publicado en el Registro Oficial Segundo Suplemento 88, del 25 de septiembre de 2013, que dispone a las Entidades de la Administración Pública Central, Institucional y que dependen de la Función Ejecutiva que dispone el uso obligatorio de las Normas Técnicas Ecuatorianas NTE INEN–ISO/IEC 27000 para la Gestión de Seguridad de las Información. (Pozo, 2013).

Según Ortega *et al* (2017), el desconocimiento, el mal uso, o la inexistente utilización de buenas prácticas para el desarrollo de aplicaciones web, hacen que este software específicamente sea susceptible de ataques informáticos.

Cada día, se desarrollan nuevos métodos que afectan la seguridad de la información de las organizaciones, de ahí la necesidad de contar con una estrategia completa de seguridad, seguir estándares y modelos de seguridad (Ortega, 2017).

Las Normas Técnicas Ecuatorianas NTE INEN–ISO/IEC 27000 establecen que la Gestión de Seguridad de la Información provee un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar la protección de los activos de información, para alcanzar los objetivos del negocio basado en una evaluación del riesgo y los niveles de aceptación del riesgo de la organización diseñados para tratar y gestionar efectivamente los riesgos. Sin embargo, debido a la brecha de implementación existente en las diferentes instituciones del sector público, es necesario establecer un modelo de gestión de seguridad de la información que extraiga los mejor de diferentes herramientas de seguridad informática.

En este contexto, es importante establecer el uso de estrategias, políticas, procedimientos, normas y estándares que garanticen la Seguridad de la Información, ya que con la ausencia de un modelo de Gestión de Seguridad de la Información, dificulta el cumplimiento de los objetivos de negocio de las entidades del sector público de Ecuador.

CAPÍTULO I. MARCO TEÓRICO

En el capítulo se desarrolla una contextualización teórica para abordar el proceso mismo de la investigación. Se presentan los elementos más relevantes teóricamente fundamentados a partir de la revisión bibliográfica de fuentes primarias y secundarias, que permiten entender los resultados generados por este trabajo de investigación.

Según Borbúa *et al* (2017), en el año 2020, la población mundial con acceso a Internet será de 5 mil millones (60% en línea), habrá 50 mil millones de dispositivos (10 representará más del 10% del producto interno bruto (PIB) mundial (Klimburg 2012, 33). Esto da cuenta de la sensibilidad de los ataques informáticos. Segú Pardo (2015), solamente al ingresar al intenet a cada minuto existen "20 víctimas de robo de identidad, 135 infecciones de Botnet y 180 nuevos malware en la red".

1.1.- Ataques cibernéticos

En la terminología de la norma ISO/IEC 27001, se entiende como ataque informático al *ciberataque*, este se refiere a los "intentos para destruir, exponer, alterar, inhabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo de información".

En la actualidad en existe en muchos riesgos que continuamente intentan atacar a los equipos informáticos, sistemas de información o de comunicación, que generan grandes pérdidas y daños a las organizaciones, todo esto debido a que no se cuentan con los controles de seguridad adecuados (Ortega, 2017).

Según Pardo (2015), los principales ataques se enfocan en la explotación de vulnerabilidades, de los eslabones más débiles de los sistemas informáticos y administrativos "como áreas administrativas, usuarios con cultura no adecuada de seguridad, proveedores, Outsourcing, terceros o firmas conexas". (Pardo, 2015)

Según Borbúa (2017), ItDigitalSecurity (2018), DealerWorld (2018), las aplicaciones web son la principal puerta de entrada para los ataques informáticos. De hecho 94% de las aplicaciones Web tienen vulnerabilidades críticas (ItDigitalSecurity, 2018). Las causas son

múltiples pero sobre todo se coincide en que el mal uso la inexistencia de buenas prácticas para el desarrollo explicaciones web hacen que estas sean et altamente vulnerables.

Como anota OWASP (2017), los atacantes utilizar las aplicaciones Web como rutas de acceso para atacar a la organización. En el siguiente gráfico, se observa las diferentes rutas que utilizan los atacantes para generar impactos al negocio de la organización.

Figura 1.1. Riesgos en seguridad de aplicaciones
Fuente: (OWASP, 2017)

a) Vulnerabilidad

La vulnerabilidad de la seguridad de los sistemas de información son una puerta abierta para los ataques informáticos, el potencial acceso no autorizado, abuso o fraude no se limitan a un solo lugar, sino que puede ocurrir en cualquier punto de acceso a la red. En el grafico a continuación, se pueden diferenciar tres tipos de vulnerabilidades según cómo afectan un sistema:

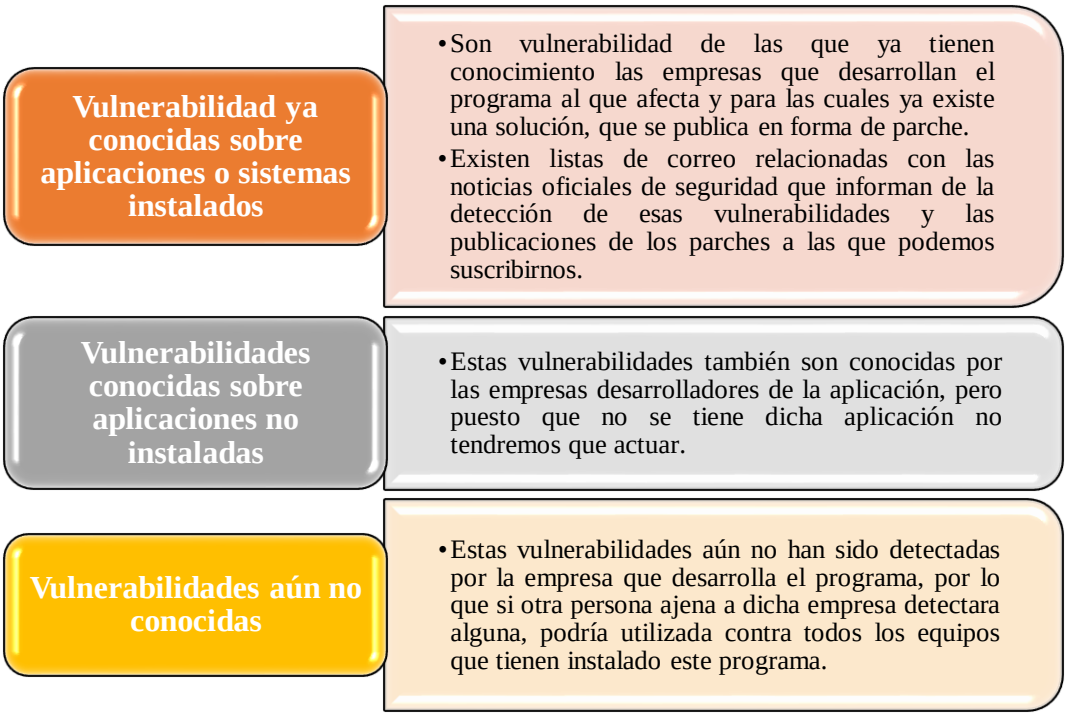

Figura 1.2. Tipo de vulnerabilidades

Tabla 1.1. Clasificación de las Vulnerabilidades Según su Gravedad

CLASIFICACIÓN	DEFINICIÓN
Crítica	Vulnerabilidad que puede permitir la propagación de un gusano de Internet sin la acción del usuario.
Importante	Vulnerabilidad que puede poner en peligro la confidencialidad, integridad o disponibilidad de los datos de los usuarios, o bien, la integridad o disponibilidad de los recursos de procesamiento.
Moderada	El impacto se puede reducir en gran medida a partir de factores como configuraciones predeterminadas, auditorías o la dificultad intrínseca en sacar partido a la vulnerabilidad.
Baja	Vulnerabilidad muy difícil de aprovechar o cuyo impacto es mínimo.

Otras vulnerabilidades son los equipos que no reciben el mantenimiento adecuado o que por fallas eléctricas suelen dañarse y dejar a la organización con menos recursos para realizar sus operaciones. Las organizaciones siempre estarán expuestas a estos tipos de riesgos o ataques informáticos.

Las principales vulnerabilidades que se encontraban las aplicaciones Web y que son consideradas debilidades que presente el sistema al momento de su desarrollo o en la aplicación de controles de seguridad son las siguientes: “la no validación de entrada de datos en las aplicaciones Web, como por ejemplo: inyecciones SQL, Cross Site Scripting (XSS),

inclusiones de ficheros locales (LFI) y remotos (RFI), Server SideIncludes (SSI)" (Ortega, 2017).

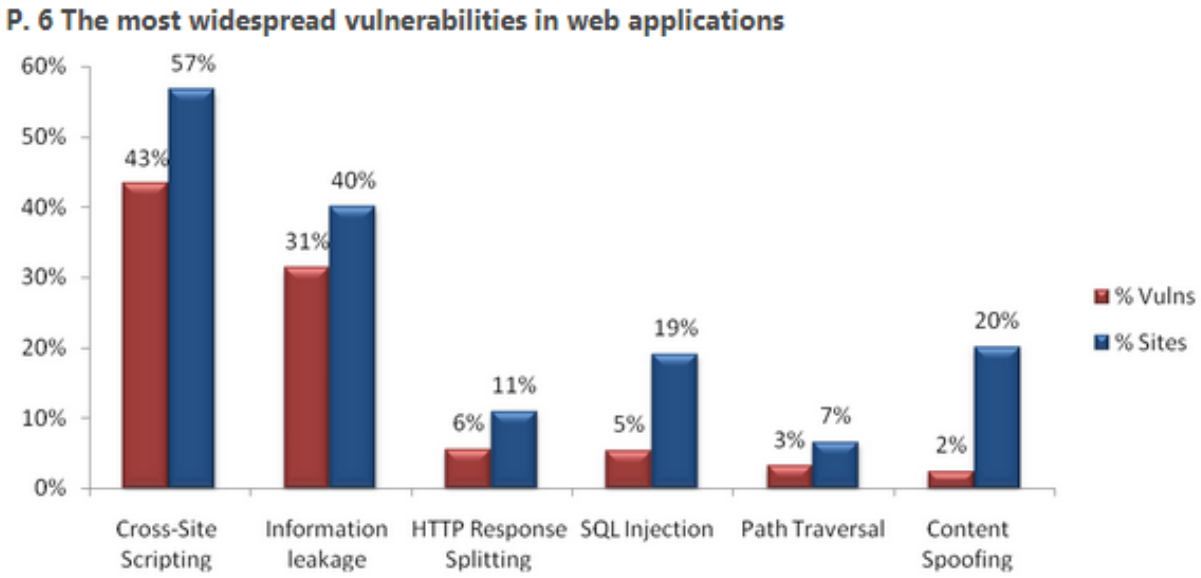

Figura 1.3. Las vulnerabilidades más comunes en las aplicaciones web
Fuente: (Ortega, 2017)

En el tráfico se puede observar de la vulnerabilidad nueva sede valiente en las aplicaciones Web es la Cross-Site Scripting, que se refiere a los diferentes tiempos de fuga de información a través de páginas a las que son de dirigidos los usuarios cuando ingresaba un sitio Web llenos cuales tienen que consignar diferentes datos. Por otro lado, está la SQL Injection y Response Splitting HTTP. Estas vulnerabilidades se centran en explotar las debilidades encuentro el al rendimiento en el software que permiten al atacante robar datos existentes asientos de incluso con las claves de desesperación de las bases de datos. Estos ataques permiten la revelación de los datos de sistemas de su subo de datos de la empresa organización y usuarios (Ortega, 2017).

1.2.- Ataques informáticos en Ecuador

Según Pardo el (2015), del informe de realizado para Digiware, los principales métodos de ataque a la seguridad informática son los métodos de infiltración de código intruso, es una vulnerabilidad que se presenta en aplicaciones para realizar consultas a bases de datos. El

principal país que realiza ataques informáticos de la región es Colombia "seguido de Argentina, Perú, México y Chile".

Por otro lado, el país que más ataques SQL Injection realiza es Ecuador. El informe indica que el sector más vulnerable frente a ataques informáticos es el de gobierno con un 49.53%, seguido por el sector financiero con 14.34%, comunicaciones con el 12.83%, industria con un 10.70% y energía con el 6.54% (Pardo, 2015).

Figura 1.4. Tipo de ataques y sectores más vulnerables en Latinoamérica
Fuente: (Pardo, 2015)

1.3.- Gestión de Seguridad de la Información

La gestión de seguridad de la información es un proceso que las organizaciones deben llevar con respecto a las amenazas que puedan existir contra sus activos de información y que se puedan materializar como riesgos de consideración (Solarte F. N., 2015).

La única manera de manejar un porcentaje mayor de las medidas de seguridad será establecer los procesos de seguridad y determinar las responsabilidades, esto sería un enfoque basado en procesos dentro de los estándares de gestión según la norma ISO 27001 (Sánchez Solá, 2013).

“Las organizaciones internacionales no se han quedado atrás. También se han esforzado de dotar con modelos o estrategias para la afrontar las amenazas de ciberdefensa y ciberseguridad a los Estados. Han publicado varios documentos o estándares, como la Guía de la ciberseguridad para los países en desarrollo (ITU 2007) o el National Cybersecurity Strategy Guide (ITU 2011). Ambos son modelos de referencia basados en la valoración de activos, capacidades, necesidades, amenazas y riesgos en sectores públicos y privados del Estado para construir y ejecutar una estrategia de ciberseguridad nacional. No podemos dejar de hablar de entidades de estandarización como la Organización Internacional de Normalización (ISO) 6 , que con sus Sistemas de Gestión de Seguridad de la Información (SGSI) contenidas en la ISO/IEC 27000, Tecnologías para la seguridad de la Información y Técnicas de Seguridad pretende dar una propuesta más orientada a los aspectos específicos de seguridad en una entidad u organización (ISO 2012)” (Borbúa, 2017).

Los controles de aseguramiento de la información deben tener un enfoque muy claro para quien tiene la responsabilidad de sus funciones y que se debe hacer al momento de fallar. Los controles de seguridad de información no son sólo técnicas implementadas, también son controles que deben estar relacionados con la tecnología de la información (Suárez & Medina Iriarte, 2006).

Existen diferentes tipos de control, uno de ellos es la documentación de las organizaciones, la implementación de software, la formación de los funcionarios que vendrían siendo un control de recursos humanos. Construir un sistema de control de seguridad describe un conjunto de reglas, entre ellas quienes pueden ser los responsables de la seguridad y que controles pueden adoptar para proteger la información, la idea no es convertir la seguridad en algo inmanejable (Ángeles, 2010). Por lo que la Gestión de Seguridad de la Información es un conjunto de procesos relacionados entre sí que tienen el fin de prestar seguridad a los activos de las empresas.

1.4.- Metodología de Evaluación de Seguridad de la Información

Según Vallejo (2014), la metodología en la norma NTE INENE-ISO/IEC27000:2012 está conformada por un grupo de etapas a seguir para realizar la evaluación de seguridad de la

información. En el gráfico a continuación se ilustra la metodología de evaluación de seguridad de la información.

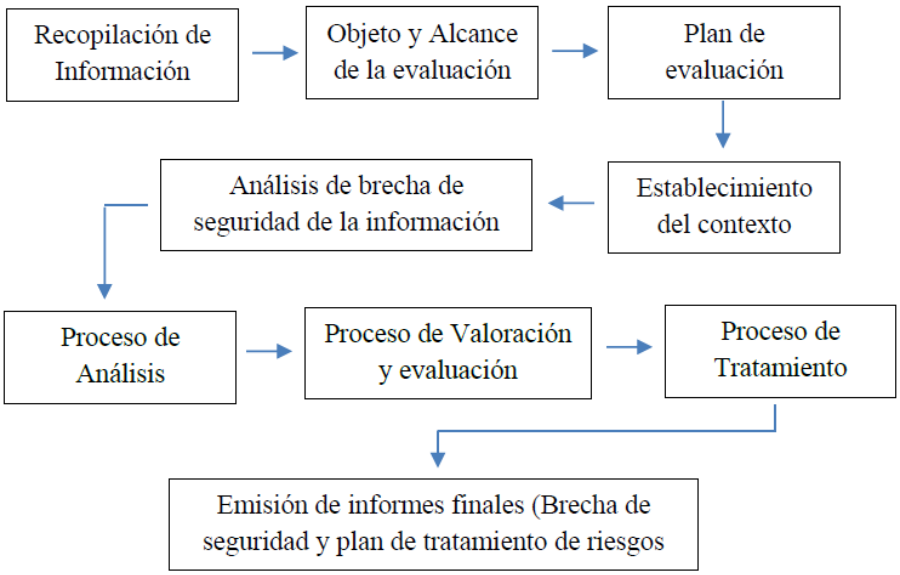

Figura 1.5. Metodología de Evaluación de Seguridad de la Información
Fuente: (Vallejo, 2014)

a) Recopilación de Información

Consiste en efectuar la observación inicial del medio, por ejemplo, entender su estructura, misión, visión, sus detalles y las relaciones funcionales de la organización. En esta etapa los evaluadores tendrán una aproximación general a la documentación, registros y recursos que se utilizan en la institución y sus procesos (Vallejo, 2014).

b) Objeto y Alcance de la Evaluación

En esta etapa se define cual será el objeto de estudio y alcance que conduce a la evaluación de seguridad de la información; y sobre el proceso de la organización, que se aplicará la evaluación. La determinación del alcance permite enfocar la evaluación de riesgos a las exigencias de la organización, con la finalidad de garantizar que todos los activos de información se tomen en cuenta durante la evaluación. Esta etapa debe ser aceptada por la dirección de la organización (Vallejo, 2014).

c) Plan de la Evaluación

En esta etapa se trata de evaluar la viabilidad para alcanzar los objetivos determinados en el proyecto, se enlistan las actividades para realizar en el marco de la evaluación; así como también se realizará la valoración de recursos y tiempos necesarios para la ejecución de cada actividad (Ángeles, 2010).

Se determina un plan de trabajo para la evaluación que contiene los procesos fijados se asigna un responsable de cada actividad. Este plan debe ser revisado y aprobado los usuarios por los usuarios del proceso evaluado (Ángeles, 2010).

d) Establecimiento del Contexto

Según Vallejo (2014, pág. 5), esta etapa consiste en establecer los criterios básicos determinados por la dirección de la organización:

- Criterios de evaluación del riesgo teniendo en cuenta el valor estratégico, criticidad de los activos, requisitos leales y reglamentarios, disponibilidad, confidencialidad e integridad y las expectativas de las partes interesadas.

- **Criterios de impacto:** Se especifica en términos del daño o costo para la organización causados por un evento adverso de seguridad de la información.

- **Criterios de aceptación del riesgo (apetito del riesgo):** Se especifica bajo qué criterios se aceptarán los riesgos, dependerán de las políticas, objetivos organizaciones y de las autoridades organizacionales.

e) Análisis de Brecha de Seguridad de la Información

Respecto del análisis de brecha en esta etapa a la sede determinada las deficiencias que pueden presentarse sobre los objetivos planteados para la seguridad de la información particularmente en esta etapa se tratan de evaluar el cumplimiento o de los requisitos de la norma ISO/IEC 27001:2005 y los controles del Anexo A. Se desarrolla a partir de un análisis cualitativo mediante la valoración de los ítems anotados (Vallejo, 2014).

Existe una tabla de cumplimiento de sistema de seguridad de la información a partir del análisis de brecha que a continuación se presenta.

Tabla 1.2. Escala de Cumplimiento

Nivel	Cumplimiento	Porcentaje
0	No está definido control	0%
1	No existen controles efectivos – Deficiencias considerables respecto a lo esperado	25%
2	Controles Básicos – Deficiencias menores con respecto a lo esperado para el requerimiento	50%
3	El requerimiento se cumple de manera efectiva	100%

Fuente: (Vallejo, 2014)

La estimación del nivel de cumplimiento se obtiene mediante el cálculo promedio de los valores de cada requisito.

f) Proceso de Análisis

En esta etapa se realiza un análisis de los posibles riesgos que pueden causar daños huasteca la organización este proceso de identificación está compuesto de las siguientes fases:

- **Identificación de riesgo:** En estará evaluar el potencial de riesgo según las pérdidas y daño puede causar se hace constar el cómo, dónde y por qué podría causar esta pérdida. Esta fase se compone de 4 actividades principales:

  - **Identificación de activos:** Este paso consiste en identificar a los activos más importantes que hacen parte del proceso que está haciendo evaluado que requiere el nivel de seguridad. En este apartado se definen los requerimientos a partir de la información detallada con los responsables de los procesos y de la valoración del siglo organización. Los activos son clasificados en la siguiente manera activos principales y activos de apoyo. Según Vallejo (2014), el listado de categorías de activos propuestos se basa en el anexo B de la norma NTE INEN-ISO/IEC 27005:2012.
  - **Identificación de amenazas:** En este apartado se identifican las amenazas que son potenciales fuentes del daño a los activos, tales como información, procesos y

sistemas. La metodología de identificación requiere que se realice una clasificación de ellas amenazas según el tipo, de manera que quedaría de la siguiente forma: Deliberada (D), Accidental (A) y Ambientales (E).

- **Identificación de controles:** Esta etapa comprender la revisión de la documentación y verificación con el personal responsable de los procesos, la existencia de controles capós por la organización (Vallejo, 2014).
- **Identificación de vulnerabilidades:** Esta fase del proceso de identificación y que anotar las vulnerabilidades pueden ser explotadas hubo las amenazas y causar daño a los activos. En este caso, Según Vallejo, por cada amenaza se determina la vulnerabilidad a nivel organizacional, en los procesos y procedimientos, gestión, personal, ambiente físico, configuraciones, hardware software e interacción con las partes externas.

g) Proceso de Valoración y Evaluación

Para el proceso de valoración y evaluación se requiere de la metodología de análisis que determinará el riesgo, establecida de forma cuantitativa y cualitativa combinado. Está compuesta de las siguientes etapas:

- **Valoración de los activos:** para valorar los activos se puede establecer diferentes técnicas y métodos, pero dependerá formalmente el tipo de activo el cual deforma cualitativa será asignado un valor de 0 a 4 según corresponda. Luego de la valoración función de la clasificación de información y de los de seguridad se procederá establece el Valor monetario de amortización del activo con la finalidad de reponerlo amante pérdida o daño.

- **Valoración de las consecuencias:** es este apartado supone determinar la consecución material de una amenaza en relación a los objetivos institucionales y los parámetros de seguridad de la información establecidos por la organización. Por cada activo se debe especificar el impacto en función de la pérdida de CID de la información. El valor del impacto se asigna en base a una escala cualitativa: Alto, Medio y Bajo.

- **Valoración de los incidentes:** Según Vallejo, respecto de la valoración de los incidentes en este paso se asignará valor a la facilidad de explotación de las vulnerabilidades y otro valor a la probabilidad de que una amenaza se materialice y afecte negativamente a las operaciones de la organización. El valor de un incidente se asigna en base a una escala cualitativa: Alto, Medio y Bajo.

- **Nivel de estimación:** La evaluación del riesgo se determina por el segundo método propuesto en el anexo E de la norma NTE INEN-ISO/IEC27005:2012, que indica realizar la valoración de los riesgos en función de la amenaza y vulnerabilidad (probabilidad) y del impacto (consecuencia) en la organización, como se anota en la siguiente figura:

	Probabilidad de ocurrencia -Amenazas	**L**			**M**			**H**		
	Facilidad de explotación vulnerabilidades	**L**	**M**	**H**	**L**	**M**	**H**	**L**	**M**	**H**
Impacto en el negocio	L	0	1	2	1	2	3	2	3	4
	M	1	2	3	2	3	4	3	4	5
	H	2	3	4	3	4	5	4	5	6

Figura 1.6. Matriz de Valoración Detallada de los Riesgos de Seguridad de la Información
Fuente: (Vallejo, 2014)

- **Evaluación del riesgo:** una vez realizadas todas las etapas anteriores se comparan los riesgos determinados con los parámetros devolución de riesgo que se definieron con anterioridad mediante el establecimiento del contexto. La evaluación del riesgo provee de la información necesaria para tomar decisiones sobre la seguridad de información.

h) Procesos de Tratamiento

En relación a la norma NTE INEN-ISO/IEC27005:2012, en esta etapa se realizan las acciones de reducir, retener, evitar o transferir el riesgo, por lo que se seleccionan controles y se proponen los más específicos y adecuados para el proceso de seguridad de la información; también se evalúa la necesidad de la implementación de otros controles adicionales. Así como, la posibilidad de retirar actividades o condiciones que modifican el desarrollo del proceso; y, por último, si es que no se puede evitar el riesgo compartir

con otras áreas de la organización. Los riesgos son priorizados en función del nivel de riesgo: Prioritario (5 y 6), Medio (3 y 4) y Bajo (0, 1 y 2) (Ángeles, 2010; Sánchez Solá, 2013).

A partir de la decisión de la organización sobre las posibilidades de tratamiento, se desarrolla el plan de tratamiento no valorado o valorado, esto dependerá del alcance de la evaluación realizada; en el primero se describen las acciones a realizar y los responsables, en el segundo se incluyen, los costos y tiempo requeridos para realizar dichas acciones (Vallejo, 2014).

i) Emisión de Informes Finales: Brecha de Seguridad y Plan de Tratamiento de Riesgos

En esta fase se procesan los informes finales: la brecha de seguridad y el plan de tratamiento. Cada informe final se entrega a la dirección de la organización, debe ser claro, conciso y ordenado, debe incluir recomendaciones fundamentales en las mejores prácticas y en el contexto de la evaluación (Vallejo, 2014).

1.5.- Análisis de vulnerabilidades

En la actualidad el uso de computadoras personales, dispositivos móviles y el acceso a la red son parte de la cotidianidad de las organizaciones o del colectivo de individuos, esto ha hecho que los procesos en empresas sean más eficientes; y, por tanto son incluidos ya en el quehacer regular de estas organizaciones. De igual forma a nivel individual el uso de las herramientas informáticas permite genera una serie de soluciones a los problemas y situaciones de la vida diaria.

A pesar de que, se identifican una serie de ventajas en el uso de herramientas informáticas ciertamente las desventajas también son visibles y tienen que ver principalmente con los ataques cibernéticos, en los cuales son blancos los diferentes dispositivos informáticos tanto para las organizaciones como para los individuos (Fernández, 2017).

Los ataques cibernéticos fundamentalmente se centran en la manipulación, acceso y robo de datos informáticos. Un análisis de vulnerabilidades trata de identificar las debilidades de la

seguridad informática, que aparecen como ventanas para la materialización de los ataques (Fernández, 2017).

Las vulnerabilidades o las debilidades que expresan un riesgo para los diferentes dispositivos informáticos pueden ser de origen interno y externo, esto quiere decir que pueden ser tanto en el hardware como en el sistema operativo y sus programas, es decir en el software (Tarazona, 2007).

Ahora, una vulnerabilidad se manifiesta como la debilidad de un instrumento informático, pero no necesariamente expresa la posibilidad de que se produzca una afectación. Por otro lado, cuando existe una amenaza es que evidentemente que hay un cierto potencial de daño al equipo y a los datos informáticos. Por último, el riesgo es la posibilidad de que la amenaza ocurra y el ataque al equipo se concrete (Solarte F. N., 2015).

Las principales vulnerabilidades que se pueden identificar en un equipo informático pueden ser sobre el diseño, debido a la debilidad de los protocolos utilizados para redes, sobre políticas de seguridad eficientes, respecto de implementación que tiene que ver con errores de programación, puertas traseras y errores no voluntarios del fabricante, una configuración errónea en sistemas informáticos, desconocimiento y descuidos de los usuarios, la disponibilidad de herramientas que facilitan ataques, limitaciones a las tecnologías de seguridad, entre otras (Solarte F. N., 2015):

a) Vulnerabilidad de la condición de carrera

Esta vulnerabilidad se presenta cuando múltiples procesos se encuentra en modo de ejecución y competición. Estos procesos al encontrarse en estado de competición no se encuentran sincronizados, por lo que al ejecutarse uno y otro a la vez quedan en modo de espera y ninguno se ejecuta definitivamente (Sánchez, 2016).

b) Vulnerabilidad Cross Site Scripting (XSS)

Es una de las vulnerabilidades más explotadas en cuanto al acceso sitio Web, se refiere a la inyección de códigos JavaScript o VBScript. Se produce una redirección a una Web

diferente, pero con las mismas características que la requerida por el usuario. Una vez ingresada las credenciales son enviadas al atacante normalmente se utiliza este tipo de vulnerabilidad para fraudes informáticos phishing y otros (Sánchez, 2016).

c) Vulneración de denegación de servicio

En este caso regularmente se envían paquetes IP pesados y formatos que ralentizan el funcionamiento de los equipos informáticos, para lograr una saturación. Además, por la respuesta del equipo se produce colapso de servicios (Solarte F. N., 2015).

d) Vulnerabilidad de ventanas de engañosas (Window ARP Spoofing)

Este tipo de ataque se realiza con la presencia de ventanas emergentes, cuyo objetivo es la sustracción de información del ordenador para redirigirlo al atacante (Sánchez, 2016).

1.6.- Software para análisis de vulnerabilidades

Los denominados *pentester* ejecutan escaneos al sistema objetivo, realizan un escaneo de puertos abiertos y luego ejecutan *Exploit* a manera de ataque para expresar las debilidades del equipo. Existen algunos programas que realizan este tipo de análisis como Nessus, OpenVAS u OWASP. Por general, los programas de análisis de vulnerabilidades presentan también recomendaciones para solucionar los riesgos potenciales y evitar las amenazas a los programas, dependiendo de la gravedad detectada de la vulnerabilidad (Pacheco, 2008).

a) OWASP ZAP

El proyecto OWASP se basa en información sobre riesgos que provienen de forma colaborativa de otras organizaciones especializadas en seguridad informática. Regularmente presentan una publicación top 10 sobre los riesgos y vulnerabilidades en aplicaciones Web. Según el top 10 de OWASP en el siguiente cuadro se presentan los riesgos y vulnerabilidades para aplicaciones web más regulares.

Figura 1.7. Top 10 OWASP 2017
Fuente: (OWASP Foundation, 2017)

Esta es una herramienta de identificación y análisis de vulnerabilidades creadas en el sistema Kali Linux, encuentra debilidades sobre todo en aplicaciones Web. Es un escáner seguridad de aplicaciones Web de código abierto. Esta herramienta multiplataforma escrita en el lenguaje de programación Java, puede utilizarse en Windows, Linux y Mac (Gomez Zafra, 2017).

1.7.- Pentesting o prueba de penetración o intrusión

Pentesting o es la abreviación de penetración y *testing*, que significa prueba de penetración, se refiere al ataque a diversos entornos con la intencionalidad de encontrar fallos, vulnerabilidades u otros, en un equipo o sistema informático. Su importancia se debe a infinidad de ataques de filtraciones que se van dando a las aplicaciones Web en los últimos tiempos (Astudillo, 2018). El *Pentesting* está construido para determinar y clasificar el alcance y la repercusión de las vulnerabilidades de seguridad, sobre los resultados que se obtienen se construyen presupuestos de riesgo y peligrosidad que tienen equipos o sistemas informáticos (Astudillo, 2018). Existen diferentes pruebas de intrusión que tienen diferente enfoque y eficiencia, los tipos de *pentest* que existen son los de caja blanca negra y gris (Astudillo, 2018).

a) Pentest de caja blanca

La prueba de caja blanca es el test de intrusión más completo, se centra en la evaluación de la infraestructura de la red, se realiza a partir de un hackeo ético, es decir a través de una explotación de vulnerabilidades con mayor precisión, debido a que el *pentester* cuenta con conocimiento de anterioridad acerca de topografía informática, contraseñas, *loggins* servidores, etc. (Astudillo, 2018).

b) Pentest de caja negra

Se realiza como un test de intrusión a ciegas, el principal fundamento de esta prueba es no poseer información anterior. Suele utilizarse para la explotación de vulnerabilidades cuando no se conoce los equipos y sistemas de informáticos a evaluar, tiene similitud con ataque externo de la ciberdelincuencia (Ramos, 2013).

c) Pentest de caja gris

Se define como una mezcla de las anteriores explotaciones de vulnerabilidades, es una prueba de intrusión en la que la información es baja, pero no completamente nula. Con esta prueba de intrusión lo que se busca es tratar de probar las vulnerabilidades específicas de un equipo o sistema (Ramos, 2013).

CAPÍTULO II. MARCO METODOLÓGICO

En el siguiente capítulo se establece la definición de la unidad de análisis u objeto de estudio, la metodología que se utilizará para el desarrollo de la investigación, así como las técnicas utilizadas para el trabajo. Por otro lado, se detallan las técnicas de recolección de la información.

2.1.- Tipo de la investigación

La investigación se define como un estudio de caso, debido a que el proceso de investigación trata sobre una organización y un proceso específico, analizado como una entidad Mertens (2005) citado en (Hernández, S. 2006), para la investigación se requerirá de la interacción de la metodología cuantitativa con la cualitativa, por lo que tendrá una metodología específica para el desarrollo de la investigación.

Por un lado, se trabajará con la metodología cuantitativa por medio del piloto experimental de explotación de vulnerabilidades, que se desarrolló aplicando herramientas de *pentesting* y para extraer los datos relevantes sobre vulnerabilidades en el proceso de formación continua a través de e-Learning del Ministerio de Finanzas.

Posteriormente se trabajó con la metodología cualitativa aplicando la entrevista los analistas de la dirección para establecer el análisis de brecha de implementación del SGSI. A la par se realizó revisión de documentos, a partir de un análisis de contenido para identificar los referidos a seguridad de informática.

2.2.- Unidad de análisis, población o muestra

Se puede definir de la siguiente manera, mediante el siguiente gráfico:

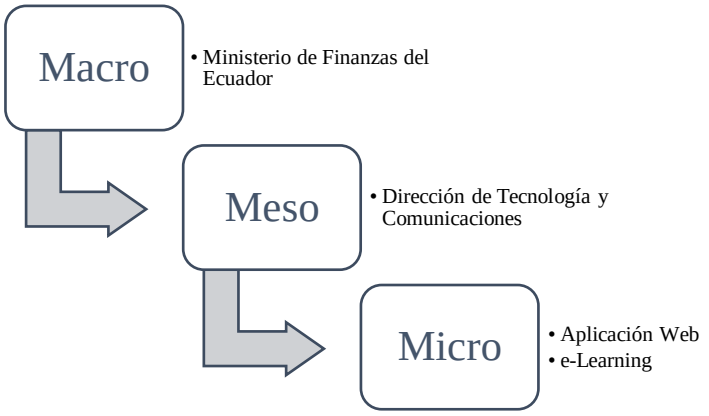

Figura 2.1. Unidad de análisis

2.3.- Técnica de recolección de datos

Según Hernández Sampieri (2016), la metodología que se aplica en el estudio de caso es una metodología mixta en la que se combinan las técnicas cuantitativas y cualitativas de recolección de información. Debido a la unidad de análisis de esta investigación se procedió a aplicar el estudio de caso. A lo largo de este trabajo se puede evidenciar la aplicación de técnicas de recolección de información de carácter cuantitativo como por ejemplo en el análisis de explotación de vulnerabilidades mediante una herramienta informática y por otro lado las técnicas cualitativas como la aplicación de matrices mediante chelis de entrevista realizadas a técnicos expertos en el área tecnológica de la dirección de tecnología comunicaciones del Ministerio de Finanzas.

En el siguiente gráfico se detallan las técnicas de recolección de datos por metodología aplicada:

Tabla 2.1. Técnicas de recolección de datos por etapa de investigación y metodología

Metodología	Etapa de investigación	Técnica de recolección de datos
Cuantitativa	Explotación de vulnerabilidades	Informe OWASP ZAP
Cualitativa	Brecha de implementación SGSI	Matriz de implementación Entrevista
Cualitativa	Identificación de riesgos, amenazas y vulnerabilidades	Matriz metodología ISO/IEC 27001
Cualitativa	Identificación de controles	Matriz metodología ISO/IEC 27001

2.4.- Metodología del trabajo

Para la investigación, se plantea la siguiente metodología, que se centra en la explotación de vulnerabilidades, análisis de brecha de implementación, identificación de activos, amenazas, riesgos, vulnerabilidades y controles.

Para esto se aplicó sobre la estructura de la plataforma e-learning las pruebas de intrusión, se logró involucrar a la compañía o institución para obtener la información requerida, a partir de reportes generados por los analistas de dirección tecnológica.

Se realizó un piloto experimental de explotación de vulnerabilidades mediante la herramienta OWASP ZAP para determinar la vulnerabilidad de la aplicación Web, de esa manera correlacionar con la metodología cualitativa de análisis de brecha de implementación del SGSI, y de aplicación de controles de la norma ISO 27001 para corroborar los niveles de riesgo en el que se encuentra la unidad estudiada.

El desarrollo de esta investigación se desarrollará de la siguiente forma:

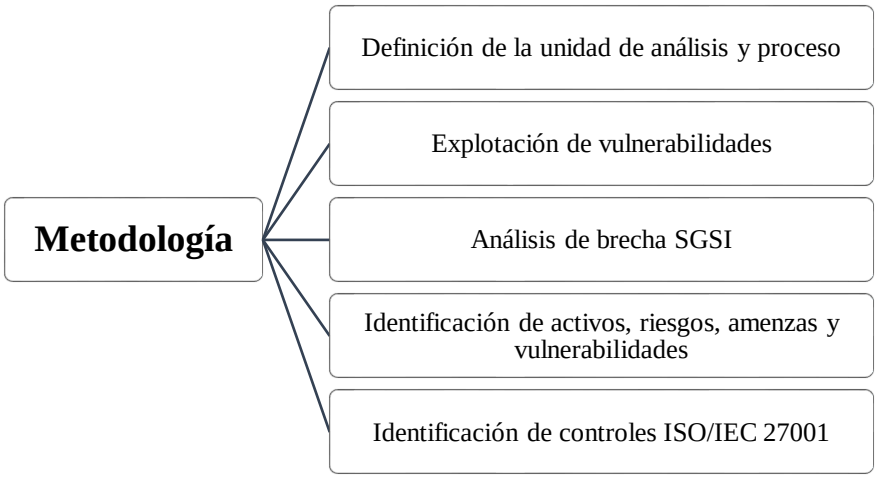

Figura 2.2. Metodología para análisis de vulnerabilidades

- **Definición de unidad de análisis**

Determinación de la unidad de análisis:

Tabla 2.2. Definición de la unidad de análisis y proceso

Unidad	**Dirección de Tecnología y Comunicaciones**
Proceso	Aplicación web: e-Learning

- **Explotación de vulnerabilidades**

  Se realizó mediante configuración de la máquina atacante Kali Linux desde el Internet hacia el ambiente de pruebas. En base a la guía web *application pentest* de OWASP se conoce el alcance y efectos que puede producir una vulnerabilidad, mediante la simulación de un ataque o hacking ético, se obtuvo reporte generado por herramienta OWASP ZAP, clasificado el nivel de alerta tipo: altas, medias y bajas.

- **Identificación de activos, riesgos, amenazas y vulnerabilidades**

  Para el proceso de identificación de activos riesgos, amenazas y vulnerabilidades se elaboraron matrices de información las mismas que siguen las recomendaciones que establece el sistema de seguridad de información basado en la metodología ISO/IEC 27001. La recopilación de la información se realizó con un analista de la Dirección de Tecnología y Comunicaciones del Ministerio.

- **Identificación de controles ISO/IEC 27001**

  Para la identificación de los controles ISO/IEC 27001, se procedió con la contrastación en una matriz, que se puede entender como declaración de aplicabilidad este documento, donde constan los controles seleccionados implementados y excluidos; así como, los procesos identificados, que deben ser mejorados, implementados y excluidos.

CAPÍTULO III. RESULTADOS

En la siguiente sección se presentan los hallazgos más relevantes que se identificaron luego de la aplicación de la metodología de investigación sobre la unidad de análisis. En este apartado se encontrará un análisis de los hallazgos a partir de la contextualización teórica que se realizó oportunamente en el marco teórico.

3.1.- Identificación de la unidad de análisis

El proceso estratégico que sirvió como unidad de análisis para esta investigación, se encuentra definido dentro de la estructura orgánica del Ministerio de Finanzas en la Dirección de Tecnología y Comunicaciones puntualmente se ha tomado la aplicación Web e-Learning, se realizó la identificación de los softwares que componen la aplicación y sus componentes físicos. Del software base de al aplicativo se tiene la utilización de Apache, PHP, MySQL y sus especificaciones técnicas son:

- Entorno Virtual de Aprendizaje (EVA) en el que se encuentra el repositorio virtual del contenido de las capacitaciones.

- Sistema de Gestión Académico (SGA) encargado de la administración de los participantes.

- Sistema de Gestión de Contenidos (SGC) que permite administrar los contenidos del sitio Web y publicar las nuevas ofertas de cursos tanto virtuales como presenciales disponibles.

- 170 cursos de capacitación virtual, con un total de 7953 estudiantes matriculados.

Tabla 3.1. Resumen de cursos y estudiantes. Ambiente de producción e-Learning

CURSO	№ cursos dictados	Total Matriculados EVA	Total Capacitados	Total Aprobados	Tasa de capacitación
Fundamentos de Base Legal	**40**	**2365**	**1753**	**1307**	**75%**
Gestión Operativa Financiera	**70**	**1959**	**978**	**802**	**82%**
Especialidad Contabilidad	**5**	**153**	**96**	**75**	**78%**
Especialidad Presupuesto	**13**	**390**	**317**	**243**	**77%**
Especialidad Tesorería	**10**	**303**	**232**	**158**	**68%**
Administración de Usuarios	**14**	**408**	**218**	**151**	**69%**
ESBYE	**5**	**150**	**109**	**90**	**83%**
SPRYN	**6**	**190**	**152**	**132**	**87%**
Avales, Certificaciones plurianuales y Contratos	**5**	**1503**			
Reclasificación automática de cuentas por pagar	**2**	**532**			
Total general	**170**	**7953**	**3855**	**2958**	**77%**

El aplicativo e-Learning, como proceso es el siguiente:

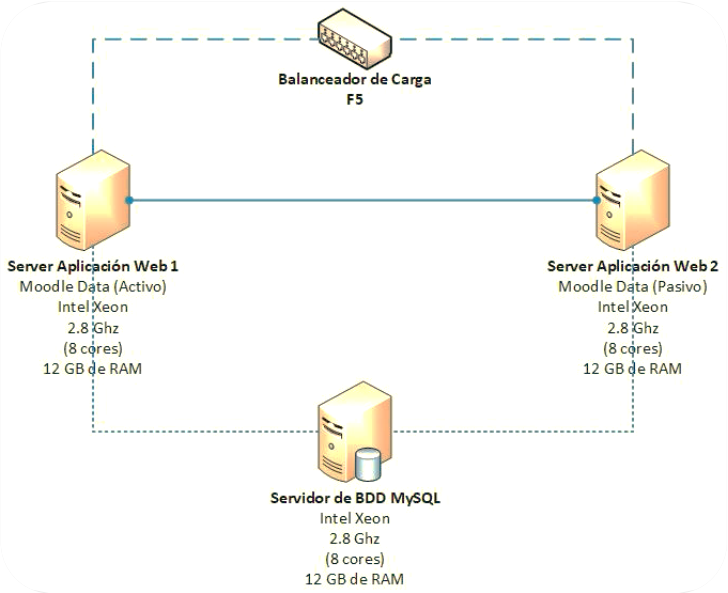

Figura 3.1. Aplicación Web e-Learning Ministerio de Finanzas

3.2.- Explotación de vulnerabilidades

La explotación de vulnerabilidades se realizó como un paso previo, para la determinación de la brecha de implementación del SGSI, para determinar cuantitativamente a través de una herramienta informática en el grado de vulnerabilidad al que está expuesto el proceso estratégico seleccionado.

Para realizar esta explotación de vulnerabilidades se realizó *pentesting* de caja negra, tratando de simular un ataque externo al proceso, a través de un *hacking* ético. Para esto se utilizó la herramienta OWASP ZAP, que realizó las pruebas de penetración o intrusión y generó un informe de resultados. Podemos ver en la figura 3.2 pantalla de arranque de la herramienta.

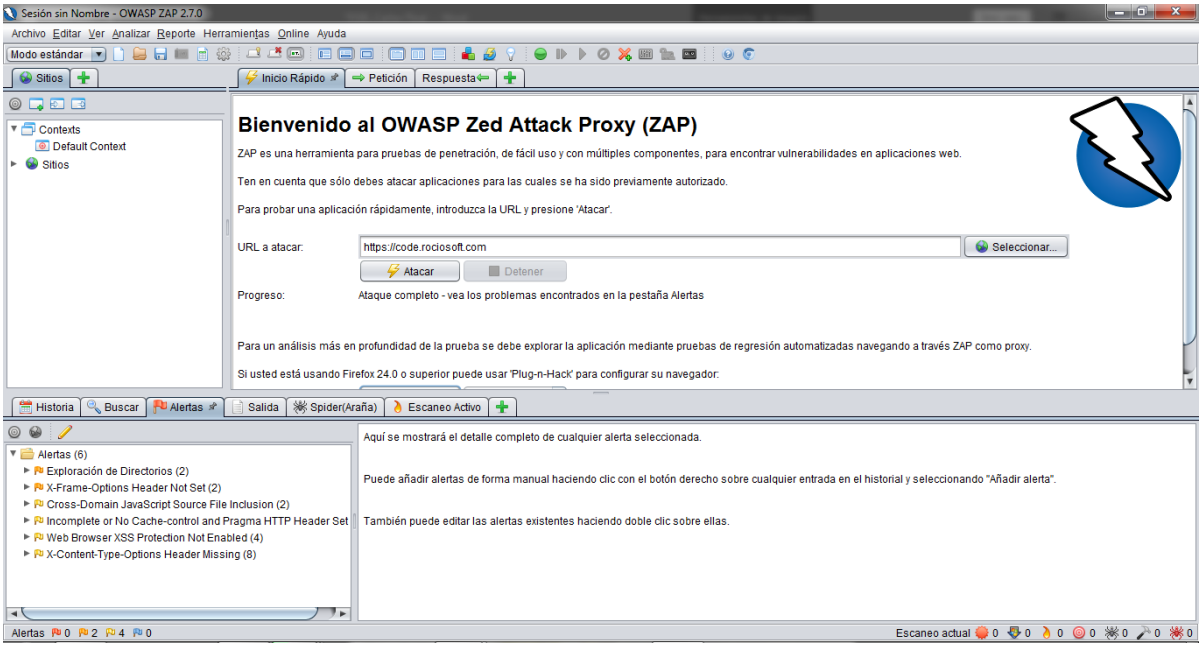

Figura 3.2. Prueba de penetración o intrusión con OWASP ZAP

Con la URL determinada para el ataque se procedió a generar una prueba de intrusión, a través de una máquina virtual soportada en Oracle Virtual Box con sistema operativo Kali Linux, con OWASP ZAP instalado, los resultados que se extrajeron del informe determinan que existen 9 vulnerabilidades clasificadas por nivel de riesgo. Como se observa en el gráfico No. el reporte de OWASP ZAP confirma los elementos abordados en la fundamentación teórica de este trabajo, la aplicación web es una ventana para ataques de alto riesgo a toda la estructura tecnológica del Ministerio de Finanzas.

Tabla 3.2. Alertas según nivel de riesgo pentesting con OWASP ZAP

Nivel de riesgo	Número de alertas
Alto	1
Medio	2
Bajo	6
Informacional	0

Con respecto a la identificación de las vulnerabilidades, con el análisis de resultados obtenidos del test de vulnerabilidades, a través del reporte generado por herramienta OWASP ZAP, las vulnerabilidades encontradas fueron:

Tabla 3.3. Tipología de vulnerabilidades encontradas en aplicación Web

Protocolo https utilizado con certificado SSL/TLS no válido
Cross Site Scripting reflejada
Xframe Header Not Set no establecida
Manipulación de parámetros por falta de manejo de excepciones
Incomplete or no cache-control and program http header set. No se ha configurado bien o correctamente el control de caché y encabezado http
Cookie no http only flay
Cookie without secure flay
Web browse XSS protection not enabled
Password autocomplete in browser

3.3.- Análisis de brecha de implementación de SGSI

Para establecer el estado de implementación del SGSI basado en ISO/IEC 27001, se tomó como herramienta de trabajo el workbook publicado por la página oficial de la norma ISO 27001. Respecto del contexto de la organización se puede observar que no existe determinado una política de seguridad de la información, que se adapte a las necesidades del proceso estratégico analizado.

Tabla 3.4. Brecha de implementación de SGSI (I)

4	**Contexto de la organización**	
4,1	**Comprensión de la organización y de su contexto**	
4,1	Determinar los objetivos del SGSI de la organización y cualquier problema que pueda afectar su eficacia	Definido
4,2	**Comprensión de las necesidades y expectativas de las partes interesadas**	
4.2 (a)	Identificar las partes interesadas incluyendo leyes aplicables, regulaciones, contratos, etc.	Definido
4.2 (b)	Determinar los requerimientos y oblicaciones relevantes de seguridad de la información	Definido
4,3	**Determinación del alcance del SGSI**	
4,3	Determinar y documentar el alcande del SGSI	Inexistente
4,4	**SGSI**	
4,4	Establecer, implementar, mantener y mejorar de forma continua el SGSI acorde al estandar	Inexistente

Fuente: En base al workbook www.iso27001security.com (2014)

En cuanto a liderazgo, referido al sistema de gestión de la seguridad de la información, se puede advertir que existe cierto compromiso con liderar un proceso de gobierno de seguridad de la información, documentar y asignar roles y responsabilidades en esa misión. Sin embargo, aún no han alcanzado los niveles de estructuración necesarios.

Tabla 3.5. Brecha de implementación de SGSI (II)

5	**Liderazgo**	
5,1	**Liderazgo y compromiso**	
5,1	La administración debe demostrart liderazgo y compromiso por el SGSI	Definido
5,2	**Política**	
5,2	Documentar la Política de Seguridad de la Informacion	Administrado
5,3	**Roles, responsabilidades y autoridades en la organización**	
5,3	Asignar y comunicar los roles y responsabilidades de seguridad de la información	Administrado

Fuente: En base al workbook www.iso27001security.com (2014)

Por otra parte, en cuanto a la planificación sobre las acciones que se deben tratar para mitigar los riesgos y explotar las oportunidades existe inicialmente una documentación sobre planes y objetivos de la seguridad de la información, así como si estos procedimientos que son propios de la formación de los analistas lo que hace necesario un sistema de gobernanza general.

Tabla 3.6. Brecha de implementación de SGSI (III)

6	**Planificación**	
6,1	**Acciones para tratar los riesgos y oportunidades**	
6.1.1	Diseñar el SGSI para satisfacer los requerimientos, tratando riesgos e identificando oportinidades	Definido
6.1.2	Definir e implementar un proceso de análisis de riesgos de seguridad de la información	Inexistente
6.1.3	Documentar e implementar un proceso de tratamiento de riesgos de seguridad de la información	Inexistente
6,2	**Objetivos de seguridad de la información y planificación para su consecución**	
6,2	Establecer y documentar los planes y objetivos de la seguridad de la información	Inicial

Fuente: En base al workbook www.iso27001security.com (2014)

Así mismo en cuanto al soporte referente a los recursos competencia y concienciación comunicación e información se encuentran todos en estado inicial y esto tiene que ver sobre todo porque luego de promulgado el acuerdo ministerial el estadio en el que se encuentra para

la implementación del esquema gubernamental de seguridad de la información es la identificación de los activos.

Tabla 3.7. Brecha de implementación de SGSI (IV)

7	Soporte	
7,1	**Recursos**	
7,1	Determinar y asignar los recursos necesaraios para el SGSI	Inicial
7,2	**Competencia**	
7,2	Determinar, documentar hacer disponibles las competencias necesarias	Definido
7,3	**Concienciación**	
7,3	Implementar un programa de concianciación de seguridad	Inicial
7,4	**Comunicación**	
7,4	Determinar la necesidades de comunicación internas y externas relacionadas al SGSI	Inicial
7,5	**Información documentada**	
7.5.1	Proveer documentacion requerida por el estandar más la requerida por la organización	Inicial
7.5.2	Proveer un titulo, autor, formato consistente, revisión y aprobacion a los documentos	Inicial
7.5.3	Mantener un control adecuado de la documentación	Inicial

Fuente: En base al workbook www.iso27001security.com (2014)

De la misma manera lo de ítems relacionados operación evaluación del desempeño y mejora estarán en el mismo punto de inicio.

Tabla 3.8. Brecha de implementación de SGSI (V)

8	Operación	
8,1	**Planificación y control operacional**	
8,1	Planificar, implementar, controlar y documentar el proceso de gestion de riesgos del SGSI (Tratamiento de riesgos)	Inicial
8,2	**Apreciación de los riesgos de seguridad de la información**	
8,2	Evaluar y documentar los riesgos de seguridad regularmente y cuando hay cambios	Inicial
8,3	**Tratamiento de los riesgos de seguridad de la información**	
8,3	Implementar un plan de tratamiento de riesgos y documentar los resultados	Inicial

Fuente: En base al workbook www.iso27001security.com (2014)

Tabla 3.9. Brecha de implementación de SGSI (VI)

9	Evaluación del desempeño	
9,1	**Seguimiento, medición, análisis y evaluación**	
9,1	Realizar un seguimiento, medición, análisis y evaluación del SGSI y los controles	Inicial
9,2	**Auditoría interna**	
9,2	Planificar y realizar una auditoria interna del SGSI	Inicial
9,3	**Revisión por la dirección**	
9,3	La administración realiza una revision periodica del SGSI	Inicial

Fuente: En base al workbook www.iso27001security.com (2014)

Tabla 3.10. Brecha de implementación de SGSI (VII)

10	Mejora	
10,1	**No conformidad y acciones correctivas**	
10,1	Identificar, arreglar y reaccionar ante no conformidades para evitar su recurrencia documentando todas las acciones	Administrado
10,2	**Mejora continua**	
10,2	Mejora continua del SGSI	Inexistente

Fuente: En base al workbook www.iso27001security.com (2014)

Como se observa en la figura 3.3, se puede entender que respecto al nivel de cumplimiento de la implementación hay difícil que es considerable respecto de la implementación de un sistema de gestión de la seguridad de la información no se llega a establecer el 50% de implementación en algunos casos lo que hace previsible entender que no cuenta la organización con controles básicos Y corrobora de alguna forma el nivel de vulnerabilidad frente a un ataque externo que ha sido demostrado con la prueba de intrusión con OWASP ZAP.

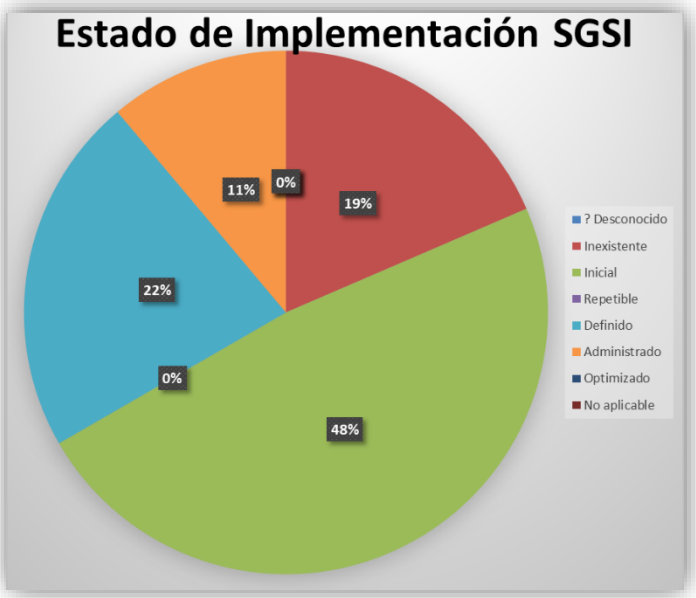

Figura 3.3. Porcentaje de implementación de SGSI por actividad

3.4.- Identificación de activos y valoración

En cuanto a la determinación de los activos y su valoración se ha realizado una tabla con la información provista por las revisiones de documentación, manuales de usuario, normativas y entrevista directa.

La tabla está dividida en dos partes, aquella que hace referencia a los activos intangibles como los activos de información, servicios informáticos, software de operación y por otro lado, aquellos activos tangibles como el hardware que utiliza como base la aplicación Web y el personal necesario para el proceso.

En la tabla constan los activos de información que son los datos que contiene la plataforma e-Learning es decir los activos intangibles, de la misma forma los servicios informáticos, como el Web Hosting, servicios técnicos de soporte de la aplicación a través del entorno virtual, base de la aplicación Web.

Por otra parte, están los activos tangibles como el hardware necesario para qué aplicación Web esté operativa, los servidores de la aplicación, la base de datos y un balanceador de carga. Para terminar con el personal necesario para el proceso.

Estas características se pueden advertir en la identificación de activos del proceso es que el personal destinado para el mismo es limitado debido a que la aplicación fue desarrollada por terceros ajenos a la institución por lo que un analista sólo se encarga del mantenimiento de la aplicación Web.

Tabla 3.11. Identificación y valoración de activos según riesgo del CID de la información

TIPO	NOMBRE DEL ACTIVO	C	I	D	VALOR
Activo de información	Bases de datos Archivos y documentos.	2	3	3	**ALTO**
	Información operacional y de configuración de sistemas.	2	3	3	**ALTO**
	Registros de actividad y evidencia digital.	2	2	2	**MEDIO**
	Contenidos educativos.	1	2	2	**BAJO**
	Exámenes y evaluaciones.	2	3	3	**ALTO**
Servicios informáticos	Web Hosting, servicio técnico, soporte de aplicación)	2	3	3	**ALTO**
Software	Apache2 (servidor Web) 2.4.12	3	3	3	**ALTO**
	PHP (servidor de aplicaciones) 5.5.21	3	3	3	**ALTO**
	MySQL (servidor de base de datos) 5.5.36	3	3	3	**ALTO**
Hardware	Server Aplicación Web 1 Moodle Data (activo) Intel Xeon 2.8 GHz 8 Cores 12 GB RAM	2	3	3	**ALTO**
	Servidor de BDD MySQL Intel Xeon 2.8 GHz 8 Cores 12 GB RAM	2	3	3	**ALTO**
	Server Aplicación Web 1 Moodle Data (pasivo) Intel Xeon 2.8 GHz 8 Cores 12 GB RAM	2	3	3	**ALTO**
	Balanceador de carga F5	2	2	2	**MEDIO**
	Equipamiento de soporte (generadores, Sistemas de alimentación interrumpida (UPS), aire acondicionado).	2	1	1	**BAJO**
Personal proceso	Analista	1	2	2	**BAJO**

3.5.- Análisis y valoración de riesgos

Para realizar el análisis de riesgo se implementó una valoración monetaria a los diferentes tipos de activos, lo que permitió determinar la criticidad del riesgo en que se encuentra en activo específicamente por el valor que representa para la organización. En este apartado, se toma como consideración especial el valor referido a personal, que ha marcado una criticidad baja debido a que el analista dispuesto para regular el proceso analizado comparte el tiempo con sus

otras actividades y no tiene dedicación exclusiva a la plataforma e-Learning, como se muestra en la Tabla 3.12.

Tabla 3.12. Identificación y valoración de riesgos sobre activos

TIPO	NOMBRE DEL ACTIVO	CANTIDAD	VALOR	CRITICIDAD
Activo de información	Bases de datos Archivos y documentos	1	3000	**ALTO**
	Información operacional y de configuración de sistemas	1	2500	**ALTO**
	Registros de actividad y evidencia digital.	1	250	**BAJO**
	Contenidos educativos	1	5000	**BAJO**
	Exámenes y evaluaciones.	1	1900	**ALTO**
Servicios informáticos	Web Hosting, servicio técnico, soporte de aplicación)	1	980	**ALTO**
Software	Apache2 (servidor web) 2.4.12	1	350	**ALTO**
	PHP (servidor de aplicaciones) 5.5.21	1	350	**ALTO**
	MySQL (servidor de base de datos) 5.5.36	1	350	**ALTO**
Hardware	Server Aplicación Web 1 Moodle Data (activo) Intel Xeon 2.8 GHz 8 Cores 12 GB RAM	1	2500	**ALTO**
	Servidor de BDD MySQL Intel Xeon 2.8 GHz 8 Cores 12 GB RAM	1	2500	**ALTO**
	Server Aplicación Web 1 Moodle Data (pasivo) Intel Xeon 2.8 GHz 8 Cores 12 GB RAM	1	2500	**ALTO**
	Balanceador de carga F5	1	990	**MEDIO**
	Equipamiento de soporte (generadores, Sistemas de alimentación interrumpida (UPS), aire acondicionado).	1	1500	**BAJO**
Personal proceso	Analista	1	12000	**BAJO**

Cómo se puede observar los activos intangibles, sobre todo los activos de información, servicio informático y software tiene un alto grado de criticidad, debido a que son los componentes principales por el funcionamiento de la plataforma e-Learning y los activos tangibles del hardware también tiene un alto grado de criticidad, lo que refiere un alto riesgo al momento que una amenaza o vulnerabilidad se presente.

3.6.- Determinación de amenazas y vulnerabilidades

En cuanto a la determinación de las amenazas por activo y las vulnerabilidades, como se observa en la Tabla 3.13, cabe aclarar en este apartado que las amenazas se refieren a las

condiciones externas que podrían motivar un daño falló en los diferentes tipos de activo, las vulnerabilidades por otro lado refieren a las condiciones internas, qué pueden presentarse como condición para dañar o afectar a los activos. En el caso particular del cuadro, se ha anotado aquellas amenazas que responden también a vulnerabilidades identificadas en el proceso de observación y revisión documental. Como por ejemplo, el fallo lógico de software, que también es una debilidad interna, debido a que la aplicación Web fue desarrollada por terceros y al momento de investigación el software de operación se encuentra desactualizado.

Tabla 3.13. Identificación de amenazas y vulnerabilidades por activos

AMENAZA	VULNERABILIDAD	ORIGEN			ACTIVO
		Natural	Humana	Entorno	
Fallo y daños Hardware			X		**Server Aplicación Web 1 Moodle Data (activo) Intel Xeon 2.8 GHz 8 Cores 12 GB RAM Servidor de BDD MySQL Intel Xeon 2.8 GHz 8 Cores 12 GB RAM Server Aplicación Web 1 Moodle Data (pasivo) Intel Xeon 2.8 GHz 8 Cores 12 GB RAM Balanceador de carga F5 Equipamiento de soporte (generadores, Sistemas de alimentación interrumpida (UPS), aire acondicionado).**
Fallo eléctrico				X	
Incendio	X			X	
Robo de hardware	X		X		
Fallo lógico de software	X		X		**Apache2 (servidor web) 2.4.12 PHP (servidor de aplicaciones) 5.5.21 MySQL (servidor de base de datos) 5.5.36**
Robo de información	X		X		**Bases de datos Archivos y documentos. Información operacional y de configuración de sistemas. Registros de actividad y evidencia digital. Contenidos educativos. Exámenes y evaluaciones.**
Intrusión y ataque de malware	X		X		**Web Hosting, servicio técnico, soporte de aplicación**

3.7.- Estado y aplicabilidad de controles ISO/IEC 27001

En cuanto a la declaración de aplicación de los controles de ISO/IEC 27001, se puede observar en los diferentes numerales que hay un estado inexistente o inicial de la aplicación de estos instrumentos de seguridad informática, otros responden a la formación de los analistas de la Dirección de Tecnología y Comunicaciones, más que a una política establecida de seguridad de la información.

Tabla 3.14. Aplicación controles ISO/IEC 27001-02 (I)

Sección	Controles de Seguridad de la Información	Estado
A5	**Políticas de seguridad de la información**	
A5.1	**Directrices de gestión de la seguridad de la información**	
A5.1.1	Políticas para la seguridad de la información	Administrado
A5.1.2	Revisión de las políticas para la seguridad de la información	Administrado
A6	**Organización de la seguridad de la información**	
A6.1	**Organización interna**	
A6.1.1	Roles y responsabilidades en seguridad de la información	Administrado
A6.1.2	Segregación de tareas	Administrado
A6.1.3	Contacto con las autoridades	Administrado
A6.1.4	Contacto con grupos de interés especial	? Desconocido
A6.1.5	Seguridad de la información en la gestión de proyectos	Definido
A6.2	**Los dispositivos móviles y el teletrabajo**	
A6.2.1	Política de dispositivos móviles	Inicial
A6.2.2	Teletrabajo	Inexistente
A7	**Seguridad relativa a los recursos humanos**	
A7.1	**Antes del empleo**	
A7.1.1	Investigación de antecedentes	Inicial
A7.1.2	Términos y condiciones del empleo	Administrado
A7.2	**Durante el empleo**	
A7.2.1	Responsabilidades de gestión	Repetible
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	Definido
A7.2.3	Proceso disciplinario	Definido
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**	
A7.3.1	Responsabilidades ante la finalización o cambio	Definido

Fuente: En base al workbook www.iso27001security.com (2014)

Tabla 3.15. Aplicación controles ISO/IEC 27001-02 (II)

A8	**Gestión de activos**	
A8.1	**Responsabilidad sobre los activos**	
A8.1.1	Inventario de activos	Inicial
A8.1.2	Propiedad de los activos	? Desconocido
A8.1.3	Uso aceptable de los activos	Repetible
A8.1.4	Devolución de activos	Repetible
A8.2	**Clasificación de la información**	
A8.2.1	Clasificación de la información	Inicial
A8.2.2	Etiquetado de la información	Inicial
A8.2.3	Manipulado de la información	Inexistente
A8.3	**Manipulación de los soportes**	
A8.3.1	Gestión de soportes extraíbles	Inicial
A8.3.2	Eliminación de soportes	Inexistente
A8.3.3	Soportes físicos en tránsito	Inexistente
A9	**Control de acceso**	
A9.1	**Requisitos de negocio para el control de acceso**	
A9.1.1	Política de control de acceso	Administrado
A9.1.2	Acceso a las redes y a los servicios de red	Repetible
A9.2	**Gestión de acceso de usuario**	
A9.2.1	Registro y baja de usuario	Definido
A9.2.2	Provisión de acceso de usuario	Definido
A9.2.3	Gestión de privilegios de acceso	Repetible
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	Repetible
A9.2.5	Revisión de los derechos de acceso de usuario	Repetible
A9.2.6	Retirada o reasignación de los derechos de acceso	Repetible
A9.3	**Responsabilidades del usuario**	
A9.3.1	Uso de la información secreta de autenticación	Repetible
A9.4	**Control de acceso a sistemas y aplicaciones**	
A9.4.1	Restricción del acceso a la información	Repetible
A9.4.2	Procedimientos seguros de inicio de sesión	Repetible
A9.4.3	Sistema de gestión de contraseñas	Repetible
A9.4.4	Uso de utilidades con privilegios del sistema	Repetible
A9.4.5	Control de acceso al código fuente de los programas	Repetible

Fuente: En base al workbook www.iso27001security.com (2014)

Tabla 3.16. Aplicación controles ISO/IEC 27001-02 (III)

A10	**Criptografía**	
A10.1	**Controles criptográficos**	
A10.1.1	Política de uso de los controles criptográficos	Inexistente
A10.1.2	Gestión de claves	Repetible
A11	**Seguridad física y del entorno**	
A11.1	**Áreas seguras**	
A11.1.1	Perímetro de seguridad física	Optimizado
A11.1.2	Controles físicos de entrada	Optimizado
A11.1.3	Seguridad de oficinas, despachos y recursos	Optimizado
A11.1.4	Protección contra las amenazas externas y ambientales	Optimizado
A11.1.5	El trabajo en áreas seguras	Optimizado
A11.1.6	Áreas de carga y descarga	Optimizado
A11.2	**Seguridad de los equipos**	
A11.2.1	Emplazamiento y protección de equipos	Optimizado
A11.2.2	Instalaciones de suministro	Optimizado
A11.2.3	Seguridad del cableado	Optimizado
A11.2.4	Mantenimiento de los equipos	Administrado
A11.2.5	Retirada de materiales propiedad de la empresa	Administrado
A11.2.6	Seguridad de los equipos fuera de las instalaciones	Repetible
A11.2.7	Reutilización o eliminación segura de equipos	Repetible
A11.2.8	Equipo de usuario desatendido	Repetible
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Inexistente

Fuente: En base al workbook www.iso27001security.com (2014)

Tabla 3.17. Aplicación controles ISO/IEC 27001-02 (IV)

A12	**Seguridad de las operaciones**	
A12.1	**Procedimientos y responsabilidades operacionales**	
A12.1.1	Documentación de procedimientos operacionales	Repetible
A12.1.2	Gestión de cambios	Inicial
A12.1.3	Gestión de capacidades	Inicial
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	Repetible
A12.2	**Protección contra el software malicioso (malware)**	
A12.2.1	Controles contra el código malicioso	Repetible
A12.3	**Copias de seguridad**	
A12.3.1	Copias de seguridad de la información	Administrado
A12.4	**Registros y supervisión**	
A12.4.1	Registro de eventos	Administrado
A12.4.2	Protección de la información del registro	Repetible
A12.4.3	Registros de administración y operación	Repetible
A12.4.4	Sincronización del reloj	Repetible
A12.5	**Control del software en explotación**	
A12.5.1	Instalación del software en explotación	Repetible
A12.6	**Gestión de la vulnerabilidad técnica**	
A12.6.1	Gestión de las vulnerabilidades técnicas	Repetible
A12.6.2	Restricción en la instalación de software	Administrado
A12.7	**Consideraciones sobre la auditoria de sistemas de información**	
A12.7.1	Controles de auditoría de sistemas de información	Repetible
A13	**Seguridad de las comunicaciones**	
A13.1	**Gestión de la seguridad de las redes**	
A13.1.1	Controles de red	Optimizado
A13.1.2	Seguridad de los servicios de red	Optimizado
A13.1.3	Segregación en redes	Optimizado
A13.2	**Intercambio de información**	
A13.2.1	Políticas y procedimientos de intercambio de información	Repetible
A13.2.2	Acuerdos de intercambio de información	Inicial
A13.2.3	Mensajería electrónica	Repetible
A13.2.4	Acuerdos de confidencialidad o no revelación	Inexistente

Fuente: En base al workbook www.iso27001security.com (2014)

Tabla 3.18. Aplicación controles ISO/IEC 27001-02 (V)

A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**	
A14.1	**Requisitos de seguridad en los sistemas de información**	
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	Definido
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	Repetible
A14.1.3	Protección de las transacciones de servicios de aplicaciones	Definido
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**	
A14.2.1	Política de desarrollo seguro	Administrado
A14.2.2	Procedimiento de control de cambios en sistemas	Administrado
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Repetible
A14.2.4	Restricciones a los cambios en los paquetes de software	Repetible
A14.2.5	Principios de ingeniería de sistemas seguros	Repetible
A14.2.6	Entorno de desarrollo seguro	Repetible
A14.2.7	Externalización del desarrollo de software	Repetible
A14.2.8	Pruebas funcionales de seguridad de sistemas	Repetible
A14.2.9	Pruebas de aceptación de sistemas	Repetible
A14.3	**Datos de prueba**	
A14.3.1	Protección de los datos de prueba	Repetible
A15	**Relación con proveedores**	
A15.1	**Seguridad en las relaciones con proveedores**	
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	Definido
A15.1.2	Requisitos de seguridad en contratos con terceros	Repetible
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	Definido
A15.2	**Gestión de la provisión de servicios del proveedor**	
A15.2.1	Control y revisión de la provisión de servicios del proveedor	Definido
A15.2.2	Gestión de cambios en la provisión del servicio del proveedor	Definido

Fuente: En base al workbook www.iso27001security.com (2014)

Tabla 3.19. Aplicación controles ISO/IEC 27001-02 (VI)

A16	**Gestión de incidentes de seguridad de la información**	
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**	
A16.1.1	Responsabilidades y procedimientos	Administrado
A16.1.2	Notificación de los eventos de seguridad de la información	Administrado
A16.1.3	Notificación de puntos débiles de la seguridad	Administrado
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	Administrado
A16.1.5	Respuesta a incidentes de seguridad de la información	Administrado
A16.1.6	Aprendizaje de los incidentes de seguridad de la información	Repetible
A16.1.7	Recopilación de evidencias	Repetible
A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**	
A17.1	**Continuidad de la seguridad de la información**	
A17.1.1	Planificación de la continuidad de la seguridad de la información	Definido
A17.1.2	Implementar la continuidad de la seguridad de la información	Repetible
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Repetible
A17.2	**Redundancias**	
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	Inexistente
A18	**Cumplimiento**	
A18.1	**Cumplimiento de los requisitos legales y contractuales**	
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Administrado
A18.1.2	Derechos de Propiedad Intelectual (DPI)	Inexistente
A18.1.3	Protección de los registros de la organización	Definido
A18.1.4	Protección y privacidad de la información de carácter personal	Administrado
A18.1.5	Regulación de los controles criptográficos	Inicial
A18.2	**Revisiones de la seguridad de la información**	
A18.2.1	Revisión independiente de la seguridad de la información	Repetible
A18.2.2	Cumplimiento de las políticas y normas de seguridad	Repetible
A18.2.3	Comprobación del cumplimiento técnico	Administrado

Fuente: En base al workbook www.iso27001security.com (2014)

Como se observa en la figura 3.4, los controles aplicados son el resultado en mayor proporción (39%) de la aplicación de conocimientos de los analistas de la Dirección, por su formación académica. De igual forma, en un porcentaje menor de 19% encontramos que hay políticas de seguridad definidas que actúan de forma segmentada en los diferentes procesos, pero para la aplicación Web no necesariamente se aplican estas políticas, por lo que queda expuesta a las amenazas, vulnerabilidades y riesgos.

Figura 3.4. Estado de aplicación porcentual de controles

Por último, se puede observar en el Tabla 3.20, cuadro comparativo que si bien el porcentaje de brecha de implementación está en la etapa inicial, es decir todavía no se han definido las políticas de seguridad de la información, se vienen aplicando controles; que responden por un lado, a la formación propia de los analistas de la organización y también un grupo de controles que están presentes en el esquema gubernamental, implementado incompletamente.

Tabla 3.20. Aplicación controles ISO/IEC 27001-02 (VII)

Estado	Significado	Proporción de requerimientos SGSI	Proporción de Controles de Seguridad de la Información
? Desconocido	No ha sido verificado	0%	2%
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.	19%	8%
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.	48%	9%
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.	0%	39%
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.	22%	12%
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.	11%	19%
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.	0%	11%
No aplicable	A fin de certificar un SGSI ,todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.	0%	0%
	Total	100%	100%

Fuente: En base al workbook www.iso27001security.com (2014)

3.8.- Propuesta de modelo de gestión de seguridad de la información para procesos estratégicos

Tomando como referencia lo realizado por Santiso, Koller, & Bisaro (2014), en *Seguridad en entornos de educación virtual* y Landeta Guachamin (2016), *Análisis y diseño de un sistema de gestión de seguridad de la información sobre la base de las normas ISO 27001 y 27002 para la Superintendencia de Control del Poder de Mercado*, la aplicación de un modelo de gestión de seguridad de la información se va construyendo a partir de la aplicación de los controles de la norma ISO/ IEC 27001 y 27002.

En el siguiente cuadro se anota un esbozo de modelo de gestión de seguridad de la información para el sector público enfocado desde los procesos estratégicos:

Tabla 3.21. Esbozo de elementos constitutivos de modelo de gestión de seguridad de la información para procesos estratégicos del sector público

Proceso	Propuesta
Gestión de indicadores	Aplicar indicadores de gestión para implementación de SGSI, como la política de seguridad de la información.
Alcance y límite de la gestión de seguridad	Hasta la implementación total del esquema gubernamental de seguridad de la información se debe procurar definir los procesos estratégicos y aplicar el SGSI basado en la Norma ISO/IEC 27001, tomando en cuenta los proceso más débiles y puertas de ingreso para atacantes, como aplicaciones Web.
Organización de seguridad	Tratar de aplicar por más de 50% los 113 controles de la norma.
Políticas de seguridad de la información	Implementar una política genérica de seguridad de la información, pero también procedimientos más específicos para procesos estratégicos. Hasta la total aplicación del esquema gubernamental.
Aspectos organizativos para la seguridad	Crear comité de seguridad de la información y disponer un oficial de seguridad.
Gestión de activos	Inventario actualizado de los activos y responsables, mantenimiento y designación de responsables.
Seguridad de los recursos humanos	Control de accesos de a niveles de información. Acuerdos de confidencialidad de la información. Régimen disciplinario para determinación de responsabilidades. Concienciación.
Gestión de incidentes	Reportes al oficial, solución de debilidades internas y externas.
Gestión de continuidad de negocios	Establecer un plan de recuperación ante riesgos.
Control de accesos	Constituir política de accesos a los activos intangibles y tangibles que hacen el proceso.
Gestión de comunicación y operaciones	Definir responsables internos sobre aplicación creada a medida por tercero.
Desarrollo de mantenimiento de sistema	Auditorias y explotación de vulnerabilidades frecuentes incluidas actualizaciones.
Seguridad física y entorno	Elevar controles de acceso a servidores, resguardar frente a daños físicos.
Conformidad	Aplicar el modelo provisional hasta aplicación de esquema gubernamental evitando conflicto legal administrativo.

CONCLUSIONES

Existe la disposición de un organismo gubernamental como la Secretaría Nacional de la Administración Pública (SNAP), que dispone la implementación del Esquema Gubernamental para la Seguridad de la Información, que está basada en la norma ISO/IEC27001, sin embargo la brecha de implementación es grande debido a que la identificación de los activos tangibles e intangibles de las áreas gubernamentales y la determinación de los riesgos amenazas y vulnerabilidades una tarea minuciosa y larga, por lo que la aplicación de un SGSI por procesos estratégicos, de acuerdo a las particularidades anotadas en esta investigación, puede dar paso a un mejor manejo de la seguridad.

Tras la evaluación de la Unión Internacional de Telecomunicaciones (UIT), se estableció una división general de los países en 3 categorías: países líderes en materia de ciberseguridad, países que están madurando todavía, y países que se encuentran en etapas iniciales de su desarrollo de políticas de seguridad informática. Entre los países de Latinoamérica, Ecuador ocupa el sexto lugar. En lo que respecta a las 3 categorías generales, Ecuador este en estado intermedio: no figura entre los líderes, pero tampoco está en la lista de países que se encuentran en etapas iniciales de su desarrollo.

La implantación de un modelo de gestión, conlleva la adopción de un proceso de mejora continua apoyado con auditorías externas que permita identificar las deficiencias en la implantación del modelo y tomar las medidas correctivas que correspondan.

La adopción de un modelo de gestión de la seguridad de la información en las Entidades del Sector Público del Ecuador les permitirá continuar operando con normalidad en caso de materializarse eventos que pongan en riesgo la seguridad de la información.

Acorde al análisis efectuado en el Ministerio de Finanzas aún no se logra una implementación clara o completa de la Seguridad de la Información siendo que el desarrollo y adopción del modelo permitirá gestionar la seguridad de la información basado en las Normas Técnicas Ecuatorianas NTE INEN-ISO/IEC 27000 en procesos estratégicos riesgosos de las entidades del sector público del Ecuador.

El modelo de gestión aplicando herramientas para la Web como OWASP ZAP, permite establecer una metodología de explotación de vulnerabilidades y auditorias, con herramientas sencillas, para corroborar mediante análisis cuantitativo, el análisis cualitativo de brecha de implementación del SGSI.

En este sentido, las acciones a considerar son:

- ✓ Comenzar a adoptar estándares de seguridad para este sector, como la ISO/IEC 27001, para procesos estratégicos.
- ✓ Definir las políticas de seguridad necesarias.
- ✓ Implantar todos los controles para procesos riesgosos.
- ✓ Concienciar a los trabajadores sobre los riesgos que existen en seguridad, al tiempo que se capacita al personal.
- ✓ Monitorear desde el punto de vista de seguridad y generar inteligencia que permita compartir conocimiento y experiencias.

Con el trabajo de investigación se determina que el SGSI gubernamental aun carece de guías formales de análisis y que una herramienta para explotación de vulnerabilidades para aplicaciones Web es OWASP ZAP, sin embargo pueden realizarse otra serie de análisis para determinación de riesgos y amenazas como análisis de código fuente y de estrés de carga que se dirigen fundamentalmente al análisis del diseño de la arquitectura de programación de la aplicación y que se puede implementar en cualquier programa.

RECOMENDACIONES

Luego de realizar la investigación se puede determinar que las aplicaciones Web, realizadas a medida o por terceros para instituciones del sector público, representa una puerta abierta para los ataques informáticos, pues tiene una serie de vulnerabilidades que son producto de la falta de asistencia técnica para el proceso de actualización del software.

Por lo que, es necesario además contar con un sistema de gestión de la información (SGSI), que contemple las auditorías y explotación de vulnerabilidades recurrentemente, pero también como medidas preventivas considere la actualización de los diferentes activos de informáticos a versiones más recientes.

Este modelo de seguridad de la información para el sector público, trata de combinar los mejores elementos de la evaluación de vulnerabilidades, con metodologías como OWASP, con los elementos de un sistema de gestión de seguridad de la información (SGSI), que está basado en la norma técnica ISO 27001. Es recomendable para todas las entidades del sector público realizar al menos la aplicación de este modelo, para la identificación de los riesgos a los que están expuestos con las aplicaciones Web que disponen, de esta manera puede evitarse la intrusión de atacantes a los sistemas más estratégicos del sector público.

Así mismo, este modelo a pesar de que fue desarrollado para el sector público ha demostrado su aplicabilidad en el sector privado, sobre todo para las diferentes organizaciones que realizan procesos formativos o de capacitación y disponen de plataformas e-Learning, con la aplicación de este modelo se pueden reducir los riesgos y mantener el CID de la información.

Es recomendable que los resultados de esta investigación sean socializados entre organizaciones del sector público como privado, para sensibilizar acerca de los riesgos de las aplicaciones Web como puertas de entrada para atacantes y la posibilidad de que se atenten contra activos informáticos más importantes.

De igual forma, en el proceso de investigación se dispuso de algunos formatos para el análisis de la brecha de implementación del SGSI. Para futuras investigaciones y para su aplicación en la práctica para las organizaciones es necesario que el modelo desarrolle formatos

únicos disponibles en la Web para el proceso de análisis. Por eso, es recomendable que se desarrollen elementos de capacitación sobre la explotación de vulnerabilidades con la aplicación OWASP-ZAP y la aplicación de los formatos para análisis de brecha de implementación del SGSI y aplicación de controles de la norma ISO 27001.

BIBLIOGRAFÍA

Ángeles, L. (2010). *Sistema de Gestión de Seguridad de Información ISO 27001 para un Data Center.* Obtenido de http://repositorio.uni.pe/handle/uni/6704

Astudillo, C. C.-M. (2018). Attacking an ERP with Open Source Software. *Enfoque UTE, 1*(9), 138-148.

Borbúa, R. V. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. *URVIO: Revista Latinoamericana de Estudios de Seguridad*(20), 31-45. Obtenido de http://revistas.flacsoandes.edu.ec/urvio/article/download/2571/2105?inline=1

Checkpoint. (s/f). Recuperado el 2018 de octubre de 19, de https://www.checkpoint.com/products/ips-software-blade/

DealerWorld. (16 de octubre de 2018). Obtenido de https://www.dealerworld.es/seguridad/aplicaciones-web-cada-vez-mas-vulnerables

Deloitte. (2018). Obtenido de file:///C:/Users/usuario/Downloads/Deloitte%202018%20Cyber%20Risk%20%20Information%20Security%20Study%20-%20Ecuador%20vF.pdf

Fernández, A. V. (2017). Análisis de las ciberamenazas. *Cuadernos de estrategia*(185), 97-138.

Garcia Sanchez, I. (s.f.). *Hablar sobre el Triángulo de la Gestión de Proyectos*. Obtenido de https://sites.google.com/site/ivangarciasanchez90/objetivos/gestion-tema-9/4o

Gomez Zafra, G. A. (2017). *Herramientas de prueba de seguridad de aplicaciones.* Obtenido de http://hdl.handle.net/10609/81450

Hernández Sampieri, R. F. (2006). *Metodología de la investigación.* México: McGraw-Hill.

INEN. (2011). *NORMA TÉCNICA ECUATORIANA NTE INEN-ISO/IEC 27001:2011.* Quito: Primera Edición.

ISOtools. (14 de abril de 2016). Obtenido de https://www.isotools.org/2016/04/14/iso-27001-aplicarla-sector-publico/

ItDigitalSecurity. (23 de abril de 2018). Obtenido de https://www.itdigitalsecurity.es/vulnerabilidades/2018/04/el-94-de-las-aplicaciones-web-sufren-vulnerabilidades-muy-graves

Kaspersky Lab. (18 de septiembre de 2017). Obtenido de https://latam.kaspersky.com/about/press-releases/2017_kaspersky-lab-incidents-of-digital-kidnappings-in-latin-america

Landeta Guachamin, F. (2016). *Análisis y diseño de un sistema de gestión de seguridad de la información sobre la base de las normas ISO 27001 y 27002 para la Superintendencia de Control del Poder de Mercado.* Quito: Tesis. Universidad Politécnica Salesiana.

Motos, V. (3 de julio de 2012). RIPS: un analizador de código estático de PHP. *HackPlayers*. Obtenido de https://www.hackplayers.com/2012/07/rips-un-analizador-de-codigo-estatico.html

Ortega, J. C. (2017). Aspectos fundamentales en la construcción de páginas web seguras basados en OWASP. *Boletín Informativo CEI, 2*(4). Obtenido de http://www.umariana.edu.co/ojs-editorial/index.php/BoletinInformativoCEI/article/download/1416/1378

OWASP. (2017). *OWASP Top 10 - 2017. Los diez riesgos más críticos en Aplicaciones Web.* Recuperado el 11 de octubre de 2018, de https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

OWASP Foundation. (2017). *OWASP Top 10 - 2017. Los diez riesgos más críticos en Aplicaciones Web.* Obtenido de https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Pacheco, F. G. (2008). *Ethical Hacking.* USERSHOP.

Pardo, M. (2015). Obtenido de http://www.digiware.net/sites/default/files/Tendencias-Seguridad-2015.pdf

Pozo, I. H. (25 de Septimbre de 2013). *Registo Oficial.* Obtenido de Secretaría Nacional de la Administración Pública: www.registroficial.gob.ec

Ramos, J. L. (2013). PRUEBAS DE PENETRACIÓN O PENT TEST. *Revista de Información, Tecnología y Sociedad*(31). Obtenido de http://www.revistasbolivianas.org.bo/scielo.php?pid=S1997-40442013000100014&script=sci_arttext&tlng=es

Sánchez Solá, Á. P. (2013). *Diseño de un Sistema de Gestión de la Seguridad de la Información para Comercio Electrónico basado en la ISO 27001 para pequeñas y medianas empresas en la ciudad de Quito* . Quito: Quito (Bachelor's thesis, QUITO/PUCE/2013).

Sánchez, J. (2016). *Ciberseguridad: mecanismos de ataque y defensa más extendidos.* Obtenido de http://oa.upm.es/44509/

Santiso, H., Koller, J. M., & Bisaro, M. G. (2014). Seguridad en Entornos de Educación Virtual. *Memoria Investigaciones en Ingeniería*. Obtenido de http://www.um.edu.uy/docs/Seguridad_en_entornos_de_educacion_virtual.pdf

Solarte, F. N. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC. *Revista Tecnológica-ESPOL,, 5*(28).

Solarte, F. N. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica-ESPOL, 5*(28).

Suárez, R., & Medina Iriarte, J. (2006). *Estándares para la seguridad de información con tecnologías de información.*

Tarazona, T. &. (2007). Amenazas informáticas y seguridad de la información. *Derecho Penal y Criminología*(28), 137.

Vallejo, R. (2014). *evaluación de seguridad de la información basada en iso/iec 27000.* Quito. Obtenido de https://repositorio.espe.edu.ec/bitstream/21000/9025/1/AC-MEAST-ESPE-048284.pdf

www.iso27001security.com. (2014). *www.ISO27001security.com.* Obtenido de http://www.iso27001security.com/ISO27k_ISMS_and_controls_status_with_SoA_and_gaps_Spanish.xlsx

ANEXOS

UNIVERSIDAD TECNOLÓGICA ISRAEL

ESCUELA DE POSGRADOS

MAESTRÍA EN TELEMÁTICA,

MENCIÓN: CALIDAD EN EL SERVICIO

(Aprobado por: RPC-SO-19-No.300-2016-CES)

ARTÍCULO CIENTÍFICO

Autor: Carlos David Rocha Cahueñas, Ing.

Tutor: Ing. Pablo Recalde, MSc.

Quito – Ecuador

2019

MODELO DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN PARA EL SECTOR PÚBLICO

Explotación de vulnerabilidades y análisis brecha de implementación del Sistema de Gestión de la Seguridad de la Información (SGSI) en un proceso estratégico.

AUTOR: ING. CARLOS DAVID ROCHA CAHUEÑAS

RESUMEN

El desarrollo de un modelo de gestión de la seguridad de la información (SGSI) para las entidades del Sector Público basado en las normas NTE INEN-ISO/IEC 27000 permite dotar a las mismas de una herramienta de gestión para la seguridad de la información adaptable a sus objetivos estratégicos y requerimientos de seguridad, que permite garantizar su confidencialidad, integridad y disponibilidad, a través de un manejo adecuado de los riesgos a los cuales pueden estar expuestos los activos de información. La plataforma e-learning del Ministerio de Finanzas del Ecuador, al igual que todas las aplicaciones web está expuestas a amenazas e intrusiones. La presente investigación está basada en métricas simples, claras y objetivas, sobre vulnerabilidades del sistema y debilidades en la gestión de la seguridad de la información, con el fin de asegurar la selección de controles de seguridad, adecuados y proporcionados para procesos estratégicos riesgosos en el sector público, para que no sirvan de puerta para ataques informáticos de mayor envergadura y que protejan los activos de información de la Institución.

PALABRAS CLAVES: SGSI, proceso estratégico, pentesting, seguridad, ISO/IEC 27001

ABSTRACT

The development of an information security management model (ISMS) for public sector entities based on the NTE INEN-ISO / IEC 27000 standards allows them to provide a management tool for the security of adaptable information to its strategic objectives and security requirements, which allows guaranteeing its confidentiality, integrity and availability, through an adequate management of the risks to which the information assets may be exposed. The e-learning platform of the Ministry of Finance of Ecuador, like all web applications, is exposed to threats and intrusions. The present research is based on simple, clear and objective metrics, on system vulnerabilities and weaknesses in the management of information security, in order to ensure the selection of security controls, adequate and proportionate for risky strategic processes in the public sector, so that they do not serve as a gateway for larger computer attacks and that protect the information assets of the Institution.

KEYWORDS: ISMS, strategic process, pentesting, security, ISO / IEC 27001

INTRODUCCIÓN

Según la *Encuesta 2018 sobre tendencias de cyber-riesgos de seguridad de la información en Ecuador*, que toma información procedente el sector público, financiero, de consumo, telecomunicaciones y energía indica que 4 de cada 10 organizaciones sufrieron incidentes de seguridad en los últimos 24 meses y, el 70% de las organizaciones afirma no tener certeza de la efectividad de su proceso de respuesta ante incidentes de seguridad. El problema para la implementación de un proceso de seguridad ante ciberamenazas es el presupuesto, como consecuencia solamente una de cada diez organizaciones cuenta con un proceso de gobierno de seguridad para proteger sus activos frente a las ciberamenazas (Deloitte, 2018).

En el presente trabajo se pretende realizar un análisis de las principales vulnerabilidades de la plataforma e-Learning del Ministerio de Finanzas del Ecuador, para formación permanente del talento humano y el análisis de la brecha de implementación del SGSI específicamente para aplicaciones Web creadas por terceros, ajenos a la entidad. Para determinar el nivel de vulnerabilidad de la plataforma ante ataques que pudieran comprometer la disponibilidad, integridad y confidencialidad de la información, se realiza un *pentesting* de caja negra simulando el ataque de un hacker, con esto se extraerá el nivel de vulnerabilidad y riesgos a los que se expone la aplicación web, para identificar la causalidad interna del riesgo debido a la brecha de implementación del SGSI. Se propondrá recomendaciones para mitigar las amenazas detectadas, con la finalidad de establecer un modelo de gestión de seguridad de la información para el sector público basado en la Norma Técnica Ecuatoriana NTE INEN-ISO/IEC 27000, principalmente con la aplicación de controles de seguridad de la norma NTE INEN-ISO/IEC 27002.

Existen organismos como OWASP, Deloitte o Kaspersky, que publican, cada año o regularmente, un análisis de los principales ataques que sufren las aplicaciones web y las organizaciones en su infraestructura tecnológica. Según Deloitte, en su *Encuesta 2018* indica que de 10 organizaciones al menos 4 han sufrido incidentes de seguridad en los últimos 24 meses y el 70% de organizaciones no poseen procesos de respuesta ante incidentes y ciberseguridad. El incremento de las ciberamenazas supone un reto para las organizaciones en particular para el sector público debido a que deben garantizar la disponibilidad de los servicios públicos. Según ISOtools (2016), la aplicación de la norma 27001 en el ámbito público se ha centrado básicamente en la necesidad de preservar los activos industriales y de la infraestructura que son la base de la de los sectores estratégicos del funcionamiento de un país.

En los últimos años, los ataques a los sectores estratégicos de varios países han generado alertas significativas entre los diferentes gobiernos. De hecho, a partir del ataque ransomware WannaCry, que no fue dirigido específicamente hacia el sector público, sino que fue progresando a medida del contagio con otros sectores. Se evidenció grandes vulnerabilidades en los sistemas de informáticos públicos, que terminaron temporalmente apagados.

Luego de 34.200 intentos de infección en 97 países India, Estados Unidos y Rusia fueron los más afectados, los ataques fueron indiscriminados tanto para el sector público como para el sector privado. Entre los afectados más representativos estuvieron la empresa Telefónica que brinda servicio de telecomunicación en España, el Servicio Nacional de Salud de Inglaterra y la empresa FedEx de entrega de paquetería en Estados Unidos (Kaspersky Lab, 2017).

El Ecuador no es ajeno a este fenómeno, según Kaspersky Lab (2017) empresa seguridad informática, al hacer un balance del ataque del ransomware señaló que WannaCry logró estar

alrededor de 200 mil equipos en 150 países. En América Latina los más afectados fueron México, Brasil, Chile, Ecuador y Colombia.

Según Ortega (2017), el desconocimiento, el mal uso, o la inexistente utilización de buenas prácticas para el desarrollo de aplicaciones web, hacen que este software específicamente sea susceptible de ataques informáticos.

La Seguridad de la Información busca establecer normas y políticas con la finalidad de mantener de confidencialidad, integridad y disponibilidad de la información (CID), puesto que la falta del cumplimiento de estos objetivos pondría a la organización en riesgo y por ende a su información.

MATERIALES Y MÉTODOS

Ataques cibernéticos

En la terminología de la norma ISO/IEC 27001, se entiende como ataque informático al *ciberataque,* este se refiere a los "intentos para destruir, exponer, alterar, inhabilitar, robar u obtener acceso no autorizado o hacer uso no autorizado de un activo de información".

Según Pardo (2015), los principales ataques se enfocan en la explotación de vulnerabilidades, de los eslabones más débiles de los sistemas informáticos y administrativos "como áreas administrativas, usuarios con cultura no adecuada de seguridad, proveedores, Outsourcing, terceros o firmas conexas".

Según Borbúa (2017; ItDigitalSecurity, 2018; DealerWorld, 2018), las aplicaciones Web son la principal puerta de entrada para los ataques informáticos. De hecho 94% de las aplicaciones Web tienen vulnerabilidades críticas (ItDigitalSecurity, 2018). Las causas son múltiples pero sobre todo se coincide en que el mal uso la inexistencia de buenas prácticas para el desarrollo explicaciones Web hacen que estas sean et altamente vulnerables.

Como anota OWASP (2017), los atacantes utilizar las aplicaciones Web como rutas de acceso para atacar a la organización. En el siguiente gráfico, se observa las diferentes rutas que utilizan los atacantes para generar impactos al negocio de la organización.

Vulnerabilidad

La vulnerabilidad de la seguridad de los sistemas de información son una puerta abierta para los ataques informáticos, el potencial acceso no autorizado, abuso o fraude no se limitan a un solo lugar, sino que puede ocurrir en cualquier punto de acceso a la red. Son los equipos que no reciben el mantenimiento adecuado o que por fallas eléctricas suelen dañarse y dejar a la organización con menos recursos para realizar sus operaciones. Las organizaciones siempre estarán expuestas a estos tipos de riesgos o ataques informáticos. Las principales vulnerabilidades que se encontraban las aplicaciones Web y que son consideradas debilidades que presente el sistema al momento de su desarrollo o en la aplicación de controles de seguridad son las siguientes: "la no validación de entrada de datos en las aplicaciones Web, como por ejemplo: inyecciones SQL, Cross Site Scripting (XSS), inclusiones de ficheros locales (LFI) y remotos (RFI), Server SideIncludes (SSI)" (Ortega, 2017).

Ataques informáticos en Ecuador

Según Pardo el (2015), del informe de realizado para Digiware, los principales métodos de ataque a la seguridad informática son los métodos de infiltración de código intruso, es una vulnerabilidad que se presenta en aplicaciones para realizar consultas a bases de datos. El principal país que realiza ataques informáticos de la región es Colombia "seguido de Argentina, Perú, México y Chile". Por otro lado, el país que más ataques SQL Injection realiza es Ecuador. El informe indica que el sector más vulnerable frente a ataques informáticos es el de gobierno con un 49.53%, seguido por el sector financiero con 14.34%, comunicaciones con el 12.83%, industria con un 10.70% y energía con el 6.54% (Pardo, 2015).

Gestión de Seguridad de la Información

La gestión de seguridad de la información es un proceso que las organizaciones deben llevar con respecto a las amenazas que puedan existir contra sus activos de información y que se puedan materializar como riesgos de consideración (Solarte F. N., 2015). Construir un sistema de control de seguridad describe un conjunto de reglas, entre ellas quienes pueden ser los responsables de la seguridad y que controles pueden adoptar para proteger la información, la idea no es convertir la seguridad en algo inmanejable (Ángeles, 2010). Por lo que la Gestión de Seguridad de la Información es un conjunto de procesos relacionados entre sí que tienen el fin de prestar seguridad a los activos de las empresas.

Metodología de Evaluación de Seguridad de la Información

Según Vallejo (2014), la metodología en la norma NTE INENE-ISO/IEC27000:2012 está conformada por un grupo de etapas a seguir para realizar la evaluación de seguridad de la información.

Recopilación de Información

En esta etapa los evaluadores tendrán una aproximación general a la documentación, registros y recursos que se utilizan en la institución y sus procesos (Vallejo, 2014).

Objeto y Alcance de la Evaluación

En esta etapa se define cual será el objeto de estudio y alcance que conduce a la evaluación de seguridad de la información; y sobre el proceso de la organización, que se aplicará la evaluación (Vallejo, 2014).

Plan de la Evaluación

En esta etapa se trata de evaluar la viabilidad para alcanzar los objetivos determinados en el proyecto, se enlistan las actividades para realizar en el marco de la evaluación; así como también se realizará la valoración de recursos y tiempos necesarios para la ejecución de cada actividad (Ángeles, 2010).

Análisis de Brecha de Seguridad de la Información

En esta etapa se trata de evaluar el cumplimiento o de los requisitos de la norma ISO/IEC 27001:2005 y los controles del Anexo A. Se desarrolla a partir de un análisis cualitativo mediante la valoración de los ítems anotados (Vallejo, 2014).

Proceso de Valoración y Evaluación

Para Vallejo, el proceso de valoración y evaluación se requiere de la metodología de análisis que determinará el riesgo, establecida de forma cuantitativa y cualitativa combinado.

Brecha de Seguridad y Plan de Tratamiento de Riesgos
En esta fase se procesan los informes finales: la brecha de seguridad y el plan de tratamiento. Cada informe final se entrega a la dirección de la organización, debe ser claro, conciso y ordenado, debe incluir recomendaciones fundamentales en las mejores prácticas y en el contexto de la evaluación (Vallejo, 2014).

Análisis de vulnerabilidades
Los ataques cibernéticos fundamentalmente se centran en la manipulación, acceso y robo de datos informáticos. Un análisis de vulnerabilidades trata de identificar las debilidades de la seguridad informática, que aparecen como ventanas para la materialización de los ataques (Fernández, 2017). Las principales vulnerabilidades que se pueden identificar en un equipo informático pueden ser sobre el diseño, debido a la debilidad de los protocolos utilizados para redes, sobre políticas de seguridad eficientes, respecto de implementación que tiene que ver con errores de programación, puertas traseras y errores no voluntarios del fabricante, una configuración errónea en sistemas informáticos, desconocimiento y descuidos de los usuarios, la disponibilidad de herramientas que facilitan ataques, limitaciones a las tecnologías de seguridad, entre otras (Solarte F. N., 2015).

Pentesting o prueba de penetración o intrusión
Pentesting o es la abreviación de penetración y *testing*, que significa prueba de penetración, se refiere al ataque a diversos entornos con la intencionalidad de encontrar fallos, vulnerabilidades u otros, en un equipo o sistema informático. Su importancia se debe a infinidad de ataques de filtraciones que se van dando a las aplicaciones Web en los últimos tiempos (Astudillo, 2018). Está construido para determinar y clasificar el alcance y la repercusión de las vulnerabilidades de seguridad, sobre los resultados que se obtienen se construyen presupuestos de riesgo y peligrosidad que tienen equipos o sistemas informáticos (Astudillo, 2018). Existen diferentes pruebas de intrusión que tienen diferente enfoque y eficiencia, los tipos de *pentest* que existen son los de caja blanca negra y gris (Astudillo, 2018).

CONCLUSIONES

Existe la disposición de un organismo gubernamental como la Secretaría Nacional de la Administración Pública (SNAP), que dispone la implementación del Esquema Gubernamental para la Seguridad de la Información, que está basada en la norma ISO/IEC27001, sin embargo la brecha de implementación es grande debido a que la identificación de los activos tangibles e intangibles de las áreas gubernamentales y la determinación de los riesgos amenazas y vulnerabilidades una tarea minuciosa y larga, por lo que la aplicación de un SGSI por procesos estratégicos, de acuerdo a las particularidades anotadas en esta investigación, puede dar paso a un mejor manejo de la seguridad.

La implantación de un modelo de gestión, conlleva la adopción de un proceso de mejora continua apoyado con auditorías externas que permita identificar las deficiencias en la implantación del modelo y tomar las medidas correctivas que correspondan.

La adopción de un modelo de gestión de la seguridad de la información en las Entidades del Sector Público del Ecuador les permitirá continuar operando con normalidad en caso de materializarse eventos que pongan en riesgo la seguridad de la información.

BIBLIOGRAFÍA

Ángeles, L. (2010). *Sistema de Gestión de Seguridad de Información ISO 27001 para un Data Center.* Obtenido de http://repositorio.uni.pe/handle/uni/6704

Astudillo, C. C.-M. (2018). Attacking an ERP with Open Source Software. *Enfoque UTE, 1*(9), 138-148.

Borbúa, R. V. (2017). Ciberdefensa y ciberseguridad, más allá del mundo virtual: modelo ecuatoriano de gobernanza en ciberdefensa. *URVIO: Revista Latinoamericana de Estudios de Seguridad*(20), 31-45. Obtenido de http://revistas.flacsoandes.edu.ec/urvio/article/download/2571/2105?inline=1

DealerWorld. (16 de octubre de 2018). Obtenido de https://www.dealerworld.es/seguridad/aplicaciones-web-cada-vez-mas-vulnerables

Deloitte. (2018). Obtenido de file:///C:/Users/usuario/Downloads/Deloitte%202018%20Cyber%20Risk%20%20Information%20Security%20Study%20-%20Ecuador%20vF.pdf

Fernández, A. V. (2017). Análisis de las ciberamenazas. *Cuadernos de estrategia*(185), 97-138.

Gomez Zafra, G. A. (2017). *Herramientas de prueba de seguridad de aplicaciones.* Obtenido de http://hdl.handle.net/10609/81450

Hernández Sampieri, R. F. (2006). *Metodología de la investigación.* México: McGraw-Hill.

INEN. (2011). *NORMA TÉCNICA ECUATORIANA NTE INEN-ISO/IEC 27001:2011.* Quito: Primera Edición.

ItDigitalSecurity. (23 de abril de 2018). Obtenido de https://www.itdigitalsecurity.es/vulnerabilidades/2018/04/el-94-de-las-aplicaciones-web-sufren-vulnerabilidades-muy-graves

Kaspersky Lab. (18 de septiembre de 2017). Obtenido de https://latam.kaspersky.com/about/press-releases/2017_kaspersky-lab-incidents-of-digital-kidnappings-in-latin-america

Landeta Guachamin, F. (2016). *Análisis y diseño de un sistema de gestión de seguridad de la información sobre la base de las normas ISO 27001 y 27002 para la Superintendencia de Control del Poder de Mercado.* Quito: Tesis. Universidad Politécnica Salesiana.

Motos, V. (3 de julio de 2012). RIPS: un analizador de código estático de PHP. *HackPlayers*. Obtenido de https://www.hackplayers.com/2012/07/rips-un-analizador-de-codigo-estatico.html

Ortega, J. C. (2017). Aspectos fundamentales en la construcción de páginas web seguras basados en OWASP. *Boletín Informativo CEI, 2*(4). Obtenido de http://www.umariana.edu.co/ojs-editorial/index.php/BoletinInformativoCEI/article/download/1416/1378

OWASP. (2017). *OWASP Top 10 - 2017. Los diez riesgos más críticos en Aplicaciones Web.* Recuperado el 11 de octubre de 2018, de https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

OWASP Foundation. (2017). *OWASP Top 10 - 2017. Los diez riesgos más críticos en Aplicaciones Web.* Obtenido de https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf

Pardo, M. (2015). Obtenido de http://www.digiware.net/sites/default/files/Tendencias-Seguridad-2015.pdf

Pozo, I. H. (25 de Septimbre de 2013). *Registo Oficial.* Obtenido de Secretaría Nacional de la Administración Pública: www.registroficial.gob.ec

Ramos, J. L. (2013). PRUEBAS DE PENETRACIÓN O PENT TEST. *Revista de Información, Tecnología y Sociedad*(31). Obtenido de http://www.revistasbolivianas.org.bo/scielo.php?pid=S1997-40442013000100014&script=sci_arttext&tlng=es

Sánchez Solá, Á. P. (2013). *Diseño de un Sistema de Gestión de la Seguridad de la Información para Comercio Electrónico basado en la ISO 27001 para pequeñas y medianas empresas en la ciudad de Quito* . Quito: Quito (Bachelor's thesis, QUITO/PUCE/2013).

Sánchez, J. (2016). *Ciberseguridad: mecanismos de ataque y defensa más extendidos.* Obtenido de http://oa.upm.es/44509/

Santiso, H., Koller, J. M., & Bisaro, M. G. (2014). Seguridad en Entornos de Educación Virtual. *Memoria Investigaciones en Ingeniería*. Obtenido de http://www.um.edu.uy/docs/Seguridad_en_entornos_de_educacion_virtual.pdf

Solarte, F. N. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC. *Revista Tecnológica-ESPOL,, 5*(28).

Solarte, F. N. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica-ESPOL, 5*(28).

Tarazona, T. &. (2007). Amenazas informáticas y seguridad de la información. *Derecho Penal y Criminología*(28), 137.

Vallejo, R. (2014). *evaluación de seguridad de la información basada en iso/iec 27000.* Quito. Obtenido de https://repositorio.espe.edu.ec/bitstream/21000/9025/1/AC-MEAST-ESPE-048284.pdf

www.iso27001security.com. (2014). *www.ISO27001security.com.* Obtenido de http://www.iso27001security.com/ISO27k_ISMS_and_controls_status_with_SoA_and_gaps_Spanish.xlsx