SISTEMA DE GESTIÓN INTEGRAL DE SEGURIDAD INFORMÁTICA EN SERVICIOS WEB DE E-LEARNING Y TELEFONÍA IP EN GRUPO NETHEXA S.A.S

SEBASTIAN RESTREPO MARIN

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA INGENIERÍAS
FACULTAD DE INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN
MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN
MEDELLÍN
2019

SISTEMA DE GESTIÓN INTEGRAL DE SEGURIDAD INFORMÁTICA EN SERVICIOS WEB DE E-LEARNING Y TELEFONÍA IP EN GRUPO NETHEXA S.A.S

SEBASTIAN RESTREPO MARIN

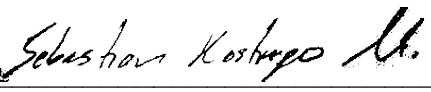
Trabajo de grado para optar al título de Magister en Gestión de Tecnologías de la Información y Comunicación

Asesor
JOHN FERNANDO VARGAS BUITRAGO
Doctor en Ingeniería

UNIVERSIDAD PONTIFICIA BOLIVARIANA
ESCUELA INGENIERÍAS
FACULTAD DE INGENIERÍA EN TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN
MAESTRÍA EN TECNOLOGÍAS DE LA INFORMACIÓN Y LA COMUNICACIÓN
MEDELLÌN
2019

DECLARACIÓN ORIGINALIDAD

"Declaro que esta tesis (o trabajo de grado) no ha sido presentada para optar a un título, ya sea en igual forma o con variaciones, en esta o cualquier otra universidad". Art. 82 Régimen Discente de Formación Avanzada, Universidad Pontificia Bolivariana.

FIRMA AUTOR (ES) 

Medellín; 14 de enero de 2018.

AGRADECIMIENTOS

Expreso mis sinceros agradecimientos a la empresa GRUPO NETHEXA S.A.S. por el compromiso y dedicación del apoyo en la implementación del SGSI de los servicios web de e-learning y telefonía IP, siguiendo los requisitos y lineamientos propuestos por la Universidad Pontificia Bolivariana.

Tabla de contenido

LISTA DE FIGURAS

GLOSARIO

COBIT: Modelo creado para la auditoría y control de sistemas de información.

E-LEARNING: Educación virtual.

ITIL: Estándar de buenas prácticas utilizado para el sostenimiento continúo de la gestión de servicios de TI.

ISO 27001 e ISO 27002: Estándares creados para la gestión de la seguridad de la información.

ISMS: Sistema de administración de seguridad informática.

MÉTRICA: Medición de resultados proporcionados por cada proceso, identificando el grado de cumplimiento de los procesos.

O-ISM3: Modelo de madurez abierto que permite implementar un sistema de gestión de seguridad de la información.

POLÍTICA: Es la gestión y cumplimiento de los procesos definidos por la organización en el SGSI; con el fin de, mejorar la administración de los activos de TIC.

PROCESO: Procedimiento estratégico en el modelo del SGSI.

SGSI: Sistema de gestión de seguridad de la información.

ACUERDO DE NIVELE DE SERVICIO (SLA): Es el cumplimiento del contrato realizo en la prestación de servicios entre cliente y proveedor.

RESUMEN

El proyecto consistió en adaptar un sistema de gestión integral de seguridad informática, que consistió en analizar y mitigar las vulnerabilidades críticas que poseen los servicios web de e-learning y telefonía IP transversalmente a todos los productos que posee GRUPO NETHEXA S.A.S. Creando actividades que ayudaron a definir e implementar lineamientos de seguridad informática, adaptando los estándares de seguridad, disponibilidad y continuidad de los servicios web en la organización.

NETHEXA es una empresa enfocada en la prestación de servicios de TIC y de productos desarrollados por la compañía, partiendo desde el análisis, diseño, implementación y operación de soluciones innovadoras que busca optimizar los recursos de TIC aportando valor agregado a todos los usuarios. La seguridad es de suma importancia y la organización desea agregar confianza a todos los clientes mitigando el riesgo que adquieren, agregando seguridad a los activos de TIC que poseen los servicios de e-learning y telefonía IP desarrollados internamente.

La organización tomó la decisión de acoger el modelo de gestión de seguridad de la información O-ISM3, al tener grandes beneficios al futuro con el grado de madurez al que se puede llegar; también, la empresa se interesa porque es una metodología libre que se puede integrar con diferentes estándares de calidad, buenas prácticas y seguridad en TIC, obteniendo beneficios importantes en la mejora continua de la seguridad en la prestación de servicios desarrollados por la organización en e-learning y telefonía IP.

En la adaptación del SGSI, se investigan y se documentan todos los procesos y políticas necesarias para mejorar la seguridad de los servicios prestados por la organización, determinando las vulnerabilidades y riesgos que poseen los activos de información de los servicios web de e-learning y telefonía IP desarrollados, donde se documenta y se establecen las metodologías alineadas con el SGSI, necesarias para tratar los riesgos críticos que deben de ser solucionados para evitar la materialización de las amenazas.

Al tener claridad del nivel de los riesgos que poseen todos los activos de información, se realiza un seguimiento de los procesos y políticas planteadas en el SGSI, donde se determinan los métodos planteados para mitigar los riesgos críticos, donde son integradas con los procesos de seguridad establecidos en el SGSI, teniendo una alineación de los estándares utilizados con la metodología propuesta por la organización, adaptando metodologías que se acogen a todas las necesidades de seguridad de los servicios prestados por GRUPO NETHEXA S.A.S.

PALABRAS CLAVE: Educación Virtual; HSTS; HTTP; SSL/TLS; VoIP.

ABSTRACT

The project consisted of adapting a comprehensive information security management system, which consisted of analyzing and mitigating the critical vulnerabilities that the e-learning and IP telephony web services have transversally to all the products that GRUPO NETHEXA S.A.S. owns. Creating activities that helped to define and implement IT security guidelines, adapting the security, availability and continuity standards of web services in the organization.

NETHEXA is a company focused on the provision of CIT services and products developed by the company, starting from the analysis, design, implementation and operation of innovative solutions that seeks to optimize CIT resources providing added value to all users. Security is of the utmost importance and the organization wishes to add confidence to all clients by mitigating the risk they acquire, adding security to the CIT assets that have e-learning and IP telephony services developed internally.

The organization made the decision to host the information security management model O-ISM3, having great benefits to the future with the degree of maturity that can be reached; also, the company is interested because it is a free methodology that can be integrated with different quality standards, good practices and security in CIT, obtaining important benefits in the continuous improvement of security in the provision of services developed by the organization in e-learning and IP telephony.

In the adaptation of the ISMS, all the processes and policies necessary to improve the security of the services provided by the organization are investigated and documented, determining the vulnerabilities and risks that the information assets of the e-learning and IP telephony web services have developed, where the methodologies aligned with the ISMS are documented and established, necessary to deal with the critical risks that must be solved to avoid the materialization of the threats.

Having clarity of the level of risks that all information assets have, the processes and policies proposed in the ISMS are monitored, where the methods proposed to mitigate critical risks are determined, where they are integrated with security processes established in the ISMS, having an alignment of the standards used with the methodology proposed by the organization, adapting methodologies that meet all the security needs of the services provided by GRUPO NETHEXA S.A.S.

KEY WORDS: e-learning; HSTS; HTTP; SSL/TLS; HTTP; VoIP.

INTRODUCCIÓN

El trabajo de grado realizado en GRUPO NETHEXA S.A.S ayuda a alinear la seguridad de la información de los productos y servicios en TIC de las plataformas web de e-learning y telefonía IP constantemente, marcando la diferencia en el sector de las TIC en la prestación de servicios informáticos, adoptando la metodología O-ISM3 como sistema de gestión de la seguridad de la información.

La organización es líder en la operación y prestación de servicios de telecomunicaciones, contando con la capacidad técnica de atender requerimientos informáticos en el área de telefonía IP, e-learning, redes de datos, seguridad perimetral, consultoría y optimización de infraestructura (Gutiérrez, 2017). Buscando optimizar cada día los recursos informáticos con mayor seguridad; el principal objetivo es robustecer la seguridad de los activos de información con el pasar del tiempo, protegiendo todos los servicios web proporcionados a los clientes de las nuevas amenazas que afectan la operación y disponibilidad de los productos. La adaptación de los procesos de seguridad de O-ISM3 generó estabilidad y organización de los procesos, alineando las buenas prácticas de seguridad informática de los recursos de TIC de e-learning y telefonía IP, teniendo como referencia las políticas y los procesos estratégicos, tácticos y operativos que se deben de cumplir diariamente para la mejora continua de la seguridad de la información de los servicios web.

Los productos que se beneficiarán cuando se aplique el SGSI de GRUPO NETHEXA S.A.S. adaptado son:

- Educación virtual y contenidos.
- Servidores, servicios en la nube y virtualización.
- Soluciones VoIP – IP PBX Básico.
- Soluciones VoIP para Call Center.

Los servicios mencionados cumplirán con el SGSI, adoptando las políticas y procesos de la metodología O-ISM3 y los demás estándares de buenas prácticas de seguridad que ayudan a la identificación y mitigación de problemas de seguridad críticos para la organización en tres fases de seguridad.

Durante la primera fase se evidencia la adaptación de la metodología O-ISM, donde se documentan los procesos y políticas de buenas prácticas de seguridad establecidas por la organización, incorporando procesos de auditoria, evaluación de amenazas y vulnerabilidades, que aporten a la mejora continua de los controles de seguridad aplicados a los activos de información de las plataformas web de e-learning y telefonía IP.

En la segunda fase se identifican todos los activos de información que poseen los servicios web de e-learning y telefonía IP, con el fin de, realizar un análisis de riesgos de las amenazas que se pueden materializar y perjudicar la disponibilidad de los activos de información. El objetivo de esta práctica es poder identificar los riesgos potenciales y evidenciar las amenazas que deben de ser tratadas para reducir la inseguridad que poseen las plataformas web de la organización.

Durante la tercera fase se definen los controles de seguridad necesarios con el propósito de reducir las amenazas identificadas que afectan la seguridad de los activos de información, las cuales fueron identificadas en el análisis de riesgos realizado en la organización.

Como resultado y beneficio del proyecto se entregan tres productos a GRUPO NETHEXA S.A.S; uno por cada objetivo específico: Documentación de los procesos y políticas del SGSI, resultados del análisis de riesgo y los controles que se deben de implementar para realizar el tratamiento del riesgo de los activos de información. Lo anterior con el propósito de que la empresa pueda ejecutar los controles propuestos y mejorar la seguridad de los activos de información.

1 PLANTEAMIENTO DEL PROBLEMA

1.1 Problema

El uso de los sistemas de información crea la necesidad y la dependencia de la utilización de los medios informáticos de navegación HTTP para realizar la mayoría de los trámites en la red, debido a la reducción de tiempo y dinero, al realizar diferentes procedimientos desde cualquier sitio con acceso a Internet. Por ende, es importante proteger los datos críticos de los usuarios que en su mayoría es tráfico HTTP; por este motivo el tráfico es asegurado bajo los protocolos de seguridad SSL/TLS, que brindan confiabilidad, integridad y autenticidad (Rodríguez, 2013). Sin embargo, los protocolos SSL/TLS han presentado grandes vulnerabilidades en la red de datos, proporcionando una brecha de seguridad para plataformas de navegación HTTP y de transferencia de archivos en la red.

Para reducir los problemas de los protocolos de seguridad SSL/TLS, se desarrolló un mecanismo de seguridad llamado HTTP Strict Transport Security (HSTS), que obliga a que las peticiones realizadas desde un navegador web sean forzadas a utilizar HTTPS, para la utilización de los protocolos SSL/TLS navegando de manera segura, pero este mecanismo HSTS es inseguro, ya que existen ataques informáticos que aprovechan vulnerabilidades en los navegadores y de los aplicativos HTTP, burlando el mecanismo de seguridad y realizando ataques de Man in the Middle (MITM), afectando la integridad de los datos (LeonardoNev, 2015).

El GRUPO NETHEXA S.A.S tiene presente todos los problemas de seguridad que poseen los protocolos HTTP, SSL/TLS y el mecanismo de seguridad HSTS, que afectan la integridad de los servicios de e-learning y telefonía IP publicados en Internet, los cuales soportan servicios web que son fundamentales para la continuidad del negocio de la compañía. Además; los servidores web de la organización no tienen un modelo de gestión de seguridad informática, que permita evaluar e implementar controles de seguridad constantemente a medida que aparecen nuevos ciberataques como consecuencia de nuevas vulnerabilidades descubiertas en las aplicaciones web. Se necesita reducir los problemas de seguridad que se tienen en el hurto de información, escalamiento de privilegios, suplantación de identidad, afectación de la disponibilidad del servicio web, etc. Afectando finalmente a la empresa con la degradación de la imagen corporativa a nivel tecnológico en la prestación de servicios informáticos.

La organización requiere implantar controles en seguridad informática que ayude a mitigar los problemas de seguridad de las plataformas web de e-learning y telefonía IP, que tenga la posibilidad de adaptarse a un sistema de gestión integral que facilite la evaluación de las vulnerabilidades de los servicios web de e-learning y telefonía IP que posee la organización, con el fin de controlar las amenazas informáticas web

existentes que afectan la confiabilidad, integridad, autenticidad y continuidad de los servicios. En el trabajo de grado de maestría, se investigó un sistema de gestión integral de seguridad informática para los servicios web de e-learning y telefonía IP en GRUPO NETHEXA S.A.S; mediante la adaptación de metodologías de seguridad informática, análisis de vulnerabilidades de seguridad web e integración de técnicas de escaneo, que facilitan la identificación y el tratamiento de los problemas de seguridad existentes que presentan las aplicaciones HTTP que operan en la empresa.

1.2 Justificación

En el entorno actual de las tecnologías de la información, se encuentra con la necesidad de depender de los sistemas informáticos, que son accedidos desde hogares y organizaciones por medio de la Internet, generando el crecimiento de aplicaciones, plataformas y entretenimiento de manera remota. Esto ha creado la necesidad de proteger los datos contra personas con altos conocimientos informáticos, que buscan beneficiarse económicamente extrayendo información sensible de los servicios de navegación web.

Es de suma importancia identificar las vulnerabilidades y los problemas de seguridad proporcionados por las malas prácticas en controles de seguridad y los problemas que contienen los protocolos y/o mecanismos de seguridad en aplicaciones HTTP, que pueden ser aprovechadas exitosamente por técnicas de ataques informáticos, permitiendo quebrantar el nivel de seguridad de los sitios web. Adaptando controles de seguridad que permitan controlar los riesgos de seguridad identificados, que exponen la integridad de la información de la navegación en servidores web.

Finalmente, poder informar a la empresa de los problemas de seguridad identificados y de los controles de seguridad que deben ser implementados en los servicios web analizados en el trabajo de grado, contribuyendo con la mejora continua de la protección de los activos de información, que permitan asegurar la navegación en los portales de e-learning y telefonía IP de los clientes que utilizan los servidores de la empresa. Con el fin de, controlar las amenazas informáticas que poseen las plataformas navegación web de la organización; y así, mejorar la disponibilidad de los servicios, disminuyendo el hurto de información crítica, suplantación de identidad, escalamiento de privilegios y la degradación de imagen corporativa, etc.

2 OBJETIVOS

2.1 Objetivo General.

Implementar un sistema de gestión integral de seguridad informática en los servicios web de e-learning y telefonía IP de GRUPO NETHEXA S.A.S. que permita la identificación y mitigación de los riesgos de seguridad críticos que afectan la disponibilidad de los servicios, implementando controles que proporcionen confiabilidad, integridad y autenticidad de los datos.

2.2 Objetivos Específicos

- Seleccionar un modelo de gestión que oriente el proceso de auditoría de seguridad en los servicios web de e-learning y telefonía IP en la organización.
- Determinar las vulnerabilidades críticas que poseen los servicios web de e-learning y telefonía IP en la organización.
- Adaptar controles de seguridad que permitan disminuir el impacto de los ataques informáticos en los servicios web de e-learning y telefonía IP en la organización.

3 MARCO REFERENCIAL

3.1 Marco contextual

El trabajo de grado de maestría busca solucionar algunos los problemas de seguridad que presentan los servicios web de e-learning y telefonía IP en la empresa GRUPO NETHEXA S.A.S., identificando y alertando las posibles vulnerabilidades y/o amenazas que presentan los activos de información web para ser controlados por el área encargada. La organización es líder en la operación y prestación de servicios de telecomunicaciones, contando con la capacidad técnica de atender requerimientos informáticos en el área de telefonía IP, e-learning, redes de datos, seguridad perimetral, consultoría y optimización de infraestructura (Gutiérrez, 2017).

La empresa se enfoca en la prestación de servicios de comunicación IP e infraestructura, que parten desde el análisis, diseño, implementación, optimización y operación de soluciones innovadoras que buscan optimizar los recursos aportando valor agregado a los clientes. Brindando soluciones personalizadas que aportan al core del negocio de cada uno de los clientes, gracias a la permanente innovación de servicios, ya que se poseen desarrollos de productos propietarios y se realiza seguimiento de estratégico de los objetivos de los clientes.

El trabajo consiste en adoptar y documentar los procesos y políticas de seguridad que se adapten a la organización en un sistema de gestión integral de seguridad informática en los servicios web de e-learning y telefonía IP en la empresa GRUPO NETHEXA S.A.S; que permita auditar la seguridad web transversalmente en las aplicaciones HTTP de la organización. Adaptando metodologías de gestión ágiles que permitan establecer políticas y procesos de seguridad que ayuden a identificar y mitigar los problemas de seguridad críticos en la organización.

Se busca que el sistema de gestión integral permita apalancar las políticas de seguridad informática establecidas en la organización, incorporando nuevos procesos que son necesarios en la auditoría constante, aportando en la evaluación y en la mejora continua de la seguridad del servicio web de las aplicaciones internas de educación virtual y soluciones de VoIP, con el fin de mejorar la disponibilidad de los diferentes servicios que son ofrecidos a los clientes de la organización.

Con el objetivo de Informar a los clientes y a la organización los reportes de las vulnerabilidades encontradas y de controles establecidos aplicados en los servicios, permitiendo resolver los problemas de seguridad identificados, con el propósito de contribuir el cumplimiento de buenas prácticas de seguridad informática que pueden ser adaptadas por la empresa, ayudando a disminuir el impacto de ataques informáticos en las aplicaciones web.

3.2 Marco conceptual

- **Aplicaciones HTTP**

Las aplicaciones web manejan diferentes lenguajes de programación como PHP, Java, JavaScript, Ruby, Python, etc. Que facilitan el desarrollo y la estructura de la página web en el servidor, estructurando toda la comunicación en la aplicación con bases de datos, diseño de la página y ejecución del desarrollo para el funcionamiento de todos los campos que posee la página web en la red, estas aplicaciones se encargan de procesar la información que visualiza el usuario en código HTML en el protocolo HTTP. El protocolo HTTP es el protocolo que soporta toda la comunicación en la navegación en aplicaciones web, el cual fue diseñado para proporcionar robustez y tolerancia a fallas prestando un rendimiento confiable en la comunicación en la Word Wide WEB. Berners-Lee, Fielding & Frystyk (1996), Fielding, Gettys, Mogul, Frystyk, Masinter, Leach & Berners-Lee (1999), Nielsen, Leach, & Lawrence (2000) y Belshe, Peon, y Thomson (2015), fueron los encargados de mejorar y actualizar las versiones del protocolo HTTP hasta la versión más reciente HTTP/2.0 informada en la RFC 7540.

- **SSL/TLS**

Rodríguez (2013), el protocolo SSL (Secure Sockets Layer) y su sucesor TLS (Transport Layer Security) son protocolos de seguridad criptográficos que trabajan sobre la capa de transporte, encargados de proporcionar comunicaciones seguras en toda la red de comunicaciones. Brinda confiabilidad, integridad y autenticación en el uso de servicios en la red como la navegación web, correo electrónico, mensajería instantánea, voz sobre IP, etc.

El protocolo HTTPS es esencial en una sesión HTTP, a través de una conexión segura SSL/TLS, utilizando el certificado X.509, que contiene varios campos adicionales que se utilizan para verificar que la clave pública es válida y pertenezca realmente al sitio (Benton, Jo y Kim, 2011).

Wang, et al. (2015), los protocolos criptográficos SSL y TLS fueron diseñados para proporcionar seguridad en las comunicaciones en toda la red de datos, encriptando los datos en la capa de aplicación y en las demás capas subyacentes. SSL/TLS es un protocolo de registro, cuyo funcionamiento se establece a través de un apretón de manos, el cual encapsula los datos en la capa de aplicación.

- **HTTP Strict Transport Security (HSTS)**

Jackson & Barth (2008) y Hodges, Jackson & Barth (2012), mecanismo de seguridad utilizado para realizar conexiones seguras HTTP y que está presente en la RFC 6797, cuyo objetivo es impedir que atacantes puedan convertir el tráfico HTTPS a HTTP. El mecanismo utiliza el navegador del usuario para inspeccionar la conexión con el servidor, con el fin de inspeccionar si ocurre algún error durante la comunicación segura SSL/TLS. La idea principal del mecanismo no es solo forzar las conexiones HTTPS, sino que también el objetivo fundamental es proporcionar

seguridad al usuario al navegar en Internet, muestreando las conexiones donde están ingresando son cifradas con los protocolos de seguridad SSL/TLS.

- **Educación Virtual**

Barhoum & Muhsen (2013), la educación se ha catalogado como una herramienta de educación que brinda calidad a todos los estudiantes que están matriculados en la plataforma, ofreciendo servicios importantes como: permitir interactividad de los canales de comunicación de educación, procesos de aprendizaje diversos para todos los estilos de los estudiantes, variedad de multimedia, descarga e impresión de material de estudio desde la web y crear medios de interacción la colaboración, conversación e intercambio de ideas.

- **VoIP**

Baz, Bonilla, Gorrotxategi, Ibarra, Santamaría & Ruiz (2009), Voz sobre IP (VoIP) es un servicio que permite establecer llamadas sobre Internet, permitiendo la comunicación de voz y video desde diferentes redes que sean convergentes. Esta técnica es llamada telefonía IP, la cual brinda calidad, fiabilidad y bajo costo de inversión para las organizaciones, ya que manejar diferentes códec de audio y video que pueden facilitar el consumo de ancho de banda, facilita la integración en la administración y de seguridad por la integración sobre redes LAN.

- **Seguridad en plataformas de e-learning**

La seguridad mínima de los servicios web de e-learning no es suficiente, debido que al transcurrir el tiempo los servicios manejados en las plataformas de e-learning son vulnerables al estar expuestos a Internet, debido a que los servicios deben de ser actualizados, monitoreados, auditados y asegurados constantemente a través de servicios de seguridad complementarios que permiten mitigar ataques informáticos realizados. Por este motivo, la importancia de regir las normas y los estándares de gestión en seguridad y riesgos informáticos, que poseen la finalidad de preservar la disponibilidad, continuidad e integridad de los servicios web de las plataformas virtuales; con el fin de, controlar y mitigar ataques informáticos como lo son: acceso no autorizado, abuso de privilegios, suplantación de identidad, hacking, divulgación o fuga de información, entre otros; que pueden degradar el servicio y la imagen corporativa de la empresa o institución (Santiso, Koller, & Bisaro, 2016).

- **Seguridad en plataformas de VoIP**

La VoIP es una tecnología que se apoya en las capas y protocolos existentes en las redes de datos, heredando los problemas de seguridad de las capas y los protocolos existentes, siendo algunas de estas las amenazas más importantes de VoIP, problemas clásicos que afectan directamente a la red de datos. Por lo que el servicio de telefonía IP posee varias capas de seguridad que deben ser protegidas, las cuales son: seguridad en aplicaciones y protocolos VoIP, seguridad en el sistema operativo, seguridad en la red, seguridad en los servicios, seguridad física, políticas y procedimientos de seguridad.

Todos los ataques de VoIP tienen un objetivo en específico, el cual es el robo de información confidencial de llamadas telefónicas, degradación de la calidad del servicio de telefonía IP, alteración de la información de llamadas entrantes y salientes, interceptación y secuestro de llamadas, reproducción de conversaciones, robo de identidad e incluso realizar llamadas gratuitas por todo el mundo. Por este motivo la importancia de implementar seguridad constante en el servicio de VoIP, ya que los servidores, sistemas operativos, protocolos con los que trabajan y la infraestructura de red VoIP es susceptible en todo momento de ser atacada (Gutiérrez, 2017).

- **O-ISM3**

O-ISM3 (2017), Es una metodología de gestión de seguridad de la información que proporciona madurez en las organizaciones, al definir los procesos y políticas de seguridad informática, con el fin administrar el sistema de gestión de seguridad de la información (ISMS). O-ISM3 asigna las responsabilidades al negocio empresarial en definir los objetivos de seguridad en políticas, ofreciendo un conjunto de procesos administrativos en seguridad donde el negocio selecciona como implementar un ISMS coherente para poder alcanzar todos los objetivos de seguridad informática del negocio.

3.3 Marco legal

El marco legal del proyecto de implantación del sistema de gestión integral de seguridad informática, que permita analizar y mitigar las vulnerabilidades críticas que poseen los servicios web de e-learning y telefonía IP transversalmente en GRUPO NETHEXA S.A.S, debe tener presente la ley Colombiana y las normas Nacionales e Internacionales de gestión de seguridad informática, protección de datos, delitos informáticos, derechos de autor y divulgación de información confidencial, que puedan apalancar la solución del problema de la organización, por este motivo debemos de tener las siguientes normas presentes:

Decisión_351 (1993), Acuerdo de Cartagena y la ley 23 de 1982 establecen las leyes sobre los derechos de autor: La ley informa sobre la Régimen común sobre derechos de autor y derechos conexos, protección de los derechos de autor, identificación del alcance; y aporta elementos de los sistemas de la información, encontrando aportes importantes en los siguientes artículos: Artículo 1, Artículo 7, Artículo 9, Artículo 11 y el Artículo 52.

Ley_1450 (2011), control de los derechos de autor, donde contiene el Artículo 28 y Artículo 20 de la propiedad intelectual de las obras en cumplimiento de un contrato de prestación de servicios o de un contrato de trabajo.

Ley_599 (2000), código Penal, establece las sanciones contra los derechos de autor y daño por divulgación de información confidencial establecidas en el Artículo 270.

Ley_222 (1995), la información puede ser confidencial establecida en el Artículo 23.

Ley_1712 (2014), ley de la transparencia y acceso a la información pública establecida en el Artículo 7. Disponibilidad de la Información y el Artículo 8. Criterio diferencial de accesibilidad.

Ley_1581 (2012), Disposiciones Generales para la Protección de Datos Personales, establecida en el Artículo 1. Objeto y el Artículo 2. Ámbito de aplicación.

Ley_1273 (2009), Delitos Informáticos establecidos en los artículos: Artículo 269A. Acceso abusivo a un sistema informático, Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación, Artículo 269C: Interceptación de datos informáticos, Artículo 269D: Daño Informático, Artículo 269E: Uso de software malicioso, 269F: Violación de datos personales, Artículo 269G: Suplantación de sitios web para capturar datos personales, Artículo 269I: Hurto por medios informáticos y semejantes y Artículo 269J: Transferencia no consentida de activos.

SGSI (2017), Modelo de Seguridad Colombiano: Sistemas de Gestión de la Seguridad de la Información. “El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones; pública El Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión. Colombia establece un modelo de seguridad y de privacidad que es actualizado periódicamente de las buenas prácticas de seguridad de la información adoptadas de la norma internacional ISO 27001 del 2013, la cual permite la confidencialidad, el aseguramiento e integridad de los datos e información que son procesados informáticamente.”

3.4 Estado del arte

Hodges, Jackson & Barth (2012), el protocolo de navegación HTTP puede ser utilizado en diversos medios de transporte, generalmente estas conexiones se realizan bajo el protocolo TCP, el cual no proporciona integridad y confiabilidad en la transferencia de datos en la red. Por este motivo, son utilizados los protocolos de seguridad Secure Sockets Layer (SSL), y su sucesor, Transport Layer Security (TLS) que fueron creados para dar seguridad de transferencia de información en la red con el protocolo TCP. Los protocolos SSL/TLS no estaba proporcionada seguridad en la comunicación web de los usuarios en la red, ya que diferentes ataques pasivos y activos pueden burlar el uso de la navegación web segura

forzando que la conexión sea insegura, con el propósito de recolectar información en texto plano, este inconveniente es solucionado con el mecanismo HTTP Strict Transport Security (HSTS).

Jackson & Barth (2008) y Hodges, Jackson & Barth (2012), el mecanismo de seguridad de navegación HSTS estándar de la RFC 6797, es creado con el objetivo de obligar a que todos los usuarios que están explorando sitios web puedan navegar de manera segura, este mecanismo exige que el navegador negocie la conexión del cliente y el servidor de manera segura a través de los protocolos de seguridad SSL y TLS; evitando que un atacante en la red pueda interceptar los datos de comunicación de la conexión en texto plano, forzando a que los usuarios se conecten por el protocolo seguro de navegación HTTPS en vez del protocolo menos seguro HTTP.

Brooks & Deng (2010), indican que la mayoría de los sitios de Internet utilizan SSL/TLS como mecanismo de confianza, el cual ha presentado una serie de debilidades en seguridad presentando problemas en la criptografía que maneja, permitiendo ser vulnerables a través de servicios que establecen funciones importantes en la red, como la resolución de nombres de dominio (DNS), enrutamiento sobre Internet, envenenamiento de caché ARP, la destitución de cifrados, errores de programación, la usabilidad del navegador y en ocasiones el criptoanálisis. Presentando lecciones importantes para diseños e implementaciones de nuevos servicios que deben de poseer confianza, por la inseguridad que presentan los ataques MITM para los usuarios en la red.

Mavrogiannopoulos, Vercauteren, Velichkov & Preneel (2012), demuestran que el protocolo SSL/TLS es vulnerable a través de los ataques Wagner y Schneier, el cual utiliza curvas elípticas con parámetros claros en el cifrado Diffie-Hellman, firmados por servidores y que pueden ser interceptados fácilmente por los usuarios. Dacosta, Ahamad & Traynor (2012), proponen utilizar el certificado de validación DVCert, modelo de confianza que propone la validación de certificados fuertes y alta detección de los ataques informáticos MITM. El método funciona con el establecimiento de secretos de doble vía con servicios web importantes, estos secretos son validados por los usuarios y el servicio para dar autenticidad, evitando ataques MITM que está aprovechando las debilidades del método certificación CA desde la red. Los cambios hechos en el protocolo TLS por DVCert, proporcionan una mejora de rendimiento y simplicidad de la seguridad, sin afectar PAK el cual es el método encargado del intercambio de claves del protocolo de seguridad TLS.

Sugavanesh, Prasath & Selvakumar (2013), informan que el protocolo TLS es inseguro, porque para todo usuario al momento de realizar la primera conexión a un sitio web, no se encuentra protegido, ya que al hacer la primera solicitud en texto plano devuelve al usuario los datos de conexión segura (HTTPS), lo que da lugar a que un atacante suplante la conexión con un MITM y el usuario acepte el certificado incorrecto proporcionado por el atacante. Se plantea la utilización de HSTS, el cual

emplea un método de inicio de confianza utilizando STS, donde realiza la primera conexión en el navegador que posee un filtro o control forzando de conexión segura, HSTS forzó la primera solicitud como los métodos HTTPS Lock y Force HTTPS, evitando ataques de MITM en el inicio de sesión de una conexión web, aunque las vulnerabilidades persisten en el apretón de manos del protocolo TLS, permitiendo que la conexión pueda ser atacada con éxito.

Eldewahi, Sharfi, Mansor & Mohamed (2015), los protocolos SSL/TLS han presentado grandes vulnerabilidades en la red de datos, el cual no está exhibiendo la confiabilidad, integridad y autenticidad, enseñando una brecha de seguridad para plataformas de navegación y de transferencia de archivos en la red, por sus debilidades que aprovechan los atacantes y las limitaciones que poseen las actuales contramedidas. Un gran número de vulnerabilidades han sido descubiertas en los protocolos SSL/TLS, en las cuales se destacan ataques como: Cipher Suites Rollback, ChangeCipherSpec Message Drop, ataque Bleichenbacher en PKCS#1, ataques de temporización remota OpenSSL, DoS, ataques sobre el almacenamiento de datos MAC, ataques CBC-Modo, ataques en algoritmos de comprensión, ataque al algoritmo RC4, Ataque Lucky 13, entre otros. Los cuales han sido satisfactorios y que proporciona inseguridad en la red de datos. Dowling, Günther, Fischlin & Stebila (2015), estudian la seguridad criptológica del protocolo TLS 1.3 y la autenticación Diffie-Hellman, el cual actualiza y mejora la seguridad de las anteriores versiones de los protocolos de seguridad TLS 1.1 y 1.2 de las vulnerabilidades que poseen, los cuales son aprovechados por la ciberseguridad con ataques conocidos como: BESTIA, Lucky 13, CANICHE, etc., comprometiendo la integridad y confiabilidad de los datos de las aplicaciones Web y correo electrónico.

Han, Kwon, Hahn, Koo, & Hur (2016), SSL/TLS utiliza certificados para mitigar los ataques MITM, entre la CA que emite un certificado de confianza garantizando la identidad del servidor. Pero al comprometerse el certificado CA, con certificados falsos y la caducidad de los certificados, todos estos métodos del protocolo de seguridad no son suficientes para detectar y prevenir los ataques de MITM. Por estas vulnerabilidades que posee el protocolo de seguridad, se realiza un análisis de ataques de MITM en el apretón de manos de SSL/TLS, se hace pasar por un usuario legítimo, demostrando que la seguridad del protocolo es vulnerable y que no puede mitigar todos los ataques de MITM.

La información investigada ayuda a aclarar que los protocolos de seguridad SSL/TLS que son utilizados en la actualidad son vulnerables; sin embargo, a pesar de que el protocolo seguridad es actualizado y mejorado, persisten las debilidades que pueden ser aprovechadas por ataques informáticos. Como punto de partida ante las vulnerabilidades encontradas en los protocolos de seguridad y de comunicación, se encuentra diferentes procedimientos de pentesting que ayudan a retroalimentar el trabajo de maestría planteado, tomando en cuenta las investigaciones y desarrollos de seguridad informática actuales que pueden apoyar

a evidenciar las vulnerabilidades existentes en los servicios web de GRUPO NETHEXA S.A.S.

LeonardoNev (2015), SSLStrip2, DNS2Proxy, Delorian, MITMF y BeterCap, son herramientas que proporcionan ataques informáticos de MITM que nacen del investigador Leonardo Nve, estas herramientas son nuevas versiones de ataques informáticos. Orientados a la navegación HTTPS, que contienen características importantes con el fin de evitar el mecanismo de protección HSTS. El propósito fundamental de estas herramientas es cambiar el tráfico HTTPS a HTTP y el nombre de la máquina en el código HTML, con el fin de evitar el mecanismo HSTS, capturando el tráfico en texto plano entre la conexión del cliente y el servidor.

Romero (2015), también, existen herramientas metodológicas que están encargadas de automatizar análisis de pentesting en aplicaciones web, proyectos enfocados en escanear, atacar e informar los problemas de seguridad de los servicios que trabajan bajo el protocolo HTTP como: OWASP, Nessus, Metasploit, Arachni, Burp, OpenVast, w3af, Acunetix, entre otras. OWASP (2013), estos proyectos poseen cualidades importantes en cross-site scripting (XSS), inyección de SQL, OS y LDAP, pérdida de autenticación y gestión de sesiones, referencias directas de objetos inseguros, exposición de datos sensibles, ausencia de control de acceso a funciones, Cross-site request forgery (CSRF), utilización de componentes con vulnerabilidades conocidas, redirección y reenvió no válidos, denegación de servicios, entre otros. Informando los problemas de seguridad, el nivel de riesgo que posee y documentación de las posibles soluciones.

Revisando la literatura se observa que existen vulnerabilidades en los protocolos de seguridad web que pueden ser identificadas por herramientas de pentesting y que son aprovechadas por ataques informáticos automatizados que son desarrollados por científicos, con la finalidad de realizar ataques informáticos que pueden afectar la disponibilidad del servicio web de las plataformas que posee GRUPO NETHEXA S.A.S, por lo que la organización identifica la necesidad de tener un plan de gestión de seguridad informática que integre y cubra los servicios web de plataformas de e-learning y de telefonía IP, con el propósito general de poder mitigar o minimizar el riesgo informático que poseen todas las aplicaciones web de la organización, por lo que se realiza un proyecto de seguridad que permite gestionar constantemente los riesgos de seguridad encontrados.

Existen métodos y normas de buenas prácticas de seguridad de la información, que orientan a las organizaciones a gestionar el riesgo informático a través de la administración de políticas y procesos informáticos que se alinean a las estrategias y al gobierno de las empresas, cuya prioridad es asegurar y tener disponibilidad de todos los sistemas de información TIC que mantienen la continuidad del negocio de toda organización que GRUPO NETHEXA S.A.S desea adaptar. En la investigación se encuentran diferentes metodologías Nacionales e Internacionales que pueden ser adaptadas por la empresa como lo son el Modelo de Seguridad y Privacidad de

la Información Colombiano (MSPI), MAGERIT, OCTAVE, CRAMM, EBIOS, MAHARI Y O-ISM3, orientando a las organizaciones en la implementación de gestión de análisis de riesgos y en la gestión de los sistemas de información, siguiendo los lineamientos de las normas ISO 27001:2013 y la ISO/IEC 27005:2008.

Torres & Rojas (2017), OCTAVE es una metodología utilizada para la evaluación y gestión de riesgos con el propósito de que las organizaciones puedan realizar gestión de activos, conocer posibles amenazas y evaluar las vulnerabilidades que poseen, garantizando la seguridad de los sistemas de información siguiendo los lineamientos del estándar internacional ISO 27001.

MEHARI (2010), MEHARI proporciona un método de evaluación y gestión de los riesgos cualitativos y cuantitativos, siguiendo los requerimientos de la norma ISO/IEC 27005:2008, proporcionado un conjunto de herramientas y bases de datos de conocimiento necesarios para la adaptación del método.

EBIOS (2003), EBIOS es un método que permite apreciar e identificar los riesgos de seguridad en los sistemas de información (SSI), proporcionando las justificaciones necesarias en la toma de decisiones como una herramienta de negociación. No se trata solo de un método de SSI, sino también de una herramienta de software libre que ayuda al diseño de proyectos asociados al campo de gestión de riesgos informáticos.

Torres & Rojas (2017), MAGERIT es una metodología de análisis y gestión de riesgos de los sistemas de información relacionados con la seguridad de las TIC, elaborado por el Consejo Superior de Administración Electrónica para dar respuesta a las necesidades de administración de TIC que depende de la seguridad, con el propósito de que la sociedad tenga un crecientemente de las tecnologías de la información y pueda cumplir con la misión de los deberes personales y empresariales, beneficiando a las organizaciones que lo implementan minimizando los riesgos seguridad adaptando medidas que generen confianza.

CRAMM (2002), CRAMM es una herramienta utilizada para el análisis y gestión de riesgos cualitativos desarrollados por la Agencia Central de Computación y Telecomunicaciones del Gobierno del Reino Unido en 1985, proporcionado a departamentos gubernamentales un método para la supervisión de seguridad en los sistemas de información. CRAMM puede ser utilizado en todo tipo de organización, con el fin de justificar las inversiones de seguridad y de contingencias en sistemas de información y redes de telecomunicaciones, demostrando la importancia de realizar gestión con resultados cuantificables y contramedidas a implementar luego del análisis de riesgos, dando cumplimento al estándar Británico BS7799 identificando y valorando los activos de la organización, identificando amenazas y vulnerabilidades, calculando los riesgos y priorizando e identificando las contramedidas.

MSPI (2017), Modelo de seguridad y privacidad de la información colombiano (MSPI) se encuentra alineado con el marco referencial de Arquitectura de TI soportando transversalmente los componentes estratégicos en servicios de TIC, gobierno Abierto de TIC y Gestión de TIC. El modelo está acorde con los lineamientos de buenas prácticas de seguridad y es actualizado periódicamente con las mejoras que se van adquiriendo, reuniendo los cambios que se realizan en la norma ISO 27001:2013, la legislación de ley en la protección de datos personales, transparencia y acceso de la información pública, las cuales son importantes para la gestión de la información. El MSPI cuenta con una serie de guías anexas que ayudan a todas las entidades en cumplir las buenas prácticas de seguridad de la información, permitiendo abordar cada una de las fases que brinda el modelo, buscando comprender los resultados a obtener y cómo desarrollarlos, incluyendo los nuevos lineamientos que permitan la adopción del protocolo de enrutamiento IPv6 en todo el estado colombiano.

O-ISM3 (2017), O-ISM3 es un estándar de madurez que define los procesos de seguridad, con el fin administrar el sistema de gestión de seguridad de la información (ISMS) de las organizaciones. O-ISM3 asigna las responsabilidades al negocio empresarial en definir los objetivos de seguridad en políticas, ofreciendo un conjunto de procesos administrativos en seguridad donde el negocio selecciona como implementar un ISMS coherente para poder alcanzar todos los objetivos de seguridad del negocio.

El proyecto O-ISM3 ha sido probado con diferentes estándares como CMMI, ISO 9001, COBIT, ITIL, ISO 27001, entre otros; hallando mejoras considerables en los campos de aplicación vinculando las necesidades del negocio, utilizando un enfoque basado en procesos proporcionando detalles adicionales en la implementación y sugerencias de métricas preservando la compatibilidad de los estándares actuales de administración en seguridad y TIC. El estándar es llamativo para la solución del trabajo de grado, ya que GRUPO NETHEXA S.A.S no tiene un sistema de gestión de seguridad de la información que pueda ser compatible con procesos de ISO 27001, ITIL y COBIT, que sea ágil de implementar, económico ya que se facilita en adaptarse en empresas de tienen recursos limitados y es compatible con los estándares más utilizados en las organizaciones, a las que le presta el servicio de TIC.

En el proyecto de maestría pretende implementar el sistema de gestión integral de seguridad informática en servicios web de e-learning y telefonía IP en GRUPO NETHEXA S.A.S, con el fin de poder utilizar una metodología que permita establecer procesos y políticas que permitan realizar una evaluación en seguridad web constante en la organización, con el objetivo de no afectar la disponibilidad del servicio web de los clientes. A través de, identificación de vulnerabilidades existentes informáticas a aplicaciones HTTP que pueden ser explotadas en los servicios web de e-learning y telefonía IP en GRUPO NETHEXA S.A.S. Con el fin de administrar y controlar el riesgo de las vulnerabilidades críticas adaptando

controles de seguridad que ayuden a mitigar y a minimizar el riesgo informático de los servicios web de la organización, contribuyendo en la mejora de la continuidad del negocio reduciendo los problemas de seguridad informática.

METODOLOGÍA

Para alcanzar los objetivos planteados, y brindarle a GRUPO NETHEXA S.A.S el conocimiento necesario para analizar las vulnerabilidades que afectan la seguridad en los servicios web de e-learning y telefonía IP. Se adaptó un sistema de gestión integral de seguridad informática que está encargado de reducir y/o mitigar los problemas de seguridad de los servicios web de la organización. El sistema de gestión integral de seguridad informática e realizó en tres fases:

Fase 1. Selección del modelo de gestión de seguridad de la información orientado la auditoría de seguridad en los servicios web de e-learning y telefonía IP.
Se analizaron los sistemas de gestión de seguridad y riesgos más populares en el mercado y se definió el modelo de seguridad de la información es O-ISM3 para la empresa, el cual permitió establecer los procesos y políticas estratégicas, tácticas y operativas ayudando al área de seguridad informática en implementar controles de seguridad y auditoria para el mejoramiento continuo del aseguramiento de los activos de información, evaluando y mitigando las vulnerabilidades.

Fase 2. **Determinación de las vulnerabilidades críticas que poseen los servicios web de e-learning y telefonía IP.**
Se defino el reporte de las vulnerabilidades identificadas en los activos de información de los servicios de e-learning y telefonía IP, donde se realizó el análisis de riesgos de los recursos que poseen los productos web con las diferentes áreas de la organización, informando las manazas y vulnerabilidades criticas valoradas tras la oportunidad y el impacto que puede afectar a la empresa en la materialización de un intendente de seguridad. El reporte realizado contiene la siguiente información importante:

- Resultados del escaneo de vulnerabilidades a los servicios web de la organización.
- Amenazas y vulnerabilidades identificadas en la investigación de los problemas de seguridad que poseen los activos de información de los servicios web de la organización.
- Resultado del análisis de riesgos realizado por las áreas interesadas de la seguridad informática de la organización, identificado los riesgos a los que se les deben de realizar un tratamiento.

Fase 3. Adaptar controles de seguridad que permitan disminuir el impacto de los ataques informáticos en los servicios web de e-learning y telefonía IP en la organización.
Con la obtención de los resultados de las vulnerabilidades críticas identificadas en el análisis de riesgos, es necesario adaptar los controles de seguridad en los servicios web de la organización, donde se crea una serie de documentos que

proporcionan las pautas de seguridad necesarias para la implementación de los controles y buenas prácticas de seguridad informática.

- Determinación de los controles que mitiguen el impacto de la materialización de las vulnerabilidades y riesgos identificados.
- Diseño de los controles de seguridad que deben ser implementados.
- Documentación del análisis de los controles y la configuración de buenas prácticas de seguridad.

4 RECURSOS UTILIZADOS

Los recursos utilizados para la implementación de los controles establecidos en el sistema de gestión integral de GRUPO NETHEXA S.A.S. Fueron tecnológicos y personas que intervinieron en el trabajo de grado de Maestría.

Personas que intervinieron:

INVESTIGADOR / ASESOR	FORMACIÓN ACADÉMICA	FUNCIÓN DENTRO DEL PROYECTO	DEDICACIÓN (h/sem)
Sebastián Restrepo	Ingeniero	Investigador	10
Juan Camilo Estrada	Ingeniero	Asesor Temático	2
Julián Gutiérrez	Ingeniero	Asesor Técnico	2
John Fernando Vargas	Doctor	Director	2

Recursos Tecnológicos

EQUIPOS/SOFTWARE	JUSTIFICACIÓN
Portátil	Equipo utilizado por el investigador dentro de las políticas de la empresa, para realizar el trabajo de grado.
Servidores Virtuales y servidores en la Nube	Máquinas virtuales de pruebas proporcionadas para realizar el análisis y escaneo de vulnerabilidades.
HexaDialer	Acceso a todos los recursos de la aplicación de marcado predictivo.
HexaHUD	Acceso s todos los recursos de la aplicación de gestión de llamadas entrantes.
Plataforma e-learning	Acceso a todos los recursos de las plataformas de educación virtual.

5 PRESENTACIÓN Y ANÁLISIS DE RESULTADOS

5.1. Objetivo 1: Seleccionar un modelo de gestión que oriente el proceso de auditoría de seguridad en los servicios web de e-learning y telefonía IP en la organización.

Después de hacer un análisis de las opciones existentes, GRUPO NETHEXA S.A.S adopta el sistema de gestión de seguridad de la información O-ISM3, la empresa se acoge al modelo tras realizar un análisis de los beneficios; teniendo la necesidad de tener un grado alto de madurez en seguridad, siguiendo los procesos y políticas de mejoramiento continuo de la seguridad información, buscando mejorar los objetivos estratégicos en la prestación de servicios web en las aplicaciones de e-learning y telefonía IP.

El propósito fundamental es formar la seguridad informática como área que vele por la gestión de seguridad en las aplicaciones web prioritarias como los son e-learning y telefonía IP de manera integral, con el objetivo de que todas las políticas apoyen una adecuada gestión de riesgos, vulnerabilidades, controles y auditoría en seguridad informática, brindando un cumplimiento normativo a las áreas relacionadas que posean desarrollos web de los servicios de e-learning y telefonía IP. El área de seguridad formada, es capaz de administrar y tener una visión estratégica del negocio, para monitorear, operar, prevenir y responder a los incidentes de seguridad informáticos de los servicios prestados a los clientes, mejorando la seguridad, disponibilidad y continuidad del servicio.

El principal objetivo de NETHEXA es mejorar cada día los servicios que presta a las organizaciones, ya que se ha encargado de invertir en estabilizar la operación de las plataformas que posee, haciendo a un lado la seguridad de los servicios que maneja. Por esa razón, la organización adopta O-ISM3 como SGSI; con la finalidad de, ayudar a la mejora de la seguridad de las aplicaciones web, las cuales poseen los servicios más críticos y que son un diferenciador importante en el mercado en la prestación de servicios de telecomunicaciones (e-learning y telefonía IP).

Las metas y los objetivos para NETHEXA son primordiales; por este motivo, la mejora de los aplicativos que posee y la fidelización de los clientes, es lo más importante para la organización. Actualmente, los clientes y los nuevos proyectos que surgen están solicitando que los servicios prestados posean una adecuada gestión de seguridad de la información, por lo que adoptar el SGSI es vital para la continuidad del negocio de la empresa en el futuro, por esta razón se deben mejorar los servicios de seguridad actuales, dando valor agregado a todos los clientes con un servicio seguro que genere confianza y trasparencia.

GRUPO NETHEXA S.A.S se acoge a O-ISM3, por ser un SGSI que maneja métricas que pueden llegar a un nivel alto de madurez de seguridad informática, al ser una

metodología que puede integrar estándares y métodos de seguridad de la información, gerencia y administración de buenas prácticas de TIC y análisis de riesgos. Adaptando el diseño, implementación y monitoreo del SGSI, enfocando los lineamientos genéricos, estratégicos, tácticos y operacionales de la metodología, los niveles son implementados a través de diferentes procesos de seguridad, los cuales son interrelacionados con otros procesos y políticas, permitiendo la evaluación por medio de métricas y la adaptación de estándares y metodologías de seguridad informática; y de análisis de riesgos.

La estructura general del modelo de seguridad O-ISM3 donde se visualizan los procesos necesarios para la adaptación del SGSI de GRUPO NETHEXA S.A.S, se observar en la figura 1:

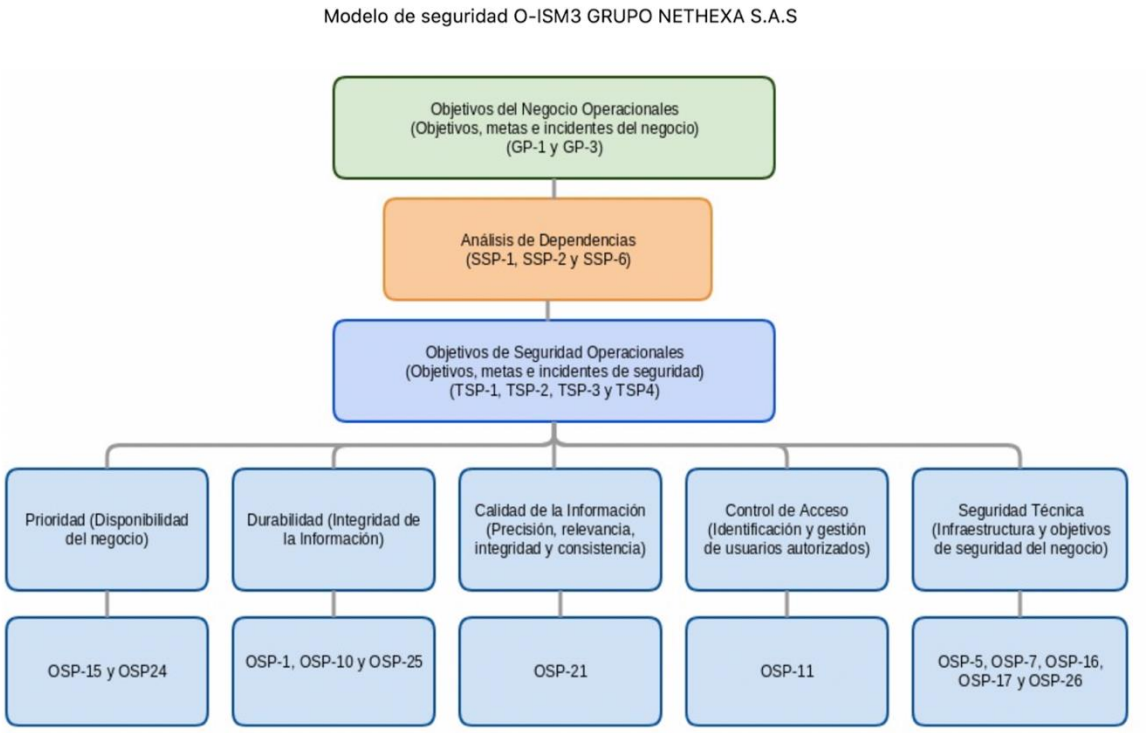


Figura 1: O-ISM3 (2017) Contexto del modelo de seguridad O-ISM3 de GRUPO NETHEXA S.A.S. Fuente: Sebastián Restrepo.

El objetivo fundamental de O-ISM3 es impedir la exposición de los activos de información como objetivo de seguridad para la organización, definiendo desviaciones tolerables, que puedan dar continuidad al negocio cuando ocurren problemas de seguridad que afectan la disponibilidad de los servicios web de e-learning y telefonía IP; con el fin de, prevenir y mitigar los incidentes que ponen en riesgos la integridad de la organización en la salida de productos y servicios que se basan en el funcionamiento de los sistemas de información. Por este motivo, la

metodología proporciona tres niveles para la gestión de seguridad de la información, ayudando a la empresa en la reducción de riesgos y confianza, optimizando el uso de la información, dinero, gente e infraestructura. Estos niveles son los siguientes:

- **Estratégico:** Se ocupa de establecer los objetivos generales, donde se toman decisiones de la coordinación y dotación de recursos para el área de seguridad informática.
- **Táctico:** Encargado de diseñar e implementar el SGSI, establecer los objetivos específicos y gestionar los recursos proporcionados por la organización.
- **Operativo:** Se ocupa del seguimiento de los objetivos definidos; por medio de, procesos técnicos establecidos por las áreas superiores, donde se encargan de ejecutar y reportar los resultados de los procesos.

Como se muestra en la figura 2, podemos observar los niveles de seguridad que tendrá la empresa que soportará toda la seguridad informática de los sistemas de información de los servicios web.

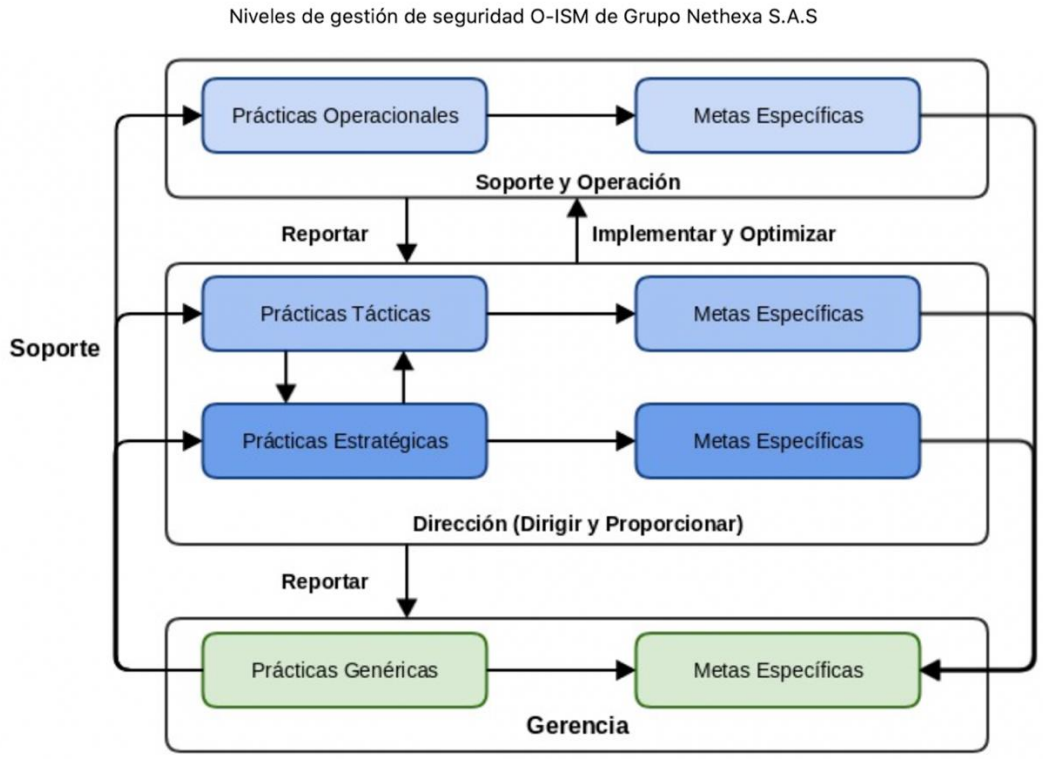


Figura 2: O-ISM3 (2017), Niveles de Gestión de Seguridad O-ISM3 en GRUPO NETHEXA S.A.S. Fuente: Sebastián Restrepo.

Como GRUPO NETHEXA S.A.S es una empresa Pyme, se toma la decisión de unir los niveles estratégicos y tácticos, con el fin de abordar todos los procesos, métricas

y responsabilidades por las áreas que se encuentran establecidas actualmente en la empresa.

Los estándares de buenas prácticas de gestión de seguridad de la información y de TIC como ISO 27001, ISO 27002, BIA, ITIL y COBIT, ayudan a la organización a alinear la metodología de gestión de la seguridad de la información ISM, cumpliendo con la metodología O-ISM3 como SGSI.

GRUPO NETHEXA S.A.S adapta la metodología propuesta, alineada con los objetivos y metas de la organización, mejorando la disponibilidad de los servicios prestados a los diferentes clientes que poseen, asegurando los servicios que suministra consiguiendo nuevos clientes potenciales que permitan una continuidad del negocio a través del tiempo.

Establecer y mantener el SGSI es uno de los principales objetivos para GRUPO NETHEXA S.A.S planteado desde el gobierno de TIC, abarcando la auditoría y el cumplimiento de las buenas prácticas de seguridad informática, permitiendo la mejora continua y la disponibilidad de los servicios de TIC implementados y administrados por la organización. Por este motivo, la empresa establece y se compromete en cumplir con la política del sistema de gestión de seguridad de la información, con la finalidad de satisfacer las necesidades, alcance, objetivos y metas de seguridad informática adoptadas.

- **Metas del SGSI**

  - Mejorar la disponibilidad de los servicios prestados por la organización constantemente.
  - Brindar continuidad del negocio a la empresa, mejorando la reputación corporativa implementando seguridad en los servicios prestados.
  - Dar cumplimiento a la norma de seguridad colombiana, en la implementación del SGSI que permita asegurar los activos de información.

- **Objetivos del SGSI**

  - Implementar sistema de gestión de seguridad de la información, que permita gestionar continuamente la seguridad informática.
  - Gestionar el riesgo asociado a los activos de información que contienen los servicios web.
  - Adoptar controles de seguridad que permitan reducir los riesgos informáticos y mitigar proactivamente las amenazas que poseen los servicios web.
  - Brindar un soporte eficaz y oportuno ante incidentes de seguridad informática.

- **Métricas del SGSI**

  - Porcentaje de cumplimiento de las metas y los objetivos de seguridad informática.
  - Nivel de cumplimiento de los procesos establecidos por el SGSI.
  - Número de eventos de seguridad mitigados proactivamente con los controles de seguridad establecidos.
  - Número de incidentes de seguridad mitigados por el equipo de soporte de seguridad informática.
  - Tiempo de interrupción de los servicios web de la organización por incidentes de seguridad informática y de TIC.
  - Conformidad de los clientes en el cumplimiento de los niveles de servicios pactados.

- **Niveles de servicio SLR y SLA**

Para GRUPO NETHEXA lo más importante en la prestación de servicios, es la disponibilidad del funcionamiento de los aplicativos web que poseen con los clientes que consumen el servicio de e-learning y telefonía IP. Por este motivo, es de suma importancia acoger los niveles de servicios pactados entre el cliente y la organización para darles el debido cumplimiento; con el propósito de, reducir los problemas legales que se pueden presentar por el incumplimiento de la disponibilidad de servicios que se tienen a nivel contractual.

La empresa se acoge al proceso y/o política de la gestión de niveles de servicio (TSP-4) del modelo del SGSI, cumpliendo con los objetivos principales en la prestación de servicios, la cual es mejorar constantemente la disponibilidad de los servicios web prestados a los diferentes clientes de la organización.

- **Políticas Corporativas**

  - Tener la capacidad de atender todos los requerimientos en el área de telefonía IP, infraestructura de TIC, plataformas de e-learning y seguridad informática en el menor tiempo posible.
  - Generar valor agregado a nuestros clientes en la prestación de servicios estables.
  - Brindar una excelente atención a nuestros usuarios, en la agilidad de la solución de problemas informáticos que puedan presentar los servicios proporcionados.
  - Asesoría continúa en los reportes generados por el área de soporte del funcionamiento y problemas que se han presentado en los servicios de TIC con la organización; con el fin de, tomar decisiones estratégicas para mejorar la disponibilidad del servicio.

- **Políticas de seguridad SGSI** (**Cardoso**, **2014**)**.**

  - **Gestión del conocimiento.**

    La política se encargará de reunir, analizar, almacenar, comunicar y compartir el conocimiento dentro de la organización, con el objetivo de obtener valor sobre la información de las soluciones brindadas a todos los clientes que poseen servicios web de la empresa. Mejorando la eficiencia, reduciendo los tiempos de soporte y disminuyendo la necesidad de volver a adquirir conocimientos de los procesos realizados a los clientes. El proceso encargado de hacer cumplir la política es GP-1 Gestión del conocimiento, encontrado en el Anexo 1.

  - **Gestión de riesgos.**

    Política encargada de identificar y mitigar los posibles riesgos que poseen los activos de información, realizando un seguimiento adecuado al proceso actual (GP-3 Diseño y evaluación del SGSI), adoptando la metodología Magerit encargada de analizar y gestionar el riesgo de los sistemas de información relacionados con la seguridad de las tecnologías de la información y la comunicación. La organización necesita cuidar la inversión que se ha realizado en los activos de información, por este motivo es necesario identificar los riesgos que impidan el retorno de la inversión y la reputación en el medio empresarial. La información del análisis de riesgo se encuentra en el Anexo 2.

  - **Reporte e informes de seguridad del comité de gerencia.**

    La política se encarga de establecer el reporte e informes periódicos que son generados a todas las partes interesadas de la organización en la seguridad informática, con el objetivo de verificar el cumplimiento de los procesos, objetivos y metas establecidas por el área de gestión de seguridad; con el fin de, mejorar continuamente el SGSI tomando decisiones acertadas por la alta dirección de la empresa. Los procesos encargados para hacer cumplir la política son SSP-1 Reporte a las partes interesadas (Anexo 3), TSP-1 Informe de gestión estratégica (Anexo 6) y OSP-1 Informe de gestión táctica (Anexo 10), revisando todos los procesos del SGSI.

  - **Coordinación de las áreas de trabajo.**

    La política establece la comunicación entre los líderes de la empresa y el área de seguridad. Teniendo una coordinación acertada y estratégica de las funciones y responsabilidades de los líderes de la empresa y el área de seguridad; con el fin de, apoyar transversalmente a todas las áreas para alcanzar los objetivos y optimizar los recursos de la organización. El proceso

encargado es el SSP-2 Coordinación encontrado en el Anexo 4.

- **Gestión de recursos de seguridad.**

  Política encargada de administrar los recursos proporcionados por la empresa, brindado una adecuada gestión de los procesos de gestión tácticos y operativos del SGSI, asignando el presupuesto al área de seguridad informática. Los procesos encargados de hacer cumplir la política son SSP-6 Asignación de recursos para la seguridad de la información (anexo 5) y TSP-2 Administración de recursos asignados (Anexo 7).

- **Metas y objetivos de seguridad.**

  Política encargada de establecer las metas y los objetivos de seguridad, en la mejora continúa de la estrategia aplicada al SGSI del negocio, madurando constantemente los procesos y estándares asociados a la seguridad de las tecnologías de la información y la comunicación. El proceso encargado de cumplir con la política es TSP-3 Definición de metas y objetivos de seguridad encontrada en el Anexo 8.

- **Gestión de los niveles de servicio.**

  Política encargada de alinear los procesos ISMS con los acuerdos de niveles de servicio que provee la organización con los diferentes clientes, proporcionado disponibilidad y continuidad de los servicios, en la ejecución de los procesos e incidentes de seguridad en los activos de información. El proceso que permite el cumplimiento es el TSP-4 Gestión de niveles de servicios encontrada en el Anexo 9.

- **Gestión de inventario de activos.**

  Política encargada de hacer cumplir el proceso OSP-3 Gestión de inventario de activos (Anexo 11), identificando los activos de información que poseen los servicios web de e-learning y telefonía IP en la organización. Levantando información importante del activo de información que permita documentar la identificación del activo con su respectiva categoría, etiqueta, nombre y criticidad en la disponibilidad del servicio.

- **Gestión de cambios de seguridad.**

  Política encargada de prevenir y gestionar los incidentes relacionados a los cambios de seguridad que son ejecutados a los activos de información de TIC. El proceso encargado de autorizar los cambios formales de seguridad informática en la organización es el OSP-4 Seguridad en gestión de cambios, encontrado en el Anexo 12.

- **Actualizaciones de seguridad.**

  La política autoriza y controla las actualizaciones de los sistemas y aplicativos, previniendo incidentes de seguridad y la explotación de vulnerabilidades, por la utilización de sistemas y aplicativos desactualizados. El proceso encargado de cumplir con las actualizaciones de seguridad que surgen en el tiempo es OSP-5 Actualizaciones de seguridad, encontrado en el Anexo 13.

- **Gestión de controles de seguridad.**

  Política encargada de gestionar la implementación de los controles de seguridad que mejoran la confiabilidad, integridad y disponibilidad de los activos de información de TIC de los servicios web de la organización. El proceso encargado de dar cumplimiento es OSP-7 Endurecimiento de activos gestionados de TIC, encontrado en el Anexo 14.

- **Gestión de copias de seguridad.**

  La política se encarga de gestionar las copias de seguridad que se realizan a los activos de información de TIC de los servicios web de la organización, reduciendo el impacto de la perdida de información, cumpliendo con los niveles de servicios acordados en la restauración de copias de seguridad, en la pérdida parcial o total de los activos de información ante incidentes de seguridad. El proceso encargado es OSP-10 Gestión de copias de seguridad, encontrado en el Anexo 15.

- **Gestión de la continuidad de las operaciones.**

  Política encargada de proporcionar redundancia y eliminación de puntos críticos de falla, reduciendo el impacto que pueden generar los incidentes negativos en la imagen corporativa de la organización, acortando los tiempos de respuesta ante incidentes que afectan los activos de TIC de los servicios web. El proceso encargado es OSP-15 Gestión de continuidad de operaciones, encontrado en el Anexo 16.

- **Gestión de tráfico de red.**

  Política encargada de gestionar el tráfico de red autorizado y no autorizado que ingresa y sale de los activos de información de los servicios web de la organización, filtrando el tráfico innecesario que consume los recursos de la red, los cuales pueden afectar el acceso del servicio a nuestros clientes. El proceso encargado de controlar el tráfico de red es OSP-16 Gestión de tráfico de red, encontrado en el Anexo 17.

- **Gestión de protección contra malware.**

  Política encargada de imponer las medidas de seguridad necesarias para proveer protección contra amenazas de seguridad como virus, spyware, troyanos, backdoors, key loggers, rootkits, ataques persistentes avanzados, entro otros servicios no autorizados que afecten la disponibilidad de los servicios web de los activos de información de la organización. El proceso encargado es OSP-17 gestión de protección contra Malware, encontrado en el Anexo 18.

- **Calidad de información y evaluación de cumplimiento.**

  Política encargada de la auditoría del SGSI, gestionado la revisión periódica de la información de seguridad; con el propósito de, garantizar que es completa, exacta y actualizada, cumpliendo con las políticas y procesos establecidos por la organización. Con el objetivo de reducir los incidentes de seguridad que son ocasionados por la mala clasificación de la información, a nivel de completitud, exactitud y expiración, a través de un proceso de auditoría. El proceso encargado es OSP-21 Calidad de información y evaluación de cumplimiento, encontrado en el Anexo 19.

- **Gestión de incidentes.**

  Política encargada de contener y mitigar el impacto generado por los incidentes de seguridad materializados en los activos de información de los servicios web de la organización. El proceso encargado es OSP-24 Gestión de incidentes, encontrado en el Anexo 20.

- **Gestión de disponibilidad de infraestructura crítica.**

  Política que provee un conjunto de medidas de seguridad basadas en la redundancia, diversidad y dispersión, con el fin de eliminar puntos de falla y reducir el impacto en la pérdida de la infraestructura crítica de seguridad. Cumpliendo con los niveles de servicios pactados, reduciendo el tiempo de indisponibilidad de los activos de información de TIC de los servicios web de la organización. El proceso encargado es OSP-26 Gestión de disponibilidad y fiabilidad de infraestructura crítica, encontrado en el Anexo 21.

- **Análisis de impacto del negocio (BIA)**

BIA (2015) La organización debe implementar una gestión del plan de continuidad del negocio, para poder responder a las políticas de seguridad de la información que apoyan la disponibilidad del servicio de TIC en el restablecimiento de actividades y servicios de las plataformas web que se

encuentran en operación en la empresa, apoyando el correcto funcionamiento de las infraestructuras de TI, minimizando las interrupciones y fallas en el servicio.

El plan de continuidad del negocio apoyará transversalmente a las políticas OSP-12 (Gestión de continuidad de operaciones), OSP-24 (Gestión de incidentes) y OSP-26 (Gestión de disponibilidad y fiabilidad de infraestructura crítica), monitoreando e identificando las amenazas de seguridad crítica que afecten la operatividad de los servicios y sistemas de información, garantizado la continuidad del negocio teniendo mecanismos de recuperación que respaldan la continuidad del servicio ante problemas de seguridad que generen interrupciones al servicio.

- **Ciclo de vida de seguridad informática**

ISO 27001 (2013) Para la organización es importante tener una constante revisión de todo el SGSI, por lo que establece un ciclo de vida que permite el cumplimiento y mejora de las políticas y procesos de seguridad informática, madurando la metodología planteada. En la figura 3 podemos observar los estándares que recorren el ciclo de vida del SGSI:

Ciclo de vida de la seguridad informática de Grupo Nethexa S.A.S.

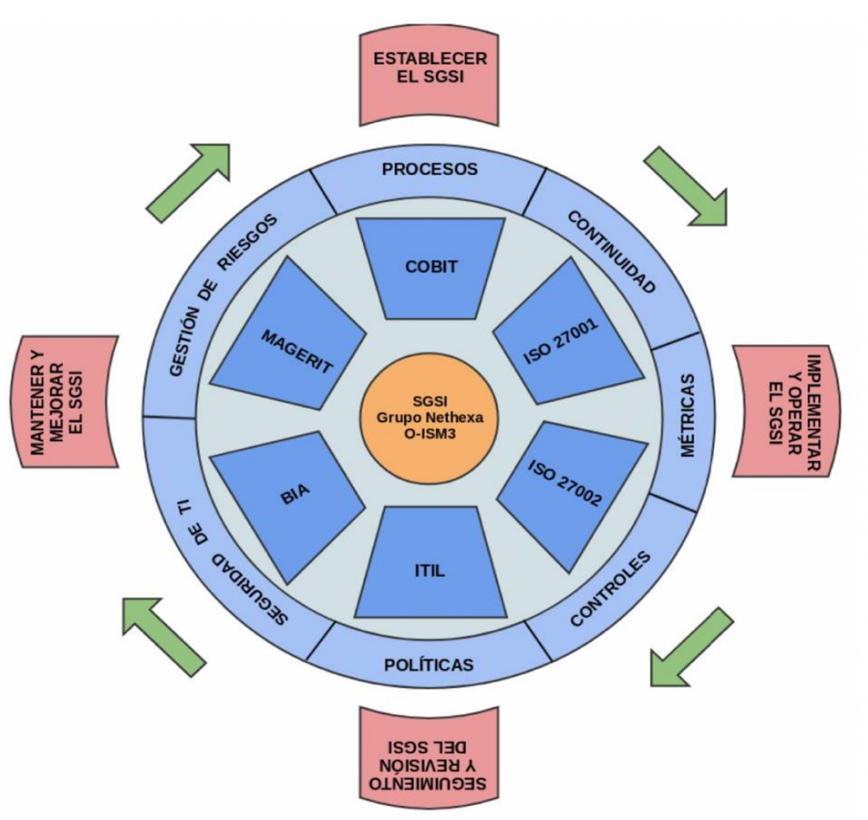


Figura 3: ISO 27001 (2013), ciclo de vida de seguridad informática de GRUPO NETHEXA S.A.S. Fuente: Sebastián Restrepo.

5.2. Objetivo 2: Determinar las vulnerabilidades críticas que poseen los servicios web de e-learning y telefonía IP en la organización.

❖ Gestión de Riesgos

MAGERIT_V3 (2012), la organización adopta las buenas prácticas de la norma de gestión de riesgos establecida en la ISO 31000, por este motivo se acoge a la metodología de implementación de gestión de riesgos Magerit, la cual permite tomar decisiones al gobierno de TIC en la aceptación, tratamiento y transferencia del riesgo de la empresa.

Los riesgos que poseen los activos de información son identificados a través de herramientas de escaneo de amenazas y vulnerabilidades con: Nessus (Escaneo avanzado y completo del servidor) y Owasp Zap (Escaneo de vulnerabilidades web), aunque también se realiza una investigación de estas para tener un panorama más completo de todos los problemas de seguridad que pueden afectar a los activos de información de la organización.

➢ Niveles de criticidad y tolerancia del riesgo de la organización

MSPI (2016), el propósito del nivel del riesgo es poder identificar cuáles son las amenazas que pueden impactar y/o perjudicar a la empresa en la continuidad del negocio; por este motivo, se crea una tabla con los valores críticos para la organización, con la finalidad de poder tomar decisiones ante los resultados de la valoración de las amenazas que pueden perjudicar a los activos de la organización, tomando decisiones estratégicas que permitan disminuir y/o mitigar las amenazas críticas.

		Impacto				
		Insignificante	Menor	Moderado	Mayor	Catastrófico
Probabilidad	Nivel	1	2	3	4	5
Raro	1	B	B	B	M	M
Improbable	2	B	B	B	M	A
Posible	3	B	B	M	A	A
Probable	4	B	M	M	A	A
Casi Seguro	5	M	M	A	A	A

Nivel de riesgo bajo: El riesgo es asumido por la organización.
Nivel de riesgo Medio: Se debe hacer un tratamiento del riesgo para

reducirlo.
Nivel de riesgo alto: Se hace un tratamiento del riesgo para reducirlo, evitarlo, compartirlo o transferirlo.

Para la organización todas las amenazas que se encuentren en el nivel riesgo alto no pueden ser tolerables, ya que el costo de la materialización de una de estas amenazas puede acabar con la organización y/o llevarla a la quiebra. Debido a que, el impacto que puede generar un incidente de seguridad alto afecta la economía y reputación de la empresa, en el mercado de prestación de servicios de TIC a nivel Nacional.

- **Valoración y análisis del riesgo**

Contiene todos los niveles de criticidad de los activos de información para la organización, con el propósito de realizar un cruce con las amenazas y la probabilidad de la ocurrencia e impacto en que pueda ocurrir la materialización de la amenaza, identificando cuales son los activos de información a los que se hace un tratamiento del riesgo y disminuyendo la probabilidad de que se puedan materializar las amenazas críticas que puedan afectar a la empresa económicamente y en el mercado de prestación de servicios de TIC.

- **Activos de Información**

MAGERIT_V3 (2011), se separan todos los servicios, aplicaciones, sistemas operativos, plataformas de virtualización, plataformas en la nube, hardware, información del servicio, medios de acceso y los activos intangibles. Con el propósito de extraer los activos esenciales los cuales son necesarios para que los servicios web puedan operar sin ningún inconveniente. En las figuras 5 y figura 6 podemos observar los activos de información de los servicios de e-learning y telefonía IP:

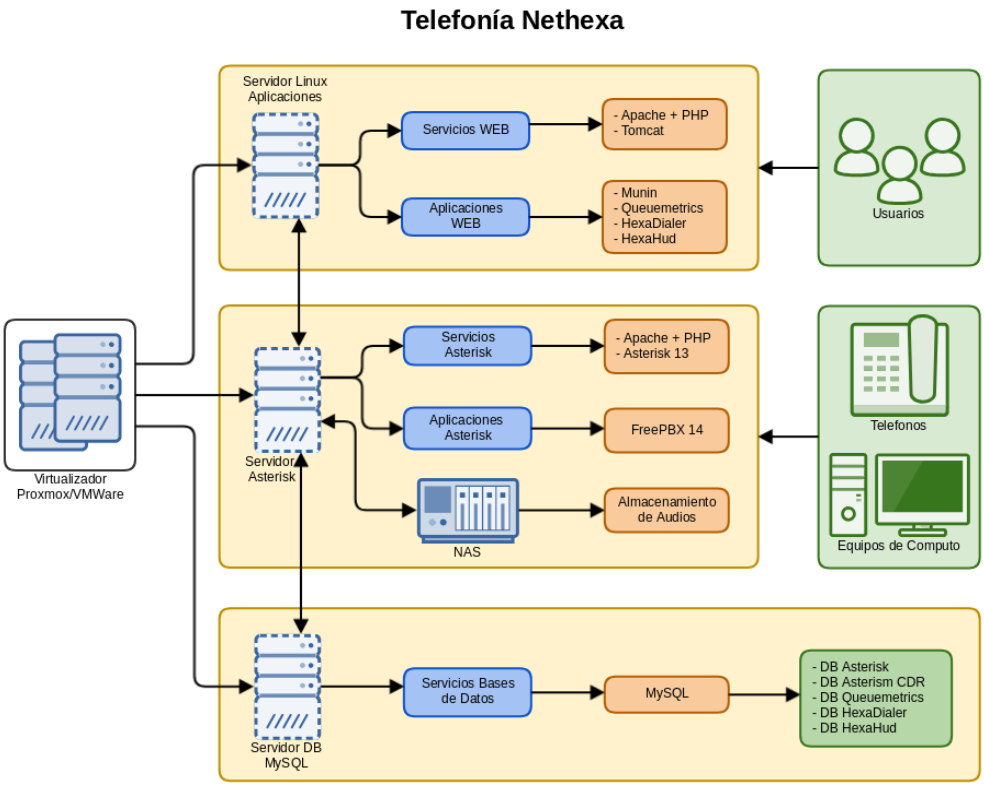


Figura 4: MAGERIT V3 (2011), activos de información telefonía IP NETHEXA. Fuente: Sebastián Restrepo.

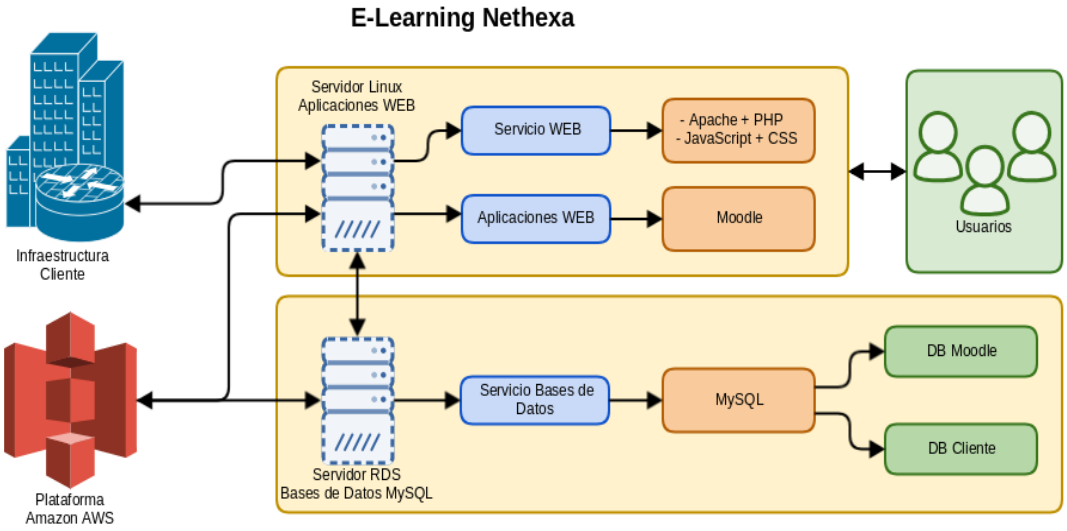


Figura 5: MAGERIT V3 (2011), activos de información e-learning. Fuente: Sebastián Restrepo.

- **Nivel del riesgo de las amenazas**

  Es el riesgo que posee el número de amenazas identificadas por el análisis de riesgo, donde se realiza un cruce de los activos de información y las amenazas y/o vulnerabilidades investigadas y escaneadas, donde se aplica el nivel de tolerancia y criticidad a los problemas de seguridad, verificando con las áreas encargadas del impacto y probabilidad que pueden causar la materialización de las amenazas en los activos de información de los servicios web de e-learning y telefonía IP. El porcentaje de número de amenazas lo podemos observar en la figura 6:

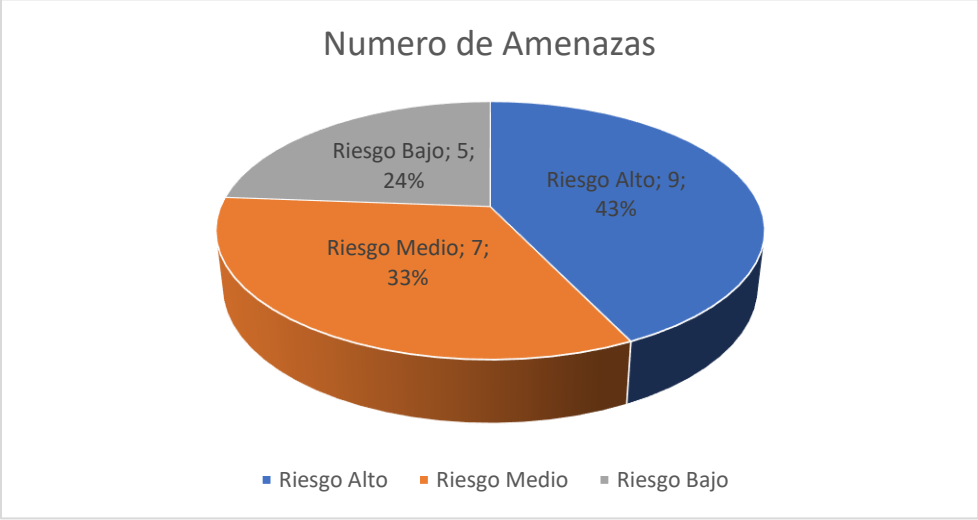


Figura 6: Número y nivel del riesgo de amenazas y/o vulnerabilidades. Fuente: Sebastián Restrepo.

Para consultar información detallada del nivel del riesgo de las amenazas, puede hacer revisión del anexo 2, en el Formato de valoración y análisis del riesgo.

- **Amenazas y vulnerabilidades analizadas**

  Son los problemas de seguridad que afectan la disponibilidad, integridad y confiabilidad de los activos de información.

Amenazas/Vulnerabilidades	Valoración Del Riesgo
Malware	Alto
Explosión de directorios y datos sensibles	Medio
Interceptación de información	Medio

DOS/DDOS	Alto
Pérdida de autenticación y gestión de sesiones	Bajo
Pérdida de control de acceso	Alto
Configuraciones de seguridad incorrectas	Alto
deserialización insegura	Bajo
Uso de componentes con vulnerabilidades conocidas	Alto
Registro y monitoreo insuficiente	Alto
Phishing	Medio
SQL injection	Alto
buffer overflow	Medio
Ataque día cero	Medio
cross-site scripting	Alto
Ataque de fuerza bruta	Medio
Robo de Información	Bajo
Man In The Middle	Alto
CSRF	Bajo
Envenenamiento de cookies	Bajo
Entidades XML(XXE)	Medio

Analizando la tabla proporcionada por la valoración del riesgo, la empresa hace el tratamiento del riesgo de las amenazas con valoración del riesgo Alto y Medio; con el objetivo de reducir el riesgo a un nivel bajo que pueda ser aceptable y tolerable para la organización, en la continuidad y disponibilidad de los servicios prestados en las plataformas WEB de e-learning y telefonía IP. Para consultar información detallada del análisis de riesgos, puede hacer revisión del anexo 22.

5.3. Objetivo 3: Adaptar controles de seguridad que permitan disminuir el impacto de los ataques informáticos en los servicios web de e-learning y telefonía IP en la organización.

- **Controles y buenas prácticas de seguridad**

Luego de realizar el análisis de riesgos, se hace el tratamiento de los riesgos altos y medios, con el propósito de reducir el nivel de riesgos que poseen los activos de información a través de las amenazas y vulnerabilidades identificadas. Con el propósito de mejorar la seguridad de los activos de información y acogiendo el SGSI implementado, se hace un diseño para que la empresa pueda implementar los siguientes controles de seguridad:

- **Actualizaciones de los activos de información.**

RedHat (2017), la aplicación de los parches de seguridad de los activos de información es de suma importancia, ya que la mayoría de las aplicaciones y servicios que contienen los servidores y equipos en red, poseen una instalación predeterminada que no es probada lo sufriente. Luego los servicios y las aplicaciones cuando se encuentran en producción, los fabricantes y desarrolladores empiezan a detectar los errores y problemas que presentan estas plataformas, donde se empieza a corregir y refinar el código al detalle mejorando la seguridad y eficiencia de los servicios y aplicaciones; por este motivo, la importancia de las actualizaciones constantes de todas las plataformas web de la organización.

Debían (2018), cuando se descubren las vulnerabilidades de seguridad en los servicios y aplicaciones que utilizan las plataformas web, se programa una actualización del software afectado de manera masiva en todos los servidores. Al encontrar una falla de seguridad en Linux, por lo general siempre viene acompañada de un parche de seguridad que soluciona los inconvenientes presentados, todos los paquetes y actualizaciones de seguridad se pueden obtener desde la página oficial de Debían, donde se encuentran todos los paquetes disponibles para las actualizaciones directas de los sistemas operativos. Par amas información consultar el Anexo 23.

- **Endurecimiento de los activos de información**

Linux_Trucepei_Blog (2017), todos los servidores web de la organización tiene que tener implementado la guía de mejores prácticas establecidas por el SGSI, donde se puede realizar el hardening de los servidores, asegurando los servicios que contienen localmente el servidor realizando actividades como: Escaneo de vulnerabilidades, tratamiento de vulnerabilidades y amenazas identificadas, aseguramiento de servicios intrínsecamente inseguros, seguridad en privilegios de usuarios, asegurar los puertos de red innecesarios e implementar buenas prácticas de configuración de las plataforma web. Para revisar la documentación de buenas prácticas por favor consultar en el anexo 25.

- **Copias de seguridad y continuidad de operaciones.**

Para la organización es de vital importancia la continuidad de las operaciones de los activos de información de las soluciones de e-learning y Telefonía IP de los productos desarrollados por GRUPO NETHEXA S.A.S. Como parte fundamental de la seguridad informática, es poder tener disponibles backups actualizados que permitan restablecer los servicios luego de sufrir un incidente de seguridad que dañe parcial o completamente los activos de información.

La empresa almacena los backups de la información y desarrollos que se

realizan específicamente a los clientes que se les presta el servicio de e-learning y telefonía IP, ya que la información que se almacenan con el tiempo de operación de las plataformas es un recurso que se protege y está siempre disponible a los usuarios que utilizan los servicios de la organización. Por este motivo, el almacenamiento es un factor crítico para los clientes, por lo que se realiza de manera interna y externa, dependiendo de la clase y el peso de su información, transportando los contenidos de manera segura.

Finalmente, tener presenta la implementación de: copias de seguridad de las maquinas en las nubes, copias de seguridad de las máquinas virtuales, alta disponibilidad y contingencia, transferencia de copias de seguridad y monitoreo, para mejorar la seguridad y continuidad los activos de información. Para más detalle de la información de copias de seguridad y continuidad de las operaciones revisar el Anexo 24.

- **Seguridad del tráfico de red.**

Define los controles de seguridad que se realiza a nivel perimetral de la red, los cuales obedecen a las políticas creadas en el SGSI. La finalidad de la seguridad perimetral del tráfico de red es poder tener una estandarización del tráfico que es permitido y rechazado en el establecimiento de la comunicación de los servicios de los usuarios y las plataformas web de cada cliente de los servicios de e-learning y telefonía IP.

El objetivo principal es poder otorgar seguridad, estabilidad, disponibilidad y eficiencia en la comunicación hacia los servicios web de las plataformas de los clientes, generando mayor seguridad y monitoreo de todas las conexiones que son realizadas a los servidores, reduciendo los riesgos identificados con la implementación de los servicios de seguridad: Segmentación y enrutamiento de red, Balanceo de cargas, Políticas de firewall, NAT, control de aplicaciones, calidad de servicio, Bloqueo de direccionamiento de países, Conexión segura IPSec , Conexión segura SSL, Protección contra ataques DoS y DDoS; y Cifrado de trafico de red DPI-SSL.

Los servicios de seguridad son implementados sobre un UTM de seguridad perimetral de última generación. Para revisar información detallada del proceso, revisar el anexo 26.

- **Protección contra malware y ataques dirigidos.**

Con el crecimiento de las TIC en el mundo, también se están reflejando los problemas de ciberseguridad en los activos de información que poseen las diferentes organizaciones, GRUPO NETHEXA S.A.S no se puede quedar atrás en la seguridad de los activos de información que proporcionan la seguridad de las plataformas web.

La protección contra código malicioso es vital para los activos de información, ya que se deben de mitigar todos los ataques de malware que lleguen a las plataformas web, mitigando o reduciendo el riesgo identificado en el análisis de riesgo.

SonicWall (2018), la finalidad de este documento es poder informar de la necesidad de los controles descritos en esta sección que tiene como objetivo fundamental, reducir el riesgo informático de los activos de información que puede ser causados por las amenazas descritas anteriormente. Los siguientes controles permiten implementar una seguridad más organizada, jerárquica y eficaz al momento de sufrir un incidente de seguridad: IPS/IDS, Gateway Antivirus y Antispyware, Sandboxing, Filtro de contenido, EndPoint, Web Application Firewall y Correlación de eventos.

Para más información detallada de la implementación del control y protección contra malware y ataques dirigidos, la pueden consultar el Anexo 27.

- **Diseño de seguridad de los servicios de e-learning y telefonía IP**

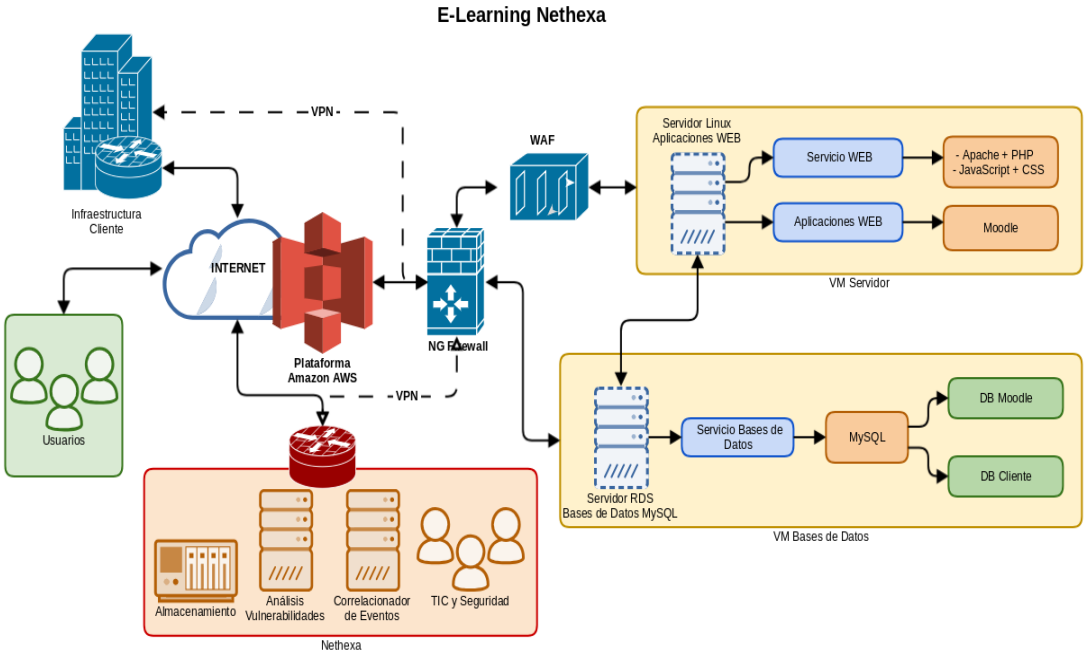


Figura 7: Diseño de seguridad de e-learning. Fuente: Sebastián Restrepo.

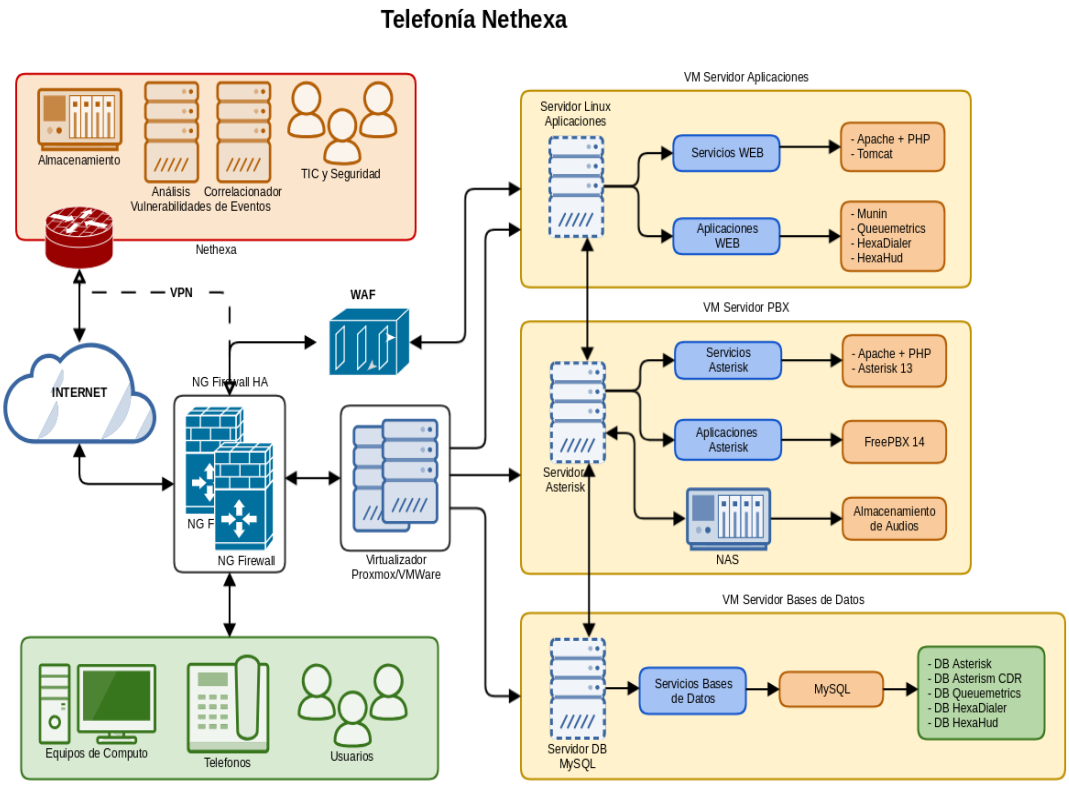


Figura 8: Diseño de seguridad de telefonía IP. Fuente: Sebastián Restrepo.

6 LIMITACIONES O DIFICULTADES

En el desarrollo se tuvieron varias limitantes presupuestales en la organización; por el motivo de que la empresa no cuenta con un presupuesto para implementar el área de seguridad informática. GRUPO NETHEXA S.A.S está haciendo todo el esfuerzo por destinar un recurso semestral para implementar controles de seguridad y está buscando la manera de tener un analista de seguridad que se encargue de realizar todos los procesos operativos del sistema de gestión de seguridad de la información en todos los servicios de e-learning y telefonía IP.

En la implementación del sistema de gestión de seguridad de información se tundieron inconvenientes con el tiempo de los asesores internos de la empresa, porque tenían las agendas muy ocupadas y no tienen el tiempo de revisar y planear la estrategia del SGSI, por lo que el primer objetivo tuvo un pequeño retraso que se puedo remediar unas semanas más adelante. Donde se definieron los procesos que adopta la organización para implementar el SGSI.

En el análisis de riesgos se tuvo también un pequeño retraso del desarrollo del segundo objetivo, ya que por el desconocimiento de la organización en seguridad informática se tuvo que realizar una investigación y explicación de los riesgos y las amenazas que poseen los activos de información de los servicios web de GRUPO NETHEXA S.A.S. Con el objetivo de poder dialogar el cruce del impacto y probabilidad de las posibles amenazas para llegar al resultado de los riesgos que son descartados y cuales deben de ser tratados.

En el último objetivo se tuvieron problemas con algunos accesos de las infraestructuras web de e-learning y telefonía IP, para revisar la seguridad y los escaneos que se realizaron para poder determinar los controles que se deben de realizar de acuerdo a la infraestructura que poseen los servicios. Retrasando un poco el trabajo que se estaba realizando.

Pese a las dificultades presentadas, se pudieron resolver todos los inconvenientes presentados con las personas encargadas, identificando y analizando todas las posibles mejoras que se pueden realizar a la infraestructura de los servicios web de la organización, agregando dispositivos de seguridad y mejorando los activos de información; con la finalidad de, poder prestar un servicio que proporcione seguridad a los clientes que utilizan estas plataformas. La empresa queda con una documentación que es exigida por muchos de los nuevos clientes que tienen implementado sistemas de gestión de calidad y de seguridad informática, los cuales exigen procesos de seguridad y buenas prácticas que permitan un excelente funcionamiento de las plataformas que está utilizando.

Con el desarrollo del trabajo, la empresa queda con el conocimiento de las mejoras que se deben de realizar en sus productos ofrecidos en cuanto a seguridad, para seguir mejorando cada día en la prestación de servicios web a los diferentes clientes que pueda tener.

7 CONCLUSIONES

Mediante la ejecución de este proyecto se define el estándar O-ISM3 como referente del sistema de gestión de seguridad de la información de la empresa GRUPO NETHEXA S.A.S, este se utilizará transversalmente en todas las plataformas web de los servicios de e-learning y telefonía IP que es ofrecido a los clientes; cumpliendo con los estándares de buenas prácticas de seguridad de la información y otros estándares de TIC que permiten tener disponibilidad en las aplicaciones que poseen los servicios web.

La empresa adquiere conocimientos de seguridad establecidos en procesos de madures, que permitan seguir mejorando constantemente los procesos del sistema de gestión de seguridad de la información, con el objetivo principal de tener un orden y una ideología clara en la administración y seguridad de los servicios web, que están implementados y son administrados en las plataformas Cloud y en los sistemas de virtualización de los clientes que adquieren los servicios.

Se realizó el diseño de la metodología de seguridad que proporciona la información necesaria para ejecutar las buenas prácticas de copias de seguridad, continuidad de operaciones, gestión de incidentes, actualización y hardening de los activos de información, que no se tenían presentes en los procesos de TIC en la organización, mejorando la seguridad, soporte y contención de los servidores que proporcionan las plataformas web. Generando políticas y procesos que son tenidos en cuenta en el mejoramiento continuo de los servicios y aplicaciones web de la empresa, sin la necesidad de invertir en soluciones de seguridad adicionales para los sistemas de distribución Debían, sistema operativo base donde corren todos los servicios de la compañía.

Estratégicamente GRUPO NETHEXA S.A.S requiere la adquisición de la certificación de seguridad, para mejorar la credibilidad de los clientes y cumplir con las regulaciones de seguridad informática colombiana, apalancándose del sistema de gestión integral de seguridad informática para la mejora continua de los procesos y políticas. Este proyecto representa un aporte importante para el logro de los objetivos, pues facilitará la certificación en O-ISM3 como sistema de gestión de seguridad de la información en los servicios web de e-learning y telefonía IP, y por lo tanto representa una mejora continua en la disponibilidad, continuidad y seguridad de los productos y servicios web que son desarrollados por la organización.

En este proyecto se logran definir las amenazas y/o vulnerabilidades que poseen los activos de información de los servicios web de la empresa, permitiendo verificar la probabilidad e impacto de materialización de las amenazas identificadas, valorando el nivel de riesgos que poseen los activos de información de los servicios web de e-learning y telefonía IP, y proporcionando la información necesaria para realizar el debido tratamiento del riesgo para el área de ciberseguridad.

Se diseñó la base del sistema de gestión integral de seguridad informática, donde se profundizó en procesos enfocados en la gestión de riesgos de los activos de información y controles de seguridad que pueden ser implementados por el personal de ciberseguridad, permitiendo la adopción de buenas prácticas de seguridad informática suministradas por el trabajo de grado, mejorando la integridad, disponibilidad y continuidad de los servicios web de e-learning y telefonía IP. Reduciendo las amenazas y/o vulnerabilidades identificadas que aporten mejoras en el soporte y la carga laboral de la mesa de ayuda de la organización, aumentando el análisis proactivo de seguridad de los activos de información, al perfeccionar cada vez la calidad del servicio y los tiempos de respuesta ante los incidentes de seguridad que afectan la continuidad del negocio, al implementar todos los controles recomendados.

8 REFERENCIAS

Ley_222. (1995). *Ley 222 de Colombia de 1995*. Recuperado el 20 de Octubre de 2017, de http://www.secretariasenado.gov.co/senado/basedoc/ley_0222_1995.html#top

Decisión_351. (1993). *Decisión 351 de 1993 de la Comunidad Andina de Naciones*. Recuperado el 20 de Octubre de 2017, de http://www.ins.gov.co/normatividad/Decisiones/DECISION%20351%20DE%201993%20DE%20LA%20COMUNIDAD%20ANDINA%20DE%20NACIONES.pdf?Mobile=1&Source=%2Fnormatividad%2F_layouts%2Fmobile%2Fview%2Easpx%3FList%3D2ce58563%252D79fd%252D4769%252D8c5e%252D3a742c40a659%26V

Berners-Lee, T., Fielding, R., & Frystyk, H. (1996). *Hypertext Transfer Protocol -- HTTP/1.0, RFC1945*. Recuperado el 2 de Marzo de 2017, de https://tools.ietf.org/html/rfc1945

Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P., & Berners-Lee, T. (1999). *Hypertext Transfer Protocol -- HTTP/1.1, RFC2616*. Recuperado el 2 de Marzo de 2017, de https://tools.ietf.org/html/rfc2616

Nielsen, H., Leach, P., & Lawrence, S. (2000). *An HTTP Extension Framework, RFC2774*. Recuperado el 2 de Marzo de 2017, de https://tools.ietf.org/html/rfc2774

Ley_599. (2000). *Ley 599 del 2000 de Colombia*. Recuperado el 20 de Octubre de 2017, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388

Jackson, C., & Barth, A. (2008). *Force HTTPS: Protecting High-Security Web Sites from Network Attacks*. Recuperado el 20 de Marzo de 2017, de https://crypto.stanford.edu/forcehttps/

CRAMM. (2002). *Análisis y Gestión de Riesgos CRAMM*. Recuperado el 20 de Noviembre de 2017, de https://www.sans.org/reading-room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm-83

EBIOS. (2003). *Metodología de Gestión de los Riesgos EBIOS*. Recuperado el 20 de Noviembre de 2017, de https://www.ssi.gouv.fr/archive/es/confianza/documents/methods/ebiosv2-methode-plaquette-2003-09-01_es.pdf

Baz, I., Bonilla, J., Gorrotxategi, G., Ibarra, S., Santamaría, D., & Ruiz, I. (2009). *Introducín a la VoIP y Asterisk Irontec*. Recuperado el 20 de Noviembre de 2017, de http://paginaspersonales.deusto.es/igor.ira/teaching/courses/voip_irontec_november_2009/igor.ira_Introduccion_a_la_VoIP_y_Asterisk.pdf

Ley_1273. (2009). *Protección de la información y de los datos TIC*. Recuperado el 21 de Octubre de 2017, de http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf

Brooks, R., & Deng, J. (2010). Lies and the Lying Liars that Tell Them: A Fair and Balanced Look at TLS - Holcombe Department of Electrical and Computer Engineering. *ACM*, 1-3.

Benton, k., Jo, J., & Kim, Y. (2011). SignatureCheck: A Protocol to Detect Man-In-The-Middle Attack in SS. *ACM*, 1-4.

MEHARI. (2010). *Metodología de Análisis y gestión de Riesgos MEHARI.* Recuperado el 20 de Noviembre de 2017, de http://meharipedia.x10host.com/wp/wp-content/uploads/2016/12/MEHARI-2010-IntroduccionESP.pdf

Ley_1450. (2011). *Plan Nacional de Desarrollo y Plan de Inversiones 2011-2014.* Recuperado el 20 de Octubre de 2017, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=43101

MAGERIT_V3. (2011). *Consejos prácticos en la identificación de activos, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Libro 1 Método.

Mavrogiannopoulos, N., Vercauteren, F., Velichkov, V., & Preneel, B. (2012). A Cross-Protocol Attack on the TLS Protocol. *ACM*, 1-11.

Dacosta, I., Ahamad, M., & Traynor, P. (2012). *Trust No One Else: Detecting MITM Attacks Against SSL/TLS Without Third-Parties*. Recuperado el 2 de Septiembre de 2016, de https://w ww.cise.ufl.edu/~traynor/papers/dacosta-esorics12.pdf

Hodges, J., Jackson, C., & Barth, A. (2012). *HTTP Strict Transport Security (HSTS) RFC6797*. Recuperado el 15 de Febrero de 2017, de https://tools.ietf.org/html/rfc6797

Ley_1581. (2012). *Disposiciones generales para la protección de datos personales*. Recuperado el 21 de Octubre de 2017, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981

MAGERIT_V3. (2012). *Método de análisis de riesgos y Proceso de gestión de riesgos, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información.* Libro 1 Método.

Rodríguez, A. (2013). *Man in the Middle Attacks on SSL/TLS (Tesis de Maestría), Universidad autónoma de Barcelona*. Recuperado el 4 de Septiembre de 2016, de http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18443/6/acaroalTFM0113memoria.pdf

Sugavanesh, B., Prasath, H., & Selvakumar, S. (2013). SHS-HTTPS Enforcer: Enforcing HTTPS and preventing MITM Attacks. *ACM*, 1-4.

OWASP. (2013). *OWASP Top 10 for 2013*. Recuperado el 15 de Marzo de 2017, de https://www.owasp.org/images/5/5f/OWASP_Top_10_-_2013_Final_-_Espa%C3%B1ol.pdf

Barhoum, K., & Muhsen, Z. (2013). *Risks and Remedies in ISRA University E-Learning System.* iJET.

ISO_27001. (2013). *Sistema de gestión de seguridad de la información (SGSI) Colombiano*. Recuperado el 12 de Agosto de 2018, de http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf

Ley_1712. (2014). *Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional*. Recuperado el 22 de Octubre de 2017, de http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882

Cardoso, O. (2014). Modelo de procesos de seguridad de la información basados en el estándar O-ISM3, Trabajo de grado, Universidad de Buenos Aires. 1-93.

Wang, J., Yang, Y., Chen, L., Yang, G., Chen, Z., & Wen, L. (2015). A Combination of Timing Attack and Statistical Method to Reduce Computational Complexities of SSL/TLS Side-Channel Attacks. 11th International Conference on Computational Intelligence and Security. *IEEE*, 1-5.

Eldewahi, A., Sharfi, T., Mansor, A., & Mohamed, N. (2015). SSL/TLS Attacks: Analysis and Evaluation. International Conference on Computing, Control, Networking, Electronics and Embedded System Engineering. *IEEE*, 1-6.

LeonardoNev. (2015). *SSLStrip version to defeat HSTS*. Recuperado el 17 de Febrero de 2017, de https://github.com/LeonardoNve/sslstrip2

Romero, D. (2015). *Awesome-web-hacking*. Recuperado el 15 de Marzo de 2017, de https://github.com/infoslack/awesome-web-hacking#tools

Belshe, M., Peon, R., & Thomson, M. (2015). *Hypertext Transfer Protocol Version 2 (HTTP/2), RFC7540*. Recuperado el 2 de Marzo de 2017, de https://tools.ietf.org/html/rfc7540

BIA. (2015). *Guía para realizar el análisis de impacto de negocios BIA*. Recuperado el 12 de Agosto de 2018, de https://www.mintic.gov.co/gestionti/615/articles-5482_G11_Analisis_Impacto.pdf

Han, S., Kwon, H., Hahn, C., Koo, D., & Hur, J. (2016). A Survey on MITM and its Countermeasures in the TLS Handshake Protocol. Department of Computer Science and Engineering. *IEEE*, 1-6.

Santiso, H., Koller, J., & Bisaro, M. (2016). *Seguridad en Entornos de Educación Virtual*. Recuperado el 21 de Marzo de 2018, de http://www.um.edu.uy/docs/Seguridad_en_entornos_de_educacion_virtual.pdf

MSPI. (2016). *Guía de gestión de riesgos, MINTIC*. Recuperado el 23 de Septiembre de 2018, de https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Gutiérrez, J. (2017). *Grupo Nethexa S.A.S*. Recuperado el 21 de Octubre de 2017, de https://nethexa.com/

Torres, S., & Rojas, J. (2017). *Modelo de Gestión de Riesgos Aplicando Metodología Octave Allegro en entidades del Sector Fiduciario*. Recuperado el 21 de Noviembre de 2017, de https://auditoriauc20102mivi.wikispaces.com/file/view/Metodolog%C3%ACas+de Gesti%C3%B2n+de+Riesgos.pdf

SGSI. (2017). *Sistemas de Gestión de la Seguridad de la Información*. Recuperado el 22 de Octubre de 2017, de http://www.mintic.gov.co/gestionti/615/w3-article-5482.html

MSPI. (2017). *Modelo de seguridad y privacidad de la información Colombiano*. Recuperado el 21 de Noviembre de 2017, de http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

O-ISM3. (2017). *Information security management maturity standard*. Recuperado el 20 de Noviembre de 2017, de http://www.ism3.com/node/42

RedHat. (2017). *Guía de seguridad, Red Hat Enterprise Linux 6*. Recuperado el 11 de Septiembre de 2018, de https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/6/pdf/security_guide/Red_Hat_Enterprise_Linux-6-Security_Guide-es-ES.pdf

Linux_Trucepei_Blog. (2017). *Aseguramiento de servidor WEB apache*. Recuperado el 8 de Noviembre de 2018, de https://juantrucupei.wordpress.com/2017/05/24/seguridad-apache-tips/

Debían. (2018). *Manual del Administración de Debían*. Recuperado el 7 de Noviembre de 2018, de https://debian-handbook.info/browse/es-ES/stable/sect.package-authentication.html

SonicWall. (2018). *Recursos de soporte de seguridad*. Recuperado el 8 de Noviembre de 2018, de https://www.sonicwall.com/en-us/support

.

ANEXO 1

GP-1 GESTIÓN DEL CONOCIMIENTO

REVISIÓN Y APROBACIÓN DE LA GESTIÓN DEL CONOCIMIENTO ADQUIRIDO.

1. Descripción del proceso

Proceso encargado de gestionar el conocimiento dentro de la organización del personal de seguridad y de TIC, los cuales poseen información y conocimiento de las diferentes soluciones proporcionadas a los clientes. Con el objetivo de, mantener la disponibilidad del conocimiento de toda infraestructura de seguridad actualizada y fiable, para dar el adecuado soporte a todos los procesos y facilitar la toma de decisiones ante los incidentes que se puedan presentar.

2. Objetivos y metas

- El conocimiento adquirido por el personal de la empresa debe ser almacenado, compartido y utilizado en equipo, realizando un trabajo colaborativo compartiendo y mejorando la información necesaria para brindar soporte continuo de los servicios.
- Proporcionar soporte ágil y eficiente a nuestros clientes, brindando servicios con eficacia y calidad.
- Garantizar que el personal de seguridad y TIC cuenten con la información adecuada.

3. Métricas

Documentación de implementaciones de seguridad realizados durante el semestre, realizando una debida planificación de la identificación, organización, recopilación, mantenimiento, uso y retirada del conocimiento, teniendo en cuenta las siguientes mediciones:

- Volumen de información clasificada.
- Porcentaje de información categorizada.
- Porcentaje de conocimiento disponible.
- Nivel de satisfacción de los usuarios.

4. Gobierno de gestión del conocimiento

- Cultivar y facilitar el intercambio de información en la organización.

- Identificar y clasificar las fuentes de información.
- Organizar y contextualizar toda la información creada; con el fin de, transformar el conocimiento de una manera íntegra y fiable.
- Utilizar y compartir el conocimiento.
- Evaluar y retirar la información.

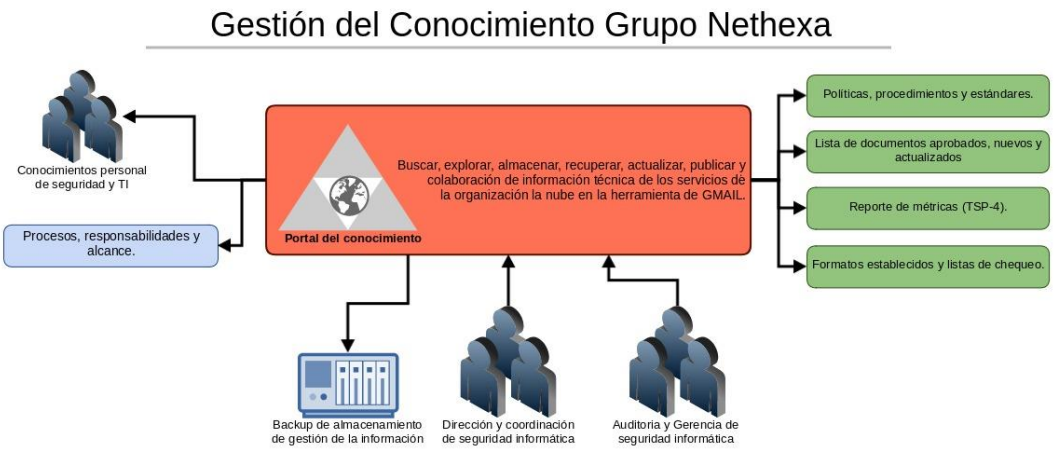
5. Actividades

- Comunicar, crear e integrar proactivamente el conocimiento de seguridad y TIC de la organización, impulsando la transferencia del conocimiento motivando al personal técnico de los beneficios que se tiene en fomentar el trabajo colaborativo, la documentación y capacitación de la información técnica.
- Implementación de herramientas de almacenamiento, que permitan la clasificación y recolección de manera ordenada de la información proporcionada por usuarios potenciales.
- Publicar la información técnica recopilada de la organización al personal encargado, proporcionando el fácil acceso a la información con los respectivos permisos de visualización otorgados por el área.
- Educar y entrenar constantemente a los usuarios con la información recopilada, mejorando la continuidad del negocio entregando el conocimiento al personal que administra los servicios de información.
- Realizar copias de seguridad de la información recopilada y retirar la información que no es útil para la organización.

6. Sistema de recolección de la información

La organización posee una política de gestión del conocimiento, donde se encarga de evaluar las entradas de conocimientos que son generadas por el área de seguridad y TIC, donde se documentan todos los procesos, responsabilidades y alcances que posee la empresa en la implementación y mejora de los servicios proporcionados.

CIBIT_5 (2012), toda la información es revisada y evaluada, con el objetivo de corregir y avalar la información que se está almacenado de los servicios implementados por la organización, con el propósito de que la información almacenada sea entendible por todo el personal encargado, para futuras consultas y capacitación del personal de soporte técnico. También, de la evaluación se pueden extraer mejoras en políticas, procedimientos y estándares implementados en la solución de los servicios implementados; con el objetivo de, tener una mejora constante de los servicios brindado continuidad al negocio y una mejora en la disponibilidad de los servicios brindados a los usuarios.



ITIL_V3 (2011), toda la información es clasificada por nombre de proyectos, los cuales contienen la documentación de la implementación, mantenimiento y soporte de los servicios instalados. También, la documentación es actualizada cada vez que se generan cambios, actualizaciones e incidentes que generen mejoras considerables en el servicio prestado a los clientes.

7. Bibliografía

CIBIT 5 (2012). Proceso BAI-08: Gestionar el conocimiento. Objetivos de control las tecnologías de información y relacionadas. Recuperado: https://adminsisuc201701.wordpress.com/bai08/. 8 de agosto de 2018.

ITIL V3 (2011). Gestión del conocimiento, Transición del servicio basada en ITIL V3. p. 109-114.

ANEXO 2

GP-3 DISEÑO Y EVOLUCIÓN DEL SGSI

POLÍTICA DE GESTIÓN DE RIESGOS

1. Descripción del Proceso

La organización adoptará las buenas prácticas de la norma de gestión de riesgos establecida en la ISO 31000, por este motivo se acoge a la metodología de implementación de gestión de riesgos Magerit, la cual permite tomar decisiones al gobierno de TIC en la aceptación, tratamiento y transferencia del riesgo de la empresa.

El proceso se encargará de analizar, evaluar e informar el nivel de riesgo que poseen los activos de información de la organización en los servicios web de e-learning y telefonía IP de GRUPO NETHEXA S.A.S. Con el fin de; realizar auditorías constantes en la gestión del riesgo con un ciclo PHVA, identificando la criticidad de los riesgos para la empresa con el objetivo de que la empresa pueda implementar controles que disminuyan y/o mitiguen los riesgos que presentan los servicios web.

2. Objetivos y Metas

- Informar a la organización y a los responsables de la existencia de los riesgos que poseen los servicios de TIC y la necesidad de gestionarlos.
- Ofrecer un método para la identificación de los riesgos de TIC.
- Establecer un método que permita analizar los riesgos identificados en los servicios de TIC.
- Ayudar a descubrir y planificar oportunamente el tratamiento del riesgo.
- Preparar a la organización para procesos de evaluación, certificación y auditorías en el área de las TIC.

3. Métricas

- Porcentaje de riesgos Identificados.
- Porcentaje de riesgos críticos para la organización.
- Porcentaje de riesgos aceptables para la organización.
- Nivel de valoración del riesgo.
- Nivel del riesgo.
- Porcentaje de disponibilidad al tratar el riesgo.

4. Escaneo e investigación de amenazas y vulnerabilidades

El propósito de escanear los servicios web de la organización, es identificar las vulnerabilidades que poseen los activos de TIC de la organización en la prestación de servicios y aplicaciones que son necesarios para el funcionamiento de las plataformas de e-learning y Telefonía IP de la organización.

Las herramientas utilizadas para realizar los escaneos constantes de las plataformas web de la organización son: Nessus (Escaneo avanzado y completo del servidor) y Owasp Zap (Escaneo de vulnerabilidades web), con la finalidad de detectar las amenazas y vulnerabilidades que pongan en riesgo los activos de TIC.

Los riesgos que poseen los activos de información no solo son identificados a través de herramientas de escaneo de amenazas y vulnerabilidades, también es necesario realizar una investigación de las mismas para tener un panorama más completo y todos los problemas de seguridad que pueden afectar a los activos de información de la organización.

Se realizará un informe de las vulnerabilidades y amenazas identificadas en los escaneos, los cuales ayudará con la alimentación de los posibles riesgos que poseen los activos de los servicios web de la organización.

5. Niveles de criticidad y tolerancia al riesgo

El propósito del nivel del riesgo es poder identificar cuáles son las amenazas que pueden impactar y/o perjudicar a la empresa en la continuidad del negocio; por este motivo, se crea una tabla con los valores críticos para la organización, con la finalidad de poder tomar decisiones ante los resultados de la valoración de las amenazas que pueden perjudicar a los activos de la organización, tomando decisiones estratégicas que permitan disminuir y/o mitigar las amenazas críticas.

Nivel del riesgo:

	Impacto					
		Insignificante	Menor	Moderado	Mayor	Catastrófico
Probabilidad	Nivel	1	2	3	4	5
Raro	1	B	B	B	M	M
Improbable	2	B	B	B	M	A
Posible	3	B	B	M	A	A
Probable	4	B	M	M	A	A
Casi Seguro	5	M	M	A	A	A

- **Nivel de riesgo bajo:** El riesgo es asumido.
- **Nivel de riesgo Medio:** Se debe hacer un tratamiento del riesgo para reducirlo.
- **Nivel de riesgo alto:** Se hace tratamiento del riesgo para reducirlo, evitarlo, compartirlo o transferirlo.

Para la organización todas las amenazas que se encuentren en el nivel riesgo alto, no pueden son tolerables, ya que el costo de la materialización de una de estas amenazas puede acabar con la organización y/o llevarla a la quiebra. Debido a que, el impacto que puede generar un incidente de seguridad alto afecta la economía y reputación de la empresa, en el mercado de prestación de servicios de TIC a nivel Nacional.

6. Valoración y análisis del riesgo

Para la valoración del riesgo se crea un formato que contiene todos los niveles de criticidad de los activos de información para la organización, con el propósito de realizar un cruce con las amenazas y la probabilidad de la ocurrencia e impacto en que pueda ocurrir la materialización de la amenaza, identificando cuales son los activos de información a los que se realiza un tratamiento del riesgo para disminuir la probabilidad de que se puedan materializar las amenazas críticas, que puedan afectar a la empresa económicamente y en el mercado de prestación de servicios de TIC.

Formato de valoración y análisis del riesgo.

Con los resultados de la valoración y análisis de riesgos, se informa a gerencia, con el propósito de tomar decisiones estratégicas que puedan ayudar al área de seguridad informática en la implementación de controles y corrección de vulnerabilidades, que permitan mitigar y/o disminuir el riesgo identificado planificando un plan de acción, que pueda ser ejecutan los más rápido posible y reducir el impacto que pueda generar un incidente de seguridad en la continuidad de los servicios web de la organización cumpliendo con los acuerdos de niveles de servicios pactados con los clientes.

Informe de valoración y análisis del riesgo.

7. Bibliografía

MAGERIT_V3 (2012). Método de análisis de riesgos y Proceso de gestión de riesgos, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1 Método, p. 22-60.

MSPI (2016). Guía de gestión de riesgos, MINTIC. Recuperado: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf. 23 de septiembre de 2018.

ANEXO 3

SSP-1 REPORTE A LAS PARTES INTERESADAS

1. Descripción del proceso

El proceso es responsable del cumplimiento de la periodicidad de reportes enviados a las partes interesadas, demostrando el cumplimiento de las regulaciones y metas de seguridad establecidas por la alta dirección de la organización.

2. Objetivos y metas

- Brindar información que apoye a la gerencia en la toma de decisiones sobre las inversiones en el área de seguridad.
- Brindar información de los riesgos operativos del negocio.

3. Métrica

Cantidad de reportes realizados a las partes interesadas para un periodo de tiempo definido.

4. Reporte general de seguridad de la información.

Es el reporte encargado de reunir la información de los demás reportes proporcionados por los procesos estratégicos, tácticos y operativos del SGSI, realizando un informe ejecutivo lo más resumido posible de la madurez y el trabajo realizado por los procesos de seguridad en la organización, con el fin de, poder tomar decisiones directivas que permitan mejorar la continuidad de la seguridad informática en la organización.

a. Reporte Estratégico

El proceso establece la realización de los reportes periódicos que son compartidos a gerencia, mostrando el cumplimiento de las políticas y metas establecidas por la gestión de seguridad en la organización.

b. Reporte de Táctico

Informar a la gestión estratégica de seguridad del rendimiento, eficacia y efectividad del modelo del SGSI.

c. Reporte operativo

Informe periódico de los resultados de los procesos y el uso de los recursos asignados.

5. Bibliografía

O-ISM3 (2017). Information security management maturity standard. Recuperado: http://www.ism3.com/node/42. 20 de noviembre de 2017.

ANEXO 4

SSP-2 COORDINACIÓN

1. Descripción del proceso

El proceso se encarga de establecer el modelo de relacionamiento de los líderes de las áreas de la organización que intervienen en el SGSI.

2. Objetivos y metas

Coordinación entre los líderes de la empresa y el área de seguridad informática; con el fin de, apoyar transversalmente a todas las áreas para alcanzar los objetivos y optimizar los recursos de la organización.

3. Métricas

Porcentaje de participación de áreas enfocadas con la seguridad informática.

4. Coordinación del área de seguridad informática y las TIC

Es de suma importancia gestionar las relaciones y responsabilidades de las áreas del negocio y seguridad informática, de una manera formal y transparente en la obtención de resultados empresariales exitosos apoyando todos los objetivos estratégicos, tácticos y operativos del SGSI.

Todas las áreas relacionadas con las TIC deben de tener una buena relación construida a través de la confianza mutua, usando términos y lenguajes entendibles al asumir las responsabilidades en las decisiones claves en la gestión de incidentes y en la mejora continua de la seguridad de los activos de información.

Todos los líderes de las áreas de la empresa tienen la obligación de tener una comunicación constante con el área de seguridad informática; con el propósito de, informar a las partes interesadas y coordinar todos los problemas relacionados con los activos de información que pueden presentar las plataformas web de e-learning y telefonía IP.

Las actividades a tener en cuenta para la coordinación son las siguientes:

- Coordinar y comunicar con el área de seguridad informática los cambios y actividades en la transición de proyectos, planes de cambio, planificación, lanzamiento de nuevas políticas, errores conocidos y concienciación de la información, con el propósito de ser evaluado y

analizado por el personal de seguridad informática con el objetivo de mitigar los riesgos que se pueden presentar.

- Coordinar y comunicar las actividades operativas, roles y responsabilidades de la organización en el área de TIC al área de seguridad, teniendo presente el árbol jerárquico de la organización para tener ayuda inmediata de las personas encargadas de la administración de las plataformas, para la comunicación y mitigación de los incidentes o problemas de seguridad que se pueden presentar ante una eventualidad.
- Tomar acciones inmediatas con las áreas encargadas en eventos que puedan influenciar la comunicación del personal de la organización.
- Mantener un plan de comunicación de todas las áreas, que contenga los destinatarios responsables de los servicios prestados por la organización.

5. Bibliografía

CIBIT 5 (2012). Proceso APO-08: Gestionar las relaciones. Objetivos de control las tecnologías de información y relacionadas. Recuperado: https://adminsisuc201701.wordpress.com/ap008-gestionar-las-relaciones/. 4 de octubre de 2018.

ANEXO 5

SSP-6 ASIGNACIÓN DE RECURSOS PARA LA SEGURIDAD DE LA INFORMACIÓN

1. Descripción del proceso

Este es el proceso en que asignan todos los recursos relacionados al área de seguridad informática en la organización.

2. Objetivos y metas

Brindar los recursos necesarios para la adecuada gestión del SGSI en procesos de gestión táctica y operativa.

3. Métricas

- Cantidad de proyectos presentados y aprobados.
- Porcentaje del consumo del presupuesto en gastos e inversiones.
- Cantidad de recursos solicitados y obtenidos.

4. Asignación de recursos se dé seguridad informática

En el área de seguridad informática es de suma importancia la asignación de recursos; con el fin de, obtener las herramientas de seguridad que permitan reducir y/o mitigar los riesgos que poseen los activos de información de e-learning y telefonía IP.

La dirección de seguridad informática de la organización es la encargada de presentar el análisis de gestión de riesgos y los controles necesarios para la mitigación y disminución del riesgo de los activos de información, presentando los diferentes proyectos y los costos de implementación, adquisición, licencias y mantenimientos de estos, para que la alta dirección pueda revisar y tomar la decisiones de la aprobación de los proyectos, delegando presupuesto al área de seguridad informática para la ejecución de los controles de seguridad.

Los recursos asignados para afrontar los proyectos de seguridad que mejorarán la seguridad de los activos de información de la empresa, son administrados por los procesos internos del área de seguridad informática, donde se proporciona el manejo y la administración del dinero en los controles de seguridad propuestos en los objetivos del SGSI.

ANEXO 6

TSP-1 INFORME DE GESTIÓN ESTRATÉGICA

1. Descripción del proceso

Proceso que presenta los resultados de los recursos de seguridad informática que fueron asignados al área.

2. Objetivos y metas

Informar a la gestión estratégica de seguridad del rendimiento, eficacia y efectividad del modelo del SGSI.

3. Métricas

- Cantidad de reportes formalizados y acordados.
- Cantidad de procesos que poseen reportes asociados.
- Cantidad de métricas de procesos operativos presentados.

4. Reporte de la gestión estratégica de seguridad informática

El propósito fundamental del proceso es poder informar el rendimiento, eficacia y efectividad de los controles invertidos e implementados en el área de seguridad informática, con el objetivo de informar a todas las partes interesadas del valor significativo que representa la seguridad informática en las plataformas web de la organización.

En el reporte entrega la siguiente información:

a. Reporte operacional de seguridad informática

El reporte operacional debe contener todas las actividades significativas que aportan a la seguridad de las plataformas web de la organización, informando a las áreas interesadas:

- Implementación de controles de seguridad en los activos en información.
- Corrección de vulnerabilidades de los activos de información.
- Actualizaciones realizadas a los activos de información.
- Incidentes de seguridad mitigados y/o prevenidos por el área de seguridad informática.
- Informe de la disponibilidad de los activos de información.

b. Reporte de métricas de procesos operacionales

El reporte contiene los resultados generados por la auditoría de los procesos de seguridad que se realizan al área de seguridad informática, verificando el rendimiento, eficacia y eficiencia de los controles de seguridad, informando las fortalezas y debilidades que poseen los procesos de gestión de seguridad informática, con la finalidad de que se tomen decisiones importantes para la mejora continua de los procesos del SGSI.

c. Rendimiento y ROI de la seguridad informática

El principal objetivo del reporte de rendimiento y ROI, es poder evaluar la inversión realizada en el área de seguridad informática, revisando el beneficio que han recibido los activos de información, reduciendo los riesgos de los activos de información medios y moderados, permitiendo la disminución y/o mitigación del riesgo, generando una valor agregado que genera el costo de la inversión y en la reducción del riesgo, evitando la perdida de dinero de la organización ante incidentes de seguridad informática.

El informe debe contener:

- ROI
- Riesgos cubiertos por los controles de seguridad implementados con el presupuesto.
- Riesgos que no se han podido reducir y/o mitigar.
- Inversión necesaria para el cubrimiento de los riesgos no gestionados.

ANEXO 7

TSP-2 ADMINISTRACIÓN DE RECURSOS ASIGNADOS

1. Descripción del proceso

Adecuada asignación de los recursos de la organización a nivel táctico y operativo.

2. Objetivos y metas

Planificación y control en la asignación de los recursos del área para asegurar los ISM planificados, para alcanzar los objetivos de seguridad.

3. Métricas

- Porcentaje de recursos asignados a procesos tácticos.
- Porcentaje de recursos asignados a procesos operativos.

4. Administración de recursos asignados de seguridad informática

La organización cambiará el concepto de la inversión de los recursos, donde cada semestre asignará un recurso para la inversión de tecnología para las áreas de seguridad informática, redes de telecomunicaciones, telefonía IP y e-learning, con el propósito de que las áreas puedan tener un recurso económico para la mejora continua de los procesos que lideran dentro de la organización.

Para el área de seguridad es importante gestionar las actividades financieras relacionadas con la implementación de controles y pago de honorarios, abarcando el presupuesto, costo y gestión de los beneficios económicos otorgados por la empresa. Los gastos realizados en el área deben de ser definidos por una priorización de gastos de manera justa, repartiendo el dinero en la inversión de tecnología de seguridad informática que ayude a tratar los riesgos que son priorizados por el nivel de gestión de riesgos.

Con la inversión y reducción constante de riesgos altos y medios, los cuales son los críticos para la organización y pueden generar una pérdida importante a nivel de reputación y de dinero, se tiene la finalidad de poder madurar constantemente la seguridad de los activos de información de las plataformas web de la organización, hasta llegar a un nivel de seguridad que genere confianza a la empresa y a los clientes que utilizan los servicios.

EL proceso hace un seguimiento a las siguientes actividades, con el objetivo de poder administrar adecuadamente los recursos proporcionados por la organización:

a. Gestión de finanzas y contabilidad

Establecer y mantener un método que permite contabilizar todos los costos, inversiones y depresiones relacionadas con la seguridad, integrando el sistema financiero de la empresa y el plan de cuentas del área de seguridad informática, administrado adecuadamente las inversiones y el costo de la seguridad de los activos de información.

b. Priorizar la asignación de recursos

Definir la priorización en la toma de decisiones en la asignación de recursos a cada proceso del SGSI, tomando como referencia el nivel de riesgo que están afrontando los activos de información, definiendo el porcentaje o la cantidad de presupuesto que es asignado a cada proceso de seguridad informática que aporten significativamente a la unidad de negocio. Incluyendo el uso potencial de proveedores de servicios, opciones de compra, desarrollo y alquiler.

c. Crear y mantener el presupuesto

Preparar un presupuesto que refleje las prioridades de inversión y apoyen a los objetivos estratégicos basados en el SGSI, planificando y administrando el uso de los recursos proporcionados al área de seguridad informática.

d. Modelar y asignar los costos

Establecer y utilizar un modelo de costos de seguridad basado en los controles y riesgos que se deben de mitigar, asegurando que la asignación de los costos de los servicios de seguridad sea identificables, medibles, priorizados y predecibles, fomentando el uso responsable de los recursos asignados, incluyendo los recursos proporcionados por proveedores de servicios.

e. Gestionar los costos

Definir en el área de seguridad el modelo de la gestión de los costos, comparando los costos reales y los presupuestos otorgados, supervisando y comunicando las desviaciones que pueden ocurrir e identificarlas oportunamente; con el fin de, evaluar su impacto en los procesos del SGSI y en la implementación de controles.

5. Bibliografía

CIBIT 5 (2012). Proceso BAI-06: Gestionar el presupuesto y los costes. Objetivos de control las tecnologías de información y relacionadas. Recuperado: https://adminsisuc201701.wordpress.com/apo06-gestionar-el-presupuesto-y-los-costes/. 30 de septiembre de 2018.

ANEXO 8

TSP-3 DEFINICIÓN DE METAS Y OBJETIVOS DE SEGURIDAD

1. Descripción del proceso

El proceso establece las metas y los objetivos de seguridad informática de la organización, asociando los estándares y políticas que deben de cumplir las áreas de TIC y de seguridad informática.

2. Objetivos y metas

Proveer las bases para contribuir los procesos del modelo de SGSI.

3. Métricas

- Objetivos de seguridad de la información.
- Requisitos de clasificación de la información.

4. Objetivos

- Informar a la organización y a los responsables de la existencia de los riesgos que poseen los servicios de TIC y la necesidad de gestionarlos.
- Ofrecer un método para la identificación de los riesgos de TIC.
- Establecer un método que permita analizar los riesgos identificados en los servicios de TIC.
- Ayudar a descubrir y planificar oportunamente el tratamiento del riesgo.
- Preparar a la organización para procesos de evaluación, certificación y auditorías en el área de las TIC.
- Gestionar el riesgo asociado a los activos de información que contiene los servicios web de la organización.
- Adoptar controles de seguridad que permitan reducir los riesgos informáticos y mitigar proactivamente las amenazas que poseen los servicios web de la organización.
- Brindar un soporte eficaz y oportuno ante incidentes de seguridad informática.

5. Metas

- Mejorar la disponibilidad de los servicios prestados por la organización constantemente.

- Brindar continuidad del negocio a la empresa, mejorando la reputación corporativa implementando seguridad en los servicios prestados.
- Dar cumplimiento a las normas de seguridad colombiana, en implementar un SGSI que permita asegurar los activos de información.

Estos son los objetivos y metas principales que son los pilares aceptados por la empresa como política para el cumplimento de la seguridad informática en la organización, la finalidad de los objetivos y las metas propuestas es poder apalancar todos los procesos implementados de seguridad informática, los cuales son necesarias para el cumplimiento del objetivo principal de la organización que es poder tener un SGSI maduro.

ANEXO 9

TSP-4 GESTIÓN DE NIVELES DE SERVICIOS

1. Descripción del proceso

Proceso encargado de gestionar los acuerdos de nivel de servicios que provee la organización alineados con los procesos ISMS; con el propósito de, proporcionar disponibilidad de los servicios y continuidad del negocio.

2. Objetivos y metas

Proporcionar las métricas necesarias para la evaluación objetiva de los ISMS y los componentes de los procesos.

3. Métricas

- Cantidad de SLAs definidos.
- Cantidad de métricas obtenidas.

4. Acuerdos de nivel de servicios de los procesos de seguridad

La organización cuenta con un contrato realizado con el cliente, donde se pactan las condiciones de la prestación de servicios. En el contrato se detalla el acuerdo del nivel de servicios que van a tener las plataformas web de e-learning y Telefonía IP en la operación continua, los mismos SLA son acogidos por el área de seguridad en la gestión de incidentes de seguridad informática.

Monitorizar constantemente los acuerdos de nivel de servicios es de suma importancia, ya que es necesario auditar y verificar el cumplimiento de los pactos realizados con los clientes; con la finalidad de, no presentar problemas legales y económicos con los clientes por una mala prestación de seguridad en los servicios web proporcionados por la organización. Este proceso, es encargado de proporcionar toda la información relevante de la gestión de incidentes de seguridad que se han presentado y definen los servicios que están incumpliendo con los pactos contractuales con los clientes, para trabajar mucho más en ellos.

Para llevar un control de los incidentes que son generados por los clientes y poder evaluar el cumplimiento de los SLA acordados, es necesario ligar a la gestión de incidentes la cual debe velar por las siguientes dificultades:

- Detectar los incidentes en el menor tiempo posible.
- Registrar todos los incidentes de seguridad en la plataforma de tickets.
- Tener documentados los problemas presentados y disponibilidad de la información, con el propósito de tener una base del conocimiento de incidencias anteriores.
- Acceso a la documentación de gestión del conocimiento, permitiendo que la primera línea de soporte pueda consultar los datos históricos de las configuraciones de seguridad en los activos de información.
- Acceso a la documentación de los acuerdos de nivel de servicios acordados con los clientes, para determinar el impacto y la prioridad que se le debe dar a los incidentes de seguridad.
- Definir matriz de escalamiento y responsabilidades, con el objetivo de ejecutar procedimientos de escalamiento de incidentes de seguridad.

El objetivo principal de los procesos, es poder brindar un soporte efectivo ante incidencias de seguridad, donde se deben tener presentes los siguientes factores críticos, los cuales son básicos para poder proporcionar una buena gestión de incidentes de seguridad informática:

- Tener una buena mesa de ayuda a los clientes.
- Definir claramente los objetivos de los SLA.
- Personal de seguridad informática con buena formación técnica y competencias adecuadas en la prestación de servicios para todos los procesos.
- Herramientas de seguridad integradas para controlar y gestionar los procesos.
- Acuerdos de nivel operativo y contratos de soporte con el personal del área de seguridad informática.

En la gestión de incidentes es necesario reducir y mitigar los riesgos, por este motivo se tiene presente la siguiente información que no puede estar dentro de la organización:

- Tener un número de incidencias elevado, que perjudique los plazos de los SLA acordados con los clientes por falta de recursos humanos y de información necesaria.
- Uso de herramientas de seguridad inadecuadas por el área de seguridad.
- Ausencia de fuentes de información, por la falta de integración o herramientas adecuadas para atender los incidentes de seguridad.
- Falta de conciencia por el área de seguridad informática.

5. Bibliografía

ITIL V3 (2011). Gestión del nivel del servicio, operación del servicio basada en ITIL V3. p. 88-89.

ANEXO 10

OSP-1 INFORME DE GESTIÓN TÁCTICA

1. Descripción del proceso

Proceso encargado de demostrar los resultados de los procesos operativos y de los recursos invertidos.

2. Objetivos y metas

Mostrar el rendimiento y la eficacia de los procesos tácticos y operativos.

3. Métricas

- Cantidad de procesos con fallas detectadas.
- Porcentajes de incidentes con criticidad alta.
- Porcentaje de incidentes ocurridos por la falla de controles.
- Porcentajes de incidentes no anticipados por el análisis de riesgos.

4. Informes de gestión táctica “Operativas”

La organización hace responsable al equipo de seguridad informática de realizar informes ejecutivos revisando todos los procesos operativos que comprendan el SGSI. Las personas que se responsabilizan del informe de seguridad informática, son las encargadas de exponer a las áreas interesadas, los recursos que se han tenido para la mejora continua de la seguridad de la información.

Todas las tareas deben de realizar la documentación y el análisis de los servicios web de la organización, con el objetivo de poder exponer los avances que ha tenido la empresa en temas de seguridad y de cómo se está comportando el equipo de seguridad con los recursos proporcionados para la seguridad informática, exponiendo el caso de todas las mejoras y fallas en el SGSI en el periodo del año solicitado; con el propósito de, tomar las decisiones futuras con respecto al área de seguridad informática de la organización.

Las partes interesadas deben de entregar un informe del manejo de todos los procesos operativos del SGSI, donde se presentará un reporte que contenga las mejoras y los problemas que proporcionó el sistema de gestión de seguridad.

El reporte debe contener como mínimo:

- Inversión realizada en seguridad informática en la organización.
- Implementaciones de seguridad en los productos web.
- Procesos con falencias identificadas.
- Número de incidentes de seguridad altos, medios y bajos.
- Número de vulnerabilidades descubiertas y controles implementados para la mitigación de amenazas.
- Número de controles que no se han podido implementar.
- Incidentes que no fueron detectados por el análisis de riesgos.
- Estado de la seguridad actual.
- Conclusiones y mejoras propuestas.

ANEXO 11

OSP-3 GESTIÓN DE INVENTARIO DE ACTIVOS

1. Descripción del proceso

El proceso es el encargado de identificar el dueño de los activos de información, el proceso al que pertenece el activo, el estado actual y la dependencia que tienen a otros activos de información

2. Objetivos y metas

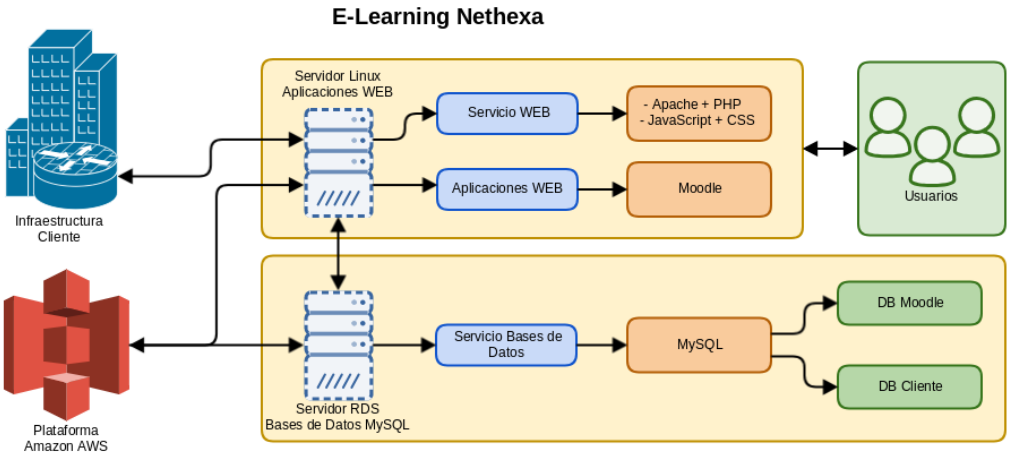
- Identificar todos los activos que componen los servicios de e-learning y Telefonía IP de la organización.
- Definir y clasificar los activos de información de los servicios de e-learning y Telefonía IP de la organización.
- Informar a la organización de la importancia de los activos de información que poseen los servicios de TIC de los servicios más importantes.

3. Métricas

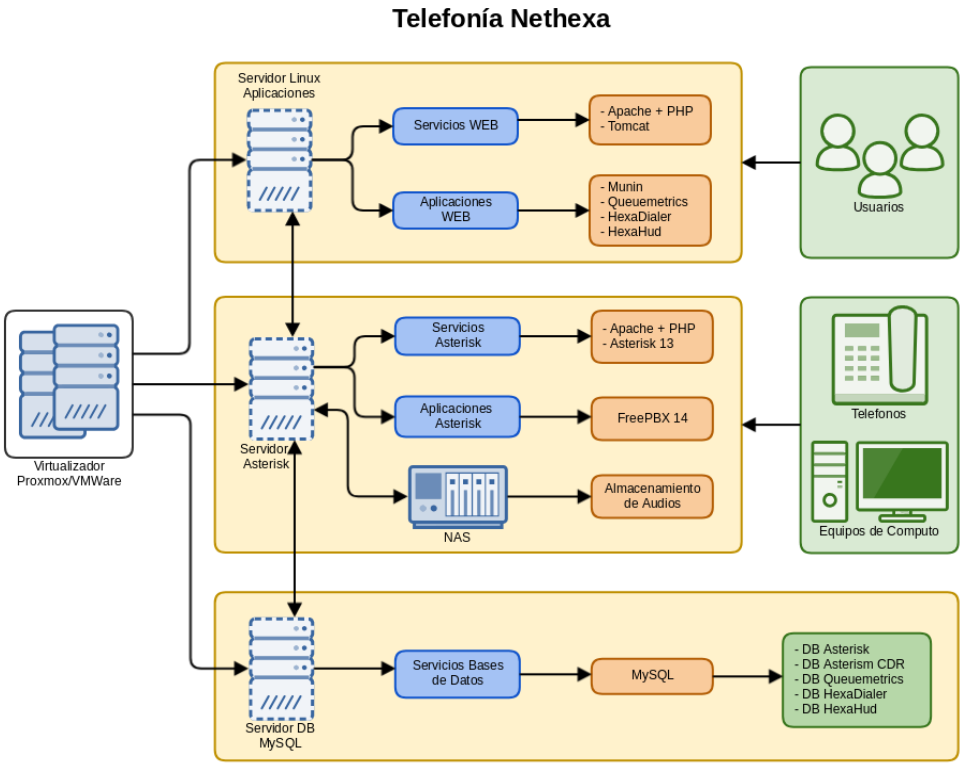
- Porcentaje de tipos de activos del inventario.
- Porcentaje del proceso de soporte de inventario.

4. Diagramas de los servicios de la organización

- **E-learning**



- **Telefonía IP**



5. Inventarios de Activos

Levantando la información de los servicios de e-learning y telefonía Ip de la organización, se separan todos los servicios, aplicaciones, sistemas operativos, plataformas de virtualización, plataformas en la nube, hardware, la información del servicio, el medio de acceso y los activos intangibles. Con el propósito de extraer los activos esenciales los cuales son necesarios para que los servicios web puedan operar sin ningún inconveniente.

Para la organización, la disponibilidad de las plataformas web es lo más importante en temas de seguridad informática, ya que el propósito fundamental es que los servicios sean siempre accesibles y utilizables por los usuarios, cumpliendo con los acuerdos de nivel de servicios pactados legalmente.

La prioridad de los activos se va a clasificar de la siguiente manera; con el fin de, poder tener un nivel de criticidad de activos que va a ser entregado por el análisis de riesgos.

Criticidad	Descripción
Alta	La no disponibilidad de los activos de información puede conllevar a un impacto negativo de índole legal, económica y las reputaciones retrasando las funciones de los clientes y degradando la imagen corporativa.
Media	La no disponibilidad de los activos de información puede conllevar a un impacto negativo de índole legal y económica, retrasando algunas funciones de los clientes y/o generando pérdidas de imagen corporativa moderada.
Baja	La no disponibilidad de los activos de información afecta la operación de los servicios web a los clientes, pero no conlleva implicaciones legales, económicas y pérdida de la imagen corporativa.

Los Activos de información son los siguientes:

- **Servicios**

Son los activos más importantes y son los que poseen mayor prioridad, ya que si estos no corren correctamente las aplicaciones no funcionan.

Etiqueta	Activo Informático	Descripción	Criticidad	Justificación
SRV-1	Apache + PHP	Visualizador de contenidos HTTP.	Alta	La no disponibilidad del servicio compromete a todas las aplicaciones web.
SRV-2	Tomcat	Visualizador de contenidos Java	Alta	La no disponibilidad del servicio compromete a la mayoría de las aplicaciones web.
SRV-3	Asterisk	Central telefónica IP	Alta	La no disponibilidad del servicio frena la operación de llamadas de las aplicaciones web.
SRV-4	MySQL	Gestor de bases de datos	Alta	La no disponibilidad del servicio frena la operación de las aplicaciones web, ya

				que necesitan la consulta de datos para la operación.

- **Aplicaciones**

Son también un activo importante para el funcionamiento del servicio, sin la programación o desarrollo de estas, el servicio quedaría vacío ya que es el complemento de este.

Etiqueta	Activo Informático	Descripción	Criticidad	Justificación
APP-1	Moodle	Sistema integrado de aprendizaje	Alta	La no disponibilidad del servicio afecta la realización de todos los cursos del cliente.
APP-2	Munin	Monitoreo de recursos web	Baja	La no disponibilidad del servicio no afecta la operación de las aplicaciones.
APP-3	Queuemetrics	Automatización de recepción de llamadas de call center	Alta	La no disponibilidad del servicio afecta directamente la operación de llamadas de Hexadialer y HexaHUD.
APP-4	HexaDialer	Marcado predictivo para Call Center	Alta	La no disponibilidad afecta la operación de los usuarios, impidiendo realizar llamadas.
APP-5	HexaHud	Gestor de llamadas entrantes para call center	Alta	La no disponibilidad afecta la operación de los usuarios, impidiendo el ingreso y visualización de llamadas.

APP-6	FreePBX	Gestor de configuración de telefonía IP web	Media	La no disponibilidad del servicio afecta la operación cuando se necesite realizar un cambio o una configuración adicional.

- **Sistemas Operativos y Plataformas de virtualización**

Estos activos son el sistema donde corren los servicios y las aplicaciones, por lo que son las plataformas que soportan la operación de los servicios prestados por la organización, por lo que son un activo de suma importancia para el funcionamiento de todos los servicios.

Etiqueta	Activo Informático	Descripción	Criticidad	Justificación
SOP-1	Proxmox	Plataforma de Virtualización Open Source	Media	La no disponibilidad de la plataforma afecta la operación de todos los servicios, pero puede ser fácilmente recuperada con una restauración del servidor.
SOP-2	VMWare	Plataforma de virtualización comercial	Media	La no disponibilidad de la plataforma afecta la operación de todos los servicios, pero puede ser fácilmente recuperada con una restauración del servidor.
SOP-3	Debían 9 Linux	Sistema operativo de software libre de formato .deb	Alta	La no disponibilidad del sistema operativo dejaría por fuera de operación a las aplicaciones web del cliente.

- **Plataformas Cloud**

  Estos activos son el sistema donde corren los servicios y las aplicaciones, por lo que son las plataformas que soportan la operación de los servicios prestados por la organización, por lo que son un activo de suma importancia para el funcionamiento de todos los servicios en la nube.

Etiqueta	Activo Informático	Descripción	Criticidad	Justificación
PCD-1	AWS Amazon	Plataforma de servicios en la nube	Alta	La no disponibilidad del servicio dejaría por fuera a todas las plataformas de e-learning de la organización.
PCD-2	OVH	Servidor dedicado de servicios en la nube	Alta	La no disponibilidad del servicio dejaría por fuera a todas las plataformas de Telefonía IP en la nube de la organización.

- **Hardware**

Activos físicos necesarios para el funcionamiento de los servicios de la organización, como lo son equipos de red, servidores, electricidad, cableado estructurado, etc.

Etiqueta	Activo Informático	Descripción	Criticidad	Justificación
HWR-1	Servidor	Máquina física que integra los servicios web.	Alta	La no disponibilidad de la máquina física, perjudica la operación de todo el servicio web.
HWR-2	Red	Sistema de comunicación de servicios.	Alta	La no disponibilidad de la red afecta toda la operación del servicio web, aunque no sea un problema del servidor.

HWR-3	NAS	Medio de almacenamiento externo.	Media	La no disponibilidad del servicio no afecta la operación de los servicios, pero se corre el riesgo de no guardar las copias de seguridad y la información de los aplicativos web.
HWR-4	Cuarto Técnico	Ubicación de servidores y equipos de comunicaciones.	Baja	La no disponibilidad del servicio afecta la operación cuando se tiene servidores físicos, pero estos problemas caen directamente sobre el cliente.

- **Información del servicio**

Son los datos de información que poseen los servicios y/o aplicaciones de la organización, que es de suma importancia para la operación de los sistemas de información.

Etiqueta	Activo Informático	Descripción	Criticidad	Justificación
IFS-1	Datos Personales	Información personal del perfil de usuario	Baja	Las aplicaciones no manejan datos sensibles de los usuarios que los perjudiquen en la pérdida de información.
IFS-2	Datos de Acceso	Credenciales de acceso a las aplicaciones web	Alta	La pérdida de la información perjudica notablemente la seguridad de las cuentas de usuarios.
IFS-3	Información de cursos	Contenido de los cursos que son implementados	Media	La pérdida de la información perjudica al cliente, pero no es información confidencial.

IFS-4	Información de llamadas	Registro de todas las llamadas realizadas por los usuarios	Alta	La pérdida de información perjudica al cliente en la extracción de informes, estadísticas y revisión de auditoría de llamadas.
IFS-4	Audios de llamadas	Grabaciones de las llamadas realizadas en las aplicaciones web	Alta	La pérdida de información perjudica al cliente en la evaluación de agentes y auditoría de llamadas.

- **Intangibles**

Son los activos vitales para la organización, ya que la empresa vive de la implementación y soporte de los servicios de las TIC, tener una buena reputación y un conocimiento técnico adecuado por todos los empleados que brindan los servicios es de suma importancia, para dar un servicio de excelencia y que satisfaga a los usuarios.

Etiqueta	Activo Informático	Descripción	Criticidad	Justificación
ITG-1	Credibilidad y buena imagen	Buena reputación en la disponibilidad de los servicios web	Alta	La no disponibilidad de los servicios afecta directamente la reputación de la organización.
ITG-2	Conocimiento adquirido	Gestión del conocimiento y adquisición de madurez en los servicios	Media	La pérdida o robo de información afectan a la empresa en temas de competitividad de servicios.

6. Bibliografía

MAGERIT_V3 (2011). Consejos prácticos en la identificación de activos, Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro 1 Método, p. 86-92.

MSPI (2016). Guía para la gestión y clasificación de activos de información, MINTIC. Recuperado: https://www.mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf. 21 de septiembre de 2018.

ANEXO 12

OSP-4 SEGURIDAD EN GESTIÓN DE CAMBIOS

1. Descripción del proceso

El proceso busca prevenir los incidentes de seguridad que se pueden generar en los cambios que se realizan en los activos de TI de los servicios web de la organización, discutiendo con las áreas encargadas de los pasos a considerar para tener continuidad de los servicios después de realizar los cambios sugeridos ante el comité de cambios.

2. Objetivos y metas

- Evitar incidentes y cambios no autorizados que pueden resultar en la ejecución de cambios de seguridad no formales.
- Los cambios autorizados deben ser realizados de acuerdo al cronograma y con los errores mínimos.
- Los cambios que se realizan de emergencia cuando se presenta un incidente de seguridad, son revisados y autorizados después de realizar los cambios respectivos.
- Responder a los cambios del negocio de los clientes.
- Responder a los cambios solicitados por seguridad informática.
- Informar a las partes interesadas de los cambios que se deben de realizar, detallando toda la información y aspectos de los cambios, conociendo los riesgos y los planes de contingencia para resolver problemas en cualquier eventualidad.

3. Métricas

- Porcentajes de cambios detectados por vulnerabilidades de seguridad.
- Porcentaje de cambios no autorizados por vulnerabilidades de seguridad.
- Número de activos de los servicios web pendientes por requisitos de seguridad.
- El número de cambios implementados que cumplen las especificaciones del cliente.
- Los beneficios del cambio en comparación con los costes.
- La reducción en el número de interrupciones del servicio.
- La reducción en el número de cambios no autorizados.

4. Entradas

Son los procesos realizaciones, lo cuales deben de realizar las solicitudes de los cambios, para poder cumplir con los objeticos plateados.

- OSP-5 Actualizaciones de seguridad.
- OSP-7 Endurecimiento de activos gestionados de TI.
- OSP-21 Calidad de información y evaluación de cumplimiento.

5. Gestión del cambio

Los cambios son necesarios para la organización, cuyo principal objetivo es reducir y/o mitigar los incidentes de seguridad de una manera proactiva o reactiva; con el propósito de, minimizar la exposición del riesgo informático, la gravedad del impacto y las interrupciones del servicio e implementar cambios que sean correctos para los activos de la organización de los servicios WEB de la organización.

La empresa crea un grupo de comité de cambios, donde los responsables de garantizar que los cambios sean registrados, evaluados, autorizados, priorizados, planificados, probados, implementados, documentados y revisados de una manera controlada por los coordinadores y gerentes responsables de los cambios realizados por el personal de la organización.

El comité de cambios son los responsables de ejecutar las siguientes actividades:

- Planificación y control de cambios.
- Programación de cambios y entregas.
- Comunicaciones.
- Toma de decisión y autorización de cambios.
- Aseguramiento de que existan planes de corrección.
- Medición y control.
- Generación de informes de gestión.
- Entendimiento del impacto.
- Mejora continua.

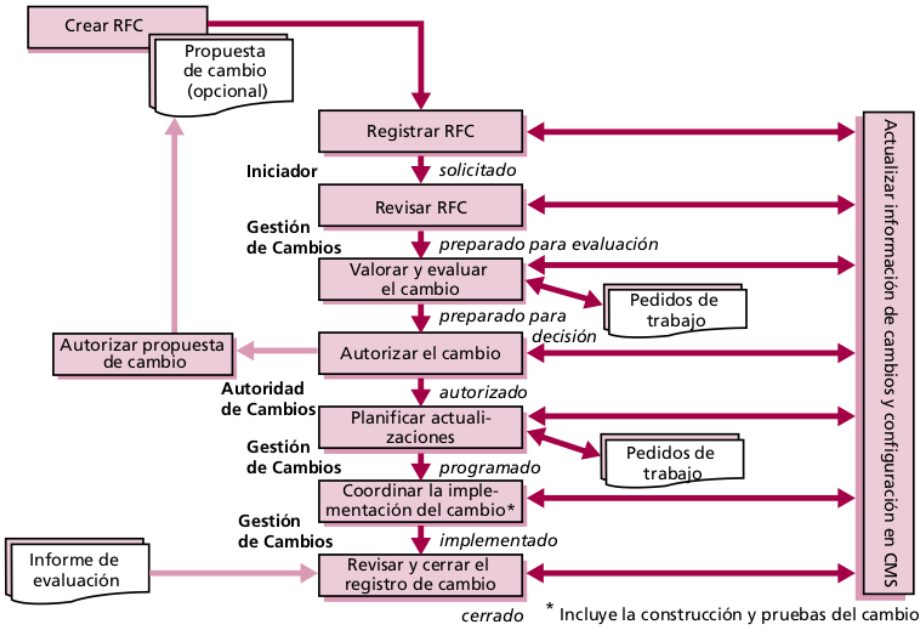
Toda el área de seguridad informática debe analizar y evaluar el impacto de los cambios que se deben de realizan en los servicios web de la organización, con el propósito de no afectar la disponibilidad de los activos de información, por lo que se crea una RFC como guía para solicitar los cambios de seguridad necesarios.

RFC SGSI Nethexa

Al llenar la RFC se envía al comité de cambios, el cual se reúne cada mes a evaluar los cambios solicitados, encargados de las siguientes actividades:

1. Creación y registro de solicitud de cambio (RFC).
2. Revisión de RFC y de propuesta de cambio.
3. Valoración y evaluación del cambio.
4. Autorización del cambio.
5. Actualización de planes.
6. Coordinación de la implantación del cambio.
7. Revisión y cierre del registro de cambio.

Figura 1: Flujo se procesos de gestión de cambios (ITIL_V3, 2011).



Como se muestra en la imagen, se debe seguir adecuadamente el proceso, revisando el motivo por el cual se deben de realizar los cambios en el activo de información y cuál es la mejora y/o incidencia que se va a solucionar, mitigando los problemas de seguridad de manera reactiva o proactiva.

Como todos los cambios que se realizan en los activos de información no son planeados, ya que pueden ocurrir incidentes de seguridad que se deben de contener de manera inmediata para preservar la disponibilidad de los servicios, se deben de tener presente las siguientes prácticas a nivel de gerencia.

- Evaluar, priorizar y autorizar cambios solicitados.

Se deben de evaluar todas las peticiones de cambios que son solicitados; con el fin de, determinar el impacto que puede generar en los procesos del negocio y los servicios de TI, analizando los riesgos que se deben de tomar operativamente, preservando la continuidad de los servicios web de la organización. Asegurando que todos los cambios que son autorizados se les puedan dar un nivel de priorización, dependiendo del nivel del riesgo que se va a mitigar o minimizar en la implementación o corrección de controles de seguridad en los activos de TI.

La priorización se da en 4 niveles:

- Prioridad baja: Un cambio deseable, pero que puede esperar hasta una mejor oportunidad.
- Prioridad media: Un cambio sin demasiada urgencia o impacto, pero que no se puede retrasar. El Comité de Cambios da a este cambio una prioridad media a la hora de asignar recursos.
- Prioridad alta: Un cambio que se refiere a un fallo grave para varios usuarios o un fallo molesto para un gran número de usuarios, o que está relacionado con otros problemas urgentes. El Comité de Cambios dará a este cambio la máxima prioridad en su siguiente reunión.
- Prioridad inmediata: Un cambio relacionado con un fallo que causa graves pérdidas de ingresos o que impide prestar importantes servicios web de la organización. Requiere una acción inmediata.

- Gestionar los cambios de emergencia.

Los cambios de emergencia se presentan cuando se posee un incidente de seguridad o un problema que pueda prestar el servicio que afecte la disponibilidad y continuidad del servicios web de la organización, estos casos son de manera urgente y se convoca una reunión extraordinaria para evaluar los problemas presentados y cómo se van a ejecutar la implementación de controles y correcciones del servicio, aprobando de manera inmediata la RFC para poder actuar y solucionar los problemas presentados en el menor tiempo posible. Luego de pasar el incidente se realiza la documentación de los cambios y realizar un informe con las causas y los pasos que se realizaron para solucionar los problemas presentados, donde también hace un análisis para corregir futuros problemas que se pueden presentar y pasarlos al comité de cambios para su debida aprobación.

- Realizar seguimiento e informar los cambios solicitados.

Tener un sistema de seguimiento y de informes, que documente y permitan auditar los cambios rechazados, el estado de los cambios aprobados y los procesos realizados de los cambios realizados. Asegurando que los cambios

aprobados se han implementados como se tenían previstos en la RFC y que se envié toda la documentación de cambios de las causas a mejorar para que sean corregidas; con el propósito de, realizar todos los cambios que generen mejoras en la disponibilidad de servicios, a través de mejoras en seguridad informática.

- Cerrar y documentar los cambios.

Cuando los cambios son implementados y actualizados correctamente, se alimenta la documentación de la solución y los procedimientos que pueden afectar el cambio, estos cambios se suben a la documentación del servicio web como mejora y se realiza una retroalimentación como gestión del conocimiento en la organización a las áreas encargadas.

6. Bibliografía

ISO_27001 (2013). Sistema de gestión de seguridad de la información (SGSI) colombiano. Recuperado: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf. 12 de agosto de 2018.

CIBIT_5 (2012). Proceso BAI-06: Gestionar los cambios. Objetivos de control las tecnologías de información y relacionadas. Recuperado: https://adminsisuc201701.wordpress.com/bai06/. 8 de septiembre de 2018.

ITIL_V3 (2011). Gestión de cambios, Transición del servicio basada en ITIL V3. p. 60-71.

ANEXO 13

OSP-5 ACTUALIZACIONES DE SEGURIDAD

1. Descripción del proceso

El proceso permite controlar las actualizaciones de seguridad que se realizan en los sistemas de información, con el fin de prevenir los incidentes y la explotación de nuevas vulnerabilidades. Con el propósito de aplicar las actualizaciones de parches de seguridad a los sistemas y aplicaciones, evitando la explotación de incidentes de seguridad que son derivados de las vulnerabilidades que surgen con el tiempo.

2. Objetivos y metas

- Mitigar y/o disminuir las vulnerabilidades que surgen con el tiempo en los servicios base.
- Mantener los activos de información actualizados.
- Mejorar la seguridad y las funcionalidades de los servicios constantemente.

3. Métricas

- Cantidad de parches de seguridad implementados con el fin de corregir las vulnerabilidades identificadas.
- Cantidad de parches de seguridad pendientes de implementación por criticidad del activo de información.
- Nivel de actualización de la red.

4. Entrada

La entrada que posee el proceso es la OSP-3 Inventario de activos, donde se encarga de analizar e identificar las nuevas actualizaciones que se le pueden realizar a todos los activos de información de los servicios web de la organización.

5. Gestión de parches de seguridad de los activos de información.

Toda la actualización de los activos de información, ya sean de seguridad o de funcionalidad, deben de estar guiados por este proceso; encargado de analizar y evaluar las actualizaciones que se pueden implementar en los activos de información que ayuden a robustecer y mejorar la seguridad de los servicios web de la organización.

El propósito de la gestión de actualizaciones de los activos de los servicios web, es hacer un cambio de cultura en el entorno de la administración de los servicios de TI, cambiando el paradigma de tecnología estática funcional, a la proactividad del cambio en la actualización de las aplicaciones, servicios y firmware que se pueden generar en las plataformas web que ayuden a mejorar la estabilidad, continuidad, seguridad y disponibilidad de servicios a todos los clientes.

El proceso propone 6 fases para realizar el seguimiento y la correcta implementación de las actualizaciones de los activos:

- Identificación del software base de los activos

Se identifica el software base con que trabajan todos los activos de información que lo requieran y el nivel de actualizaciones que tiene cada uno de ellos, porque teniendo esta información base nos permitirá llevar cambios en los sistemas sin riesgos y permite volver a un estado previo que es conocido y funcional, en el caso de tener un problema a la hora de instalar una actualización.

Para la identificación del software base del sistema y para validar las actualizaciones podemos utilizar herramientas de escaneo de servicios y vulnerabilidades como los son nmap, Nessus, Owasp Zap, entre otras. Las cuales nos pueden arrojar información importante cuando se aplican en el análisis de riesgos y poder seguir los procedimientos adecuando de este proceso.

- Disponibilidad

El principal problema de las actualizaciones del software base, es que puede presentar problemas con el funcionamiento de las aplicaciones que actualmente está corriendo en el sistema, generando problemas en el funcionamiento de los servicios que son prestados a los clientes de la empresa, por lo que se realiza un análisis de las afectaciones que se pueden tener en cada uno de los activos de información.

- Aplicabilidad

Todos los parches de seguridad que contienen las actualizaciones de los servicios base de las plataformas web de la organización no siempre son válidos para todas las distribuciones de software o para los dispositivos, por lo que se realiza la verificación de que las actualizaciones se puedan aplicar en todas las distribuciones de software y dispositivos; de no ser así, se revisan cuáles son los procesos que se tienen que realizar para tomar una

decisión en aceptar o no el nivel de riesgo, que se puede generar no seguir actualizando los diferentes activos de información que no lo permiten.

- Adquisición

Obtener los ficheros de actualización de la página principal del fabricante del software, comprobando la veracidad de la actualización, analizando que los paquetes a instalar sean confiables y no contengan malware que pueda afectar a la plataforma web de la organización. También es importante verificar el hash de la descarga del paquete sea igual.

- Validación

El principal objetivo de la validación es poder probar y asegurar que la actualización no impacta de forma adversa el funcionamiento de las plataformas web de la organización, realizando escenarios de prueba y error en activos de información en un ambiente de pruebas. También, se pueden realizar los cambios creando una copia y un Snapshot de la máquina; con el fin de, poder actualizar el activo de información y de no ser exitosas las pruebas poder restaurar el activo a un punto anterior.

- Despliegue

Cuando se terminan de hacer todas las validaciones, se crea un proceso de despliegue, permitiendo la implementación de las actualizaciones en todos los activos realizando los cambios pertinentes, informando de los procedimientos de instalación y los ficheros necesarios al comité de cambios, para evaluar el riesgo y la importancia para la organización de las correcciones que se van a realizar para mejorar la seguridad de los activos de información.

6. Bibliografía.

CERT de Seguridad e Industria (2018). Gestión de parches en sistemas de control. Recuperado: https://www.certsi.es/blog/gestion-parches-sistemas-control. 9 de septiembre de 2018.

ANEXO 14

OSP-7 ENDURECIMIENTO DE ACTIVOS GESTIONADOS DE TI

1. Descripción del proceso

El proceso permite madurar las configuraciones de los servicios, canales, puertos, interfaces y repositorios, mejorando la confiabilidad, integridad y disponibilidad de la seguridad en los activos de información.

2. Objetivos y metas

- Mejorar la seguridad física de los activos de información.
- Reducir las vulnerabilidades que poseen los activos de información, deshabilitando las configuraciones estándar del sistema que no son necesarias para el funcionamiento de los servicios web.
- Asegurar el funcionamiento de las plataformas web del servidor, robusteciendo las configuraciones de red, permisos de usuarios y configuraciones básicas de los servicios locales de los activos de información.

3. Métricas

- Número y porcentaje de activos de TI con requerimientos de seguridad pendientes.
- Número de medidas de seguridad implementadas que solucionan incidentes y/o vulnerabilidades de seguridad identificadas.

4. Entrada

El proceso está encargado de revisar y asegurar los activos de información de la organización, por este motivo solo se centra en asegurar los activos que se encuentran en el proceso OSP-3 Inventario de activos**.**

5. Hardening de servidores

El propósito de este proceso es poder realizar un endurecimiento de los activos en los servicios web de e-learning y telefonía IP de la organización, disminuyendo la probabilidad de los atacantes que puedan afectar las plataformas web, materializando las vulnerabilidades que contengan los servidores que se encuentran en funcionamiento.

La capa de hardening del servidor, es una de las más importantes para la organización; ya que la empresa cuando presta los servicios web puede o no tener también la administración de la demás capaz de seguridad que protegen los activos de las plataformas web. Por este motivo, este proceso ayuda a fortalecer la seguridad de los servidores, reduciendo las vulnerabilidades que pueden ser materializadas interna o externamente en las instalaciones de los clientes y cuando se encuentran publicadas en Internet.

El aseguramiento de los servidores web es un punto más dentro de la cadena de seguridad que se implementa para proteger las plataformas web de la organización, por esta razón se ejecuta como mínimo las siguientes actividades para tener la seguridad de los activos asegurados:

- Aseguramiento de ataques físicos

Es el aseguramiento que se puede realizar en el hardware de los servidores que contiene las plataformas web de la organización, lo cuales deben de tener los siguientes requisitos de seguridad:

  - Actualizaciones de firmware de los servidores y dispositivos de almacenamiento.
  - Establecer contraseñas complejas para el ingreso del sistema de arranque de los equipos.
  - Configuración adecuada de la BIOS.
  - Habilitar que el inicio del sistema se establezca sólo con la unidad del disco principal.
  - Deshabilitar dispositivos ópticos y USB.
  - Protección y monitoreo de seguridad física para los activos físicos en la organización.
  - Accesos restringidos a los activos de información físicos.
  - Vigilancia de cámaras de seguridad.

- Instalación segura del sistema operativo

Actividad encargada de establecer las pautas mínimas que se deben de tener presentes al momento de implementar un nuevo servidor, asegurando la estabilidad y la seguridad del sistema operativo.

  - Implementación de sistema de virtualización en clúster.
  - Asignación de recursos necesarios para el correcto funcionamiento del servidor.
  - Instalación de al menos dos particiones primarias para la separación del sistema operativo de los datos de información.

- Instalación de un sistema de archivos que contenga prestaciones de seguridad y pueda converger con el sistema operativo.
- Instalación de cifrado de datos en las particiones del servidor.
- Instalación mínima del sistema operativo, evitando instalar servicios que no sean necesarios para el funcionamiento de las plataformas web.
- Instalación y protección del sistema de arranque.
- Configuración de Snapshot y copia de la imagen de los servidores constantemente.

- Instalación, configuración y mantenimientos de aplicaciones de seguridad

Actividad encargada de implementar y mantener las aplicaciones de seguridad que se instalan en el servidor; con el fin de analizar el tráfico que ingresa y sale del servidor, protegiéndolo de amenazas de seguridad que se encuentran presentes en el funcionamiento del activo de información. El servidor debe tener las siguientes aplicaciones instaladas localmente:

- Antivirus
- Antispyware
- Anti spam
- Firewall local
- Cifrado Open SSL
- Monitoreo de correlación de eventos de seguridad

- Configuración de políticas locales del sistema

Asegurar los permisos que son otorgados en el manejo del servidor localmente, reduciendo el riesgo de elevación de privilegios y el acceso no autorizado a los archivos de configuración del servidor. Se realizan las siguientes actividades de seguridad:

- Contraseñas robustas y complejas
- Caducidad de contraseñas
- Almacenamiento histórico de contraseñas
- Bloqueo de cuentas de usuarios por intentos de sesión erróneos.
- Creación y eliminación de usuarios estándar del sistema.
- Asignación de permisos de usuarios.
- Reducir las posibilidades de elevación de privilegios de usuarios
- Configuración de opciones de seguridad generales del sistema

- Restricciones de software

  Configuración de listas blancas del software que es permitido en el servidor, con el objetivo de que cualquier otro software que no se encuentre en la lista no pueda ser instalado, reduciendo la instalación de malware en el sistema operativo.

- Configuración de los servicios del sistema

  El objetivo de esta actividad es desactivar todos los servicios que posee el sistema operativo y que no son necesarios para el correcto funcionamiento del servidor. También, configurando los servicios que están corriendo en el servidor y que son necesarios, no contengan configuración por defecto que afecte la seguridad de las plataformas web de la organización.

- Configuración de red

Es necesario deshabilitar todos los protocolos que no son utilizados y que se encuentran habilitados en los sistemas operativos del servidor, limitando el uso de protocolos de comunicación que no son utilizados, evitando vulnerabilidades de seguridad que pueden afectar los puertos de red abiertos en los servidores.

- Configuración de permisos de seguridad de archivos y directorios

Revisar los permisos de directorios y archivos, revisando el nivel de permisos y los usuarios que pueden leer y modificar archivos de configuración, asignando los permisos adecuados a los usuarios del sistema y eliminados usuarios anónimos que vienen por defecto en el sistema operativo. Haciendo el uso adecuado de los permisos a nivel de usuarios y archivos, evitando el acceso no deseado a los contenidos que poseen los servicios web de la organización.

- Configuración de opciones de seguridad de las aplicaciones

Restringir la seguridad de las aplicaciones que se encuentran instaladas en el sistema operativo, permitiendo ejecutar los procesos necesarios reduciendo los procesos que no son utilizados por las plataformas web de la organización; evitando que un software malicioso ejecute procesos innecesarios en el servidor.

- Configuraciones de acceso remoto

Cuando sea necesaria la administración del servidor por accesos remoto, se deben de tener presentes los siguientes requisitos en el servidor:

- Restringir el acceso a un número limitado de usuarios.
- Restringir el número de conexiones concurrentes de acceso remoto.
- Configuración de cierre de sesión por inactividad del usuario.
- Establecer la comunicación del acceso remoto cifrado de la conexión.
- Instalar herramientas de acceso remota seguras debidamente analizadas.
- Hacer uso de llaves de seguridad para el ingreso seguro al servidor.
- Utilizar autenticación de dos factores de ser necesario.

- Cifrado de archivos o unidades de almacenamiento

Cifrar todos los datos del servidor, teniendo mucho cuidado con el adecuado almacenamiento seguro de las llaves del cifrado de los archivos y de unidades de almacenamiento; con el fin de, preservar la información crítica de los servicios web de la organización evitando fuga de información sensible.

- Realizar respaldos frecuentes de los archivos y del sistema

Realizar copias de seguridad frecuentes a los archivos de configuración, bases de datos y a los servidores, con el objetivo de poder recuperar la información y los servicios ante un incidente de seguridad que afecte la disponibilidad y continuidad de las plataformas web de la organización.

- Almacenar los respaldos de información locamente.
- Almacenar los respaldos en una unidad de almacenamiento externa.
- Almacenar los respaldos en la nube.

6. Bibliografía

Scarfone, K., Jansen. W. & Tracy, M. (2008). Guide to General Server Security, NIST 800-123. Recuperado: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-123.pdf. 10 de septiembre de 2018.

Callejas, A. (2014). Seguridad y Hardening de Servidores Linux. RedHat. Recuperado: http://www.rootzilopochtli.com/wp-content/uploads/2015/01/Seguridad_y_Hardening.pdf. 10 de septiembre de 2018.

Pichel, F. (2011). Hardening Básico de Linux Permisos y Configuraciones, Internet Security Auditors. Recuperado: https://es.scribd.com/document/351733368/Hardening-basico-de-Linux-Permisos-y-Configuraciones-pdf. 10 de septiembre de 2018.

ANEXO 15

OSP-10 GESTIÓN DE COPIAS DE SEGURIDAD

1. Descripción del proceso

Proceso encargado de reducir el impacto ante la pérdida de información, cumpliendo con los niveles de servicios de la organización en la copia y restauración de las copias de seguridad

2. Objetivos y metas

- Mitigar los incidentes derivados de la pérdida de información de repositorios y procesos de copias de seguridad.
- Realizar copias de seguridad determinando la periodicidad y la prioridad del backup.
- Garantizar la confidencialidad, integridad y disponibilidad ante una pérdida de información de los servicios web.

3. Métricas

- Cantidad de backup exitosos.
- Cantidad de pruebas de restauración exitosas.

4. Entrada

El proceso está encargado de analizar el proceso Inventario de activos (OSP-3), verificando que se realicen adecuadamente las copias de seguridad.

5. Gestionar las copias de seguridad

Para la organización es de vital importancia que los datos almacenados de configuración, contenido de cursos, audios de llamadas, registros de llamadas, etc. En los servidores de e-learning y telefonía IP que son administrados a los clientes, no se presente un incidente de pérdida total o parcial de los datos de información que son almacenados en el servidor de manera local, ya que los datos de la operación son muy importantes para todos los clientes, ya que son un medio de poder analizar la operación y obtener información necesaria para la operación.

Cuando se implementa un servicio de e-learning y telefonía IP, las plataformas web son un medio para poder agregar, modificar o eliminar

información que es valiosa para los clientes, ya que las plataformas solo es un medio para captar información de los contenidos recopilados en la operación, pasando la información como las más relevante en los servicios prestados por la empresa.
La información es la más valiosa y perder datos de información es muy delicado; por el motivo, de que los clientes pueden perder tiempo de trabajo al fallar una unidad de almacenamiento que contengan los equipos que se encuentran en operación. Las fallas de las unidades de almacenamiento se pueden dar por los siguientes motivos:

- Falla del medio de almacenamiento.
- Operación incorrecta por parte del personal de soporte.
- Ataques internos y externos.
- Incompatibilidad con el hardware.
- Problemas en las aplicaciones o drivers que generen comportamientos inesperados que afecten el almacenamiento de la información.
- Desaparición o pérdida del medio de almacenamiento.

Teniendo presentes todos los problemas que se pueden generar en los medios de almacenamiento, que permiten la operación de todos los activos de información de la organización, se consideran las siguientes tareas en los medios de destino:

- Almacenar en un medio de almacenamiento externos los datos originales generados por las plataformas web.
- Los Backups no pueden estar en el mismo sitio físico de los servidores que contienen la información original.
- Los medios de almacenamiento deben de guardarse en un lugar seguro, seco y fresco.
- La información tiene que organizarse y etiquetarse de una manera ordenada y clara.
- Se debe verificar que los datos almacenados como backup, son los mismos que los datos originales.

No solo los datos generados por las plataformas web son los que se deben de resguardar, también es importante poder realizar backup de las configuraciones de los servicios y aplicaciones que son utilizados para el funcionamiento de los sistemas de información, por este motivo se deben de tener presentes las siguientes actividades:

- Realizar copias de seguridad a los archivos de configuración.
- Realizar copias de seguridad de las bases de datos.

- Hacer copias de seguridad de más máquinas virtuales constantemente.
- Almacenar las copias de seguridad en un medio de almacenamiento en red.
- Almacenar la información de los backup en la nube, con la finalidad de tener un respaldo seguro y siempre disponible.
- Actualización periódica de Backups completos, incrementales y diferenciales, como lo defina la política del activo de información.
- Implementación de escenario de pruebas de restauración de Backups de los activos de información.

6. Bibliografía

Montoya, M. (2006). Copias de seguridad, mailxmall.com. Recuperado de http://www.nacio.unlp.edu.ar/archivos/concursos/copias-seguridad-5002.pdf. 12 de septiembre de 2018.

Ballen, D. & Díaz, J. (2015). Diseño de proceso de copias de seguridad de TI de la subdirección de innovación y servicios tecnológicos que apoyen el modelo GRC para el Instituto Nacional de Metrología-INM, Universidad Católica de Colombia. Recuperado de https://repository.ucatolica.edu.co/bitstream/10983/2473/1/proyecto%20INM.pdf. 12 de septiembre de 2018.

ANEXO 16

OSP-15 GESTIÓN DE CONTINUIDAD DE OPERACIONES

1. Descripción del proceso

Utilizar redundancia y dispersión con el fin de eliminar puntos críticos de falla y reducir el impacto de los incidentes que generen la degradación de la imagen de la organización, implementando todos los requerimientos regulatorios y de la organización para acotar el tiempo de los incidentes que se puedan presentar.

Proceso encargado de proporcionar redundancia y eliminación de puntos críticos de falla, reduciendo el impacto que pueden generar incidentes, acortando los tiempos de respuesta ante incidentes que afectan los activos de TI.

2. Objetivos y metas

- Evitar que la organización sea afectada por eventos que generan dificultad en la prestación constante de servicios de los clientes.
- Mejora continua de los procesos realizados en el sistema de gestión de seguridad de la información.

3. Métricas

- Cantidad de pruebas realizadas del plan de continuidad de operaciones durante el periodo establecido.

4. Entradas

- Inventario de activos (OSP-3).
- Reporte de backup (OSP-10).
- Reporte de restauración (OSP-10).
- Análisis de impacto del negocio (BIA).

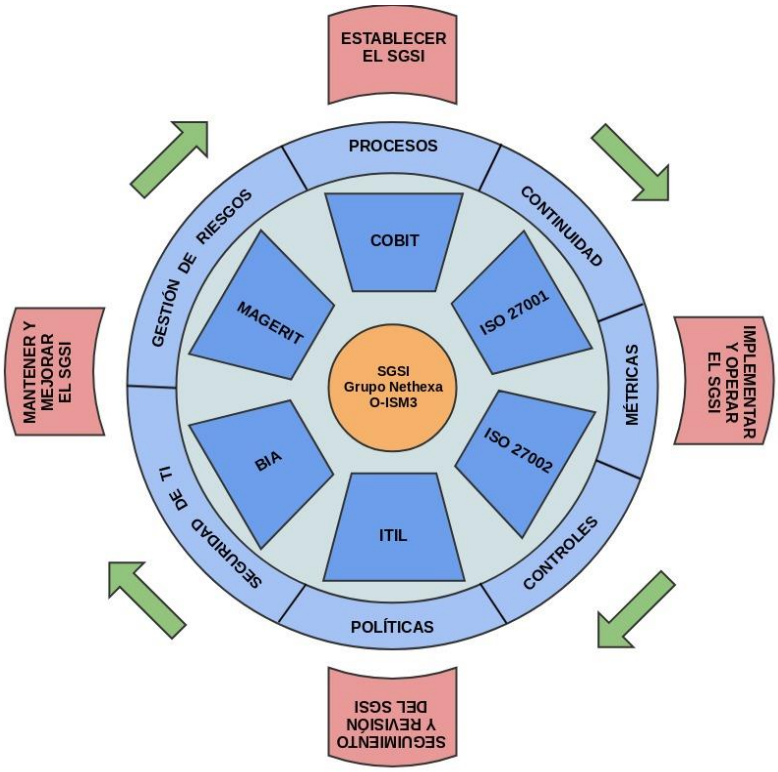
5. Plan de continuidad de las Operaciones

El sistema de gestión de seguridad de la información es desarrollado por la organización, donde contiene un conjunto de prácticas de seguridad informática, permitiendo la eficacia de los sistemas de información que comprenden las plataformas web de la organización; con el propósito de, seguir operando continuamente ante incidentes de seguridad que se pueda

presentar en los activos de información, implementando estrategias adecuadas en la recuperación de desastres informáticos y planes de gestión de crisis, que afecten la seguridad de la organización.

Las estrategias a tener en cuenta son las siguientes:

- Adaptación del sistema de gestión de seguridad O-ISM3.
- Implementación de análisis de riesgos, que permita a ayudar a la organización en la toma de decisiones, en la planificación e implementación de controles de seguridad a los activos de información que presentan riesgos que comprometan la disponibilidad de los servicios prestados por la empresa.
- Implementación de controles de seguridad que permitan reducir y/o mitigar los riesgos que son perjudiciales para la organización.
- Auditoria constante del adecuado manejo y aplicación de los diferentes procesos de seguridad que permiten mejorar la seguridad de los servicios web de la empresa.
- Se establece un ciclo de mejora continuidad, el cual contiene todos los estándares, metodologías y contenidos de suma importancia para la adopción y el mejoramiento continuo del sistema de gestión de seguridad de los servicios web de manera integral.



- Establecer el SGSI

    - Planificar los procesos y políticas.
    - Detallar la información del contenido de los procesos.
    - Establecer los objetivos y metas por los procesos.
    - Establecer las métricas para evaluar los procesos.

- Implementar y Operar el SGSI

    - Ejecutar los procesos y políticas.
    - Proporcionar los resultados a través de métricas.
    - Documentar las acciones realizadas.
    - Informar de los controles de seguridad informática que se deben de implementar en los activos de información.

- Seguimiento y Revisión del SGSI

    - Verificar la ejecución de los procesos y políticas de seguridad.
    - Recopilar los datos de métricas y analizarlos.
    - Revisión de los resultados obtenidos en los activos de información.
    - Documentación de las conclusiones.
    - Auditoría a todos los procesos del SGSI.

- Mantener y mejorar el SGSI

    - Modificar los procesos según los resultados y las mejoras que se encuentren que ayuden a fortalecer la seguridad de la organización.
    - Actualizar y documentar la información de las mejoras realizadas a los procesos.

6. Beneficios

- Adquisición de responsabilidades impuesta por las políticas y procesos establecidos por la organización.
- Identificación y disminución de vulnerabilidades y/o amenazas que poseen los activos de los servicios web de la organización.
- Participación de seguridad informática por la organización.
- Mejora de la disponibilidad de los servicios al mejorar la seguridad de los activos de información.
- Garantizar la seguridad a las partes interesadas.
- Mora de la conciencia en seguridad al aplicar controles de seguridad en la organización.

7. Bibliografía

ISO_27001 (2013). Sistema de gestión de seguridad de la información (SGSI) colombiano. Recuperado: http://intranet.bogotaturismo.gov.co/sites/intranet.bogotaturismo.gov.co/files/file/Norma.%20NTC-ISO-IEC%2027001.pdf. 12 de agosto de 2018.

UrbiCAD (2015). Plan de Continuidad de Operaciones. Recuperado: http://www.safety-management.eu/PDF/normas_bcm.pdf. 13 de septiembre de 2018.

ANEXO 17

OSP-16 GESTIÓN DE TRÁFICO DE RED

1. Descripción del proceso

Define las políticas técnicas de la gestión de tráfico de mensajes y paquetes de datos autorizados en las diferentes zonas de red, detectando y analizando el tráfico no autorizado, también cifrando el tráfico como lo defina la política.

2. Objetivos y metas

- La segmentación de red y repositorios, junto con el filtrado de mensajes y paquetes, pueden prevenir y mitigar incidentes de seguridad.
- La implementación de dispositivos de red que contengan servicios de seguridad, robustece la seguridad de los activos de información.

3. Métricas

- Cantidad de servicios de seguridad implementados en la red.
- Cantidad de reglas de firewall por cantidad de bloqueos.
- Número de ataques bloqueados por la seguridad en la red.

4. Gestión de Tráfico de Red Seguro

La seguridad perimetral de la red es de suma importancia para la constante operación y disponibilidad de los servicios web de la organización, teniendo sistemas de red que permitan proteger lógicamente las plataformas web de la organización directamente por ataques que pueden generarse, por intrusos que tiene una mala intención contra la organización.

La finalidad del proceso es poder tener una primera línea de defensa en la red, que proteja a los servidores web de ataques informáticos los cuales se pueden generar desde la red externa e interna, añadiendo una capa de seguridad adicional que debe ser vulnerada para poder llegar directamente a los servidores internos en la red.

Las funciones básicas a las que llega la organización para proteger a los servidores a nivel de red son:

- Resistir los ataques informáticos que se realizan desde la red externa.

- Identificar y detectar los ataques informáticos sufridos y alertar de ellos de manera automática.
- Segmentar las redes de la organización, con el objetivo de tener mejor seguridad en la red y disminuir los ataques de red al tener los servidores menos expuestos.
- Filtrar y bloquear el tráfico, permitiendo solamente el tráfico que es necesario para el funcionamiento de los servicios web de la empresa.

Con el propósito de cumplir con las principales funciones de una seguridad perimetral, se deben adquirir herramientas de seguridad perimetral informática y establecer un análisis de las reglas que se deben crear en las herramientas, con el fin de, establecer las configuraciones necesarias que permitan reducir y mitigar los riesgos informáticos de la organización. Para cumplir con la seguridad mínima, se deben de realizar los siguientes controles básicos de seguridad, determinados por el análisis de riesgos:

- Establecer e implementar una adecuada segmentación de red internamente, con el objetivo de separar la red de los servicios web de los demás servicios.
- Diseñar un direccionamiento de red interno que permita establecer la adecuada comunicación con las demás redes de la compañía, permitiendo la fácil gestión de configuraciones de seguridad que se puedan presentar en la red del cliente.
- Tener un Firewall en red que permita o deniegue el tráfico establecido, reduciendo el ingreso a los dispositivos directamente.
- Configurar el direccionamiento de los servidores con direccionamiento privado y realizar NAT desde la zona perimetral, para no permitir que sea accedido directamente, denegando los servicios web que poseen el direccionamiento público directamente, reduciendo el impacto del riesgo por las amenazas que son encontradas constantemente.
- Implementar un sistema de detección y prevención de intrusos de red, los cuales permiten monitoreo y alertas de seguridad en tiempo real en la red del perímetro de los servidores, bloqueado y reportando el tráfico sospechoso que ingresa a la red.
- Implementación de antivirus y anti spam en la red, evitando afectar a los activos de información de los servicios web de la organización.
- Tener el servicio de sandbox, permitiendo el análisis directo del malware o ataques informáticos que son generados.
- Tener mitigación de ataques de denegación de servicio distribuido.
- Implementar filtro de contenido en los servidores web, permitiendo el ingreso solo a sitios web seguros para la descarga de actualizaciones.
- Integrar a la solución del servicio web de e-learning y telefonía IP firewall de aplicaciones web, con el fin de, poder implementar un sistema de seguridad que pueda ser analizado por capas superiores.

Con esta solución de seguridad perimetral, los servicios web de la organización pueden tener una capa de seguridad muy robusta e importante que es vital para el mejoramiento constante de las organizaciones a nivel de seguridad informática.

ANEXO 18

OSP-17 GESTIÓN DE PROTECCIÓN CONTRA MALWARE

1. Descripción del proceso

Proceso encargado de imponer las medidas de seguridad necesarias para proveer protección contra amenazas de seguridad como virus, spyware, troyanos, backdoors, key loggers, rootkits, ataques persistentes avanzados, entro otros servicios no autorizados.

2. Objetivos y metas

- Una protección de malware que permite prevenir y/o mitigar los niveles de incidentes de seguridad relacionados con la infección de activos informáticos.
- Proteger la integridad de los activos de información de las plataformas web.

3. Métricas

- Nivel de actualización contra malware para los sistemas de información.
- Número de equipos desactualizados.

4. Protección contra Malware

Los activos de información están expuestos a códigos maliciosos que pueden generar problemas en el funcionamiento de los servicios, la integridad de los datos de información y en la pérdida de los sistemas de información; por este motivo, se requieren precauciones para evitar y detectar la infección de código malicioso en los servicios de e-learning y telefonía IP.

Todo tipo de software y servicio de información que puede procesar información es vulnerable en la introducción de código malicioso, como los virus, gusanos de red, spyware, troyanos, backdoors, key loggers, rootkits, ataques persistentes avanzados, entro otros servicios no autorizados. Los usuarios del sistema deben de ser responsables y dar un excelente manejo de los sistemas de información web de la organización, para evitar incidentes de seguridad en los activos de información.

La finalidad del proceso es poder tener la capacidad de introducir controles de seguridad que eviten, detecten y retiren los códigos maliciosos que están amenazando a los activos de información de las plataformas web de la organización; por esta razón, se deben de implementar controles de detección, prevención y recuperación de los sistemas de información, protegiéndolos contra cualquier código malicioso que pueda ingresar a la infraestructura de la organización.

Cumpliendo con las buenas prácticas de seguridad, se deben de proteger todos los activos de las plataformas web con protección contra códigos maliciosos, conciencia de los usuarios por la seguridad, control de accesos a los sistemas de información y controles de gestión de cambios.

Para seguir los lineamientos de la norma debemos de implementar las siguientes directrices:

- Establecer políticas de seguridad que prohíba el uso de software no actualizado en los servicios web de la organización.
- Establecer políticas de protección contra los riesgos asociados a la descarga de archivos y software desde redes internas y externas, indicando los contenidos y los sitios recomendados, tomando medidas de protección.
- Realizar revisiones periódicas del software instalado y los contenidos de datos que posee los sistemas de información, con el fin de poder detectar la presencia de software y contenido inusual en las plataformas web de la organización.
- Hacer uso regularmente de software de detección y reparación de software malicioso; con el propósito de; explorar los servidores de manera concurrente como un control preventivo que ayude verificar el código malicioso.
- Definición de responsabilidades y procedimientos de gestión de seguridad, que permitan reaccionar de manera oportuna ante un incidente de seguridad, con la contención y la recuperación de los sistemas de información.
- Establecer planes de continuidad del negocio, que permita recuperarse totalmente ante un ataque de código malicioso.
- Recolectar y analizar información de seguridad, permitiendo estar actualizo ante una vulnerabilidad y/o riesgo que pueda ser aprovechado por un atacante, nutriendo de información a la organización de los nuevos ataques informáticos que se pueden sufrir, reaccionando proactivamente ante estas dificultades.
- Implementar procedimientos perimetrales y locales que permitan la identificación y erradicación de malware al instante, que permita la continuidad del servicio web.

5. Bibliografía

ISO_27002 (2005). Protección contra códigos maliciosos y móviles. Recuperado: http://www.slinfo.una.ac.cr/documentos/EIF402/ISO27001.pdf. 18 de septiembre de 2018.

ANEXO 19

OSP-21 CALIDAD DE INFORMACIÓN Y EVALUACIÓN DE CUMPLIMIENTO

1. Descripción del proceso

Proceso encargado de la revisión periódica de la información de seguridad informática, garantizando el cumplimiento de las políticas y los procesos establecidos por la organización.

2. Objetivos y metas

Reducir los incidentes de seguridad que son ocasionados por la mala clasificación de la información, a nivel de completitud, exactitud y expiración, a través de un proceso de auditoría.

3. Métricas

- Cantidad de issues remediados por procesos de auditoría.
- Estado de cumplimiento por ente de control.

4. Calidad de información y evaluación de cumplimiento.

El propósito fundamental del proceso es hacer un seguimiento constante del cumplimiento de todos los procesos establecidos en el SGSI, ejecutando todos los requisitos regulatorios, contractuales y adopción de buenas prácticas que apoyen la mejora continua de los procesos de seguridad informática en la organización.

Para cumplir el objetivo del proceso es necesario hacer un seguimiento de auditoría que abarque el seguimiento, medición, análisis y evaluación de los procesos y política establecidos en el SGSI, con el propósito de encontrar los errores o debilidades del sistema de gestión y mejorarlos de manera continúa realizando métricas de cada proceso del proceso de auditoría.

La empresa establece lo siguiente:

- Realizar seguimiento y medición de métricas de los procesos establecidos en el SGSI.
- Realizar y utilizar plantilla de seguimiento, medición, análisis y evaluación de los procesos y política, con el fin de conseguir

resultados válidos del manejo de la seguridad informática en la organización.

- Se establece que los seguimientos de auditoría se deben de realizar cada 6 meses.
- Luego de la auditoría se realiza una reunión con las partes interesadas, informando el estado de todos los procesos de seguridad informática, donde se notifican las falencias y los resultados positivos de los procesos; con el fin de, llegar un acuerdo de cómo se procede con la corrección de falencias encontradas para la mejora del SGSI.

La empresa definirá una persona interna que ayude a evaluar el desempeño y la eficiencia de auditoría como control de calidad, documentando todas las tareas realizadas para tener una trazabilidad que sirva de evidencia en la mejora continua del sistema de gestión.

La organización también debe realizar un seguimiento de satisfacción del cliente, para validar cual es la percepción de los servicios prestados por GRUPO NETHEXA S.A.S, en el cumplimiento de todas las necesidades y expectativas del funcionamiento y seguridad del servicio de e-learning y Telefonía IP.

Al final de toda la revisión, la empresa analiza y realiza una evaluación de los resultados obtenidos en la auditoría del SGSI, obteniendo la siguiente información que ayudará en la toma de decisiones en el seguimiento y mejora del sistema de seguridad informática:

- Conformidad de los productos y servicios en la organización.
- Nivel de satisfacción de los clientes que hacen uso de los servicios.
- Desempeño y eficiencia proporcionado por el SGSI.
- Análisis de eficacia y eficiencia en las acciones tomadas en el análisis de riesgos y en la implementación de controles.
- Labor realizada por los proveedores externos.
- Mejora del sistema de gestión de seguridad de la información.

La empresa busca la manera de cómo almacenar y analizar los resultados de las auditorías, debido a que concurrentemente se deben de ingresar datos y es de suma importancia tener una estadística de la evolución del SGSI en la organización.

5. Bibliografía

ISO_9001 (2015). Seguimiento, medición, análisis y evaluación. Recuperado: ISO 27002 (2005). Protección contra códigos maliciosos y móviles. Recuperado:

http://www.slinfo.una.ac.cr/documentos/EIF402/ISO27001.pdf. 18 de septiembre de 2018. 19 de septiembre de 2018.

CIBIT_5 (2012). Proceso MEA-03: Supervisar, evaluar y valorar la conformidad con los requerimientos externos. Objetivos de control las tecnologías de información y relacionadas. Recuperado: https://adminsisuc201701.wordpress.com/mea03/. 19 de septiembre de 2018.

ANEXO 20

OSP-24 GESTIÓN DE INCIDENTES

1. Descripción del proceso

Proceso encargado de mitigar el impacto generado por los incidentes de seguridad de los activos de información.

2. Objetivos y metas

- Realizar procedimientos claros y precisos en el manejo de incidentes de seguridad, que ayuden a mitigar los incidentes de seguridad y previniendo su recurrencia.
- Medir la eficiencia de las medidas de seguridad, para la toma de decisiones y el mejoramiento sobre la inversión de la seguridad.

3. Métricas

- Porcentajes de incidentes de seguridad reportados y solucionados dentro del tiempo establecido.
- Porcentajes de incidentes de seguridad críticos.
- Cantidad de mejoras propuestas de lecciones aprendidas.

4. Gestión de Incidentes

Se necesita tener un enfoque estructurado y planificado en gestión de incidentes de seguridad en los sistemas de información de la organización, que permita manejar adecuadamente la mayoría de los incidentes de seguridad que puedan sufrir los productos de servicios de e-learning y Telefonía IP.

Para obtener los objetivos y metas establecidas en este proceso, se deben de involucrar en los sistemas de gestión de incidentes de seguridad de la información, son necesarios tener los siguientes subprocesos:

- Planificación y preparación de gestión de incidentes de seguridad.
- Análisis y detección de incidentes de seguridad.
- Contención, erradicación y recuperación.
- Actividades de lecciones aprendidas

El proceso está encargado de afrontar cada una de las etapas anteriores, definiendo las responsabilidades y procedimientos del área de seguridad informática en la respuesta ante incidentes de seguridad, de una manera rápida, eficaz y ordenada.

1. **Características del modelo de gestión de incidentes.**

El proceso se compromete en plantear una serie de actividades de buenas prácticas de gestión de incidentes de seguridad, lo cuales son definidos en la NIST ISO 27036-2013, la cual propone la implementación de un ciclo de vida de gestión y respuesta a incidentes de seguridad.

La organización tiene la necesidad de tener un CSIRT o un SOC de seguridad, quienes son los encargados de definir los procedimientos de atención de incidentes, manejar las relaciones de seguridad con entes internos y externos, definir la clasificación de incidentes de seguridad y la prioridad de atención dependiendo de un análisis de riesgos que debe tener elaborado la organización.

Además, el grupo de seguridad SOC o CSIRT está encargado de:

- Detección de incidentes de seguridad, monitoreando y verificando las herramientas de control que permitan detectar los posibles incidentes de seguridad que se realizan a los activos de información.
- Atención de incidentes de seguridad, recibiendo y resolviendo los incidentes de seguridad que son generados hacia los activos de información, de acuerdo con los procedimientos establecidos del SGSI.
- Recolección y análisis de evidencia digital para revisar cuando sea requerida.
- Anunciar a los funcionarios, contratistas y clientes de la organización, de las nuevas vulnerabilidades, las nuevas actualizaciones de seguridad disponibles y las recomendaciones a tener en cuenta de la seguridad que se tienen que controlar.
- Auditorías y trazabilidad de seguridad informática, con el fin de verificar constantemente identificando las vulnerabilidades y las brechas de seguridad de los servicios web de la organización, permitiendo la mejora continua.
- Administración adecuada de los dispositivos de seguridad informática aportados por la organización.

- Clasificación y priorización de los servicios expuestos dependiendo el análisis de riesgos, para la intervención de las mejoras de seguridad necesarias para el correcto funcionamiento de los activos de información.
- Investigación y desarrollo de nuevos productos de seguridad, que permitan combatir las brechas de seguridad y la implementación de nuevos proyectos que mejoren la seguridad de la organización.

2. Recursos de comunicación.

La organización establece los elementos necesarios para el equipo de atención a incidentes de seguridad internamente, la cual contiene la siguiente información:

- Información de contacto de las personas que conforman el grupo de gestión de incidentes.
- Información de escalamiento de la estructura establecida por el grupo de gestión de incidentes.
- Política de comunicación para la identificación y filtro de los incidentes de seguridad que se pueden atender por el equipo de gestión de incidentes.

3. Herramientas de detección y análisis de incidentes de seguridad.

Con el fin de tener una correcta y eficiente gestión de los incidentes de seguridad, la organización tiene en cuenta los siguientes elementos:

- Equipos y software para realizar análisis forense.
- Análisis de protocolos.
- Aplicaciones para la recolección de evidencias.
- Herramientas de respuesta a incidentes de seguridad.
- Medios de almacenamiento.
- Correlación de eventos de seguridad.
- Alertas e identificación ante incidentes de seguridad.
- Diagramas de red y de servicios.

4. Mitigación y remediación.

La organización está siempre preparada ante cualquier eventualidad de seguridad que genere la pérdida parcial o total de los activos de información que poseen los productos de servicios web de e-learning y telefonía IP, por lo que se consideran todos los elementos y procedimientos de gestión de incidentes, con el propósito de recuperar los más rápido posible la continuidad de los servicios prestados a los clientes, afectando el menor tiempo posible la disponibilidad de los servicios web.

- Backup de la información.
- Copia de las imágenes de los servidores.
- Copia de los archivos de configuración.
- Snapshot de puntos anteriores.

5. Detección y análisis.

Es vital la implementación de indicadores de los servicios y aplicaciones web de la organización, que nos permitan identificar los eventos que nos informan el establecimiento de un incidente de seguridad, que pueda afectar los activos de información, por lo que algunos elementos que se deben de adquirir son los siguientes:

- Alertas tempranas de seguridad.
- Caída de servidores.
- Caída de servicios.
- Reportes de usuarios.
- Software de antivirus o EndPoint que permita visualizar los informes.
- Correlacionador de eventos de seguridad.

Para la utilización de estos elementos, la organización tiene que madurar la información que proporcionan los desarrollos propietarios y los servicios que están corriendo en los servidores, los cuales permitan realizar un análisis e identificar si se están presentando problemas de seguridad que generen incidentes, por lo que se deben de mejorar los siguientes elementos en los servicios:

- Logs de los servidores.
- Logs de las aplicaciones y servicios.
- Logs de las herramientas de seguridad.
- Logs de los equipos de red.

Con toda la información detectada, se debe de tener personal idóneo que permita analizar toda la información y poder determinar los incidentes de seguridad que se están presentando; con el fin de, poder detener todos los ataques informáticos que se presentan a las infraestructuras web de la organización.

6. Evaluación y clasificación de incidentes de seguridad.

Para realizar la correcta evaluación y clasificación de los incidentes de seguridad, se deben de tener presentó los niveles de impacto y la clasificación de los activos de información que son proporcionados por el análisis de riesgos de la organización.

La severidad de los incidentes puede ser:

- "**Alto Impacto**: El incidente de seguridad afecta a activos de información considerados de impacto catastrófico, que influyen directamente a los objetivos de la organización. Se incluyen en esta categoría aquellos incidentes que afecten la reputación y el buen nombre o involucren aspectos legales. Estos incidentes deben tener respuesta inmediata."
- "**Medio Impacto**: El incidente de seguridad afecta a activos de información considerados de impacto moderado, que influyen directamente a los objetivos de un proceso determinado."
- "**Bajo Impacto**: El incidente de seguridad afecta a activos de información considerados de impacto menor e insignificante, que no influyen en ningún objetivo. Estos incidentes deben ser monitoreados con el fin de evitar un cambio en el impacto."

7. Priorización y tiempos de respuesta.

Con el objetivo de permitir una adecuada atención de incidentes de seguridad, la organización determina un nivel de prioridad para el análisis, contención y erradicación; y de esta manera atenderlos adecuadamente según el nivel de criticidad de los activos de información que se encuentran comprometidos.

- Nivel de Prioridad

  Depende del valor y la importancia de la organización y de los procesos de activos de información afectados.

Nivel de Criticidad	Valor	Definición
Bajo	0,30	Activos que no afectan la disponibilidad del servicio
Medio	0,60	Activos que afectan de manera parcial la disponibilidad del servicio
Alto	1,0	Activos críticos que afectan totalmente la disponibilidad del servicio

- Impacto Actual

Depende del daño que ha generado actualmente el incidente de seguridad al momento de ser detectado.

Nivel de Criticidad	Valor	Definición
Bajo	0,30	Impacto leve en la afectación de los activos de información.
Medio	0,60	Impacto moderado en la afectación de los activos de información.
Alto	1,0	Impacto crítico en la afectación de los activos de información.

- Impacto Futuro

  Es la cantidad de daño que puede causar un incidente de seguridad si no es contenido, ni erradicado por el grupo de gestión de incidentes.

Nivel de Criticidad	Valor	Definición
Bajo	0,30	Impacto leve en la afectación de los activos de información en el futuro.
Medio	0,60	Impacto moderado en la afectación de los activos de información en el futuro.
Alto	1,0	Impacto crítico en la afectación de los activos de información en el futuro.

- **Priorización**

Para la obtención de la prioridad de realiza la siguiente formula:

Nivel de Prioridad = (Impacto Actual * 2,5) + (Impacto Futuro * 2,5) + (Criticidad del sistema * 5)

El resultado es comparado con la siguiente tabla, la cual determinará la prioridad de la atención.

Nivel de Prioridad	Valor
Bajo	00,00 - 02,59
Medio	03,00 - 05,59
Alto	06,00 - 10,00

- **Tiempos de respuesta**

Para la atención a incidentes de seguridad, se establecen los tiempos de respuesta tolerables para la organización, cumpliendo con los acuerdos de niveles de servicios de los productos WEB dependiendo de la criticidad del incidente.

Nivel de Prioridad	Valor
Bajo	8 horas
Medio	2 horas
Alto	30 minutos

8. Contención, erradicación y recuperación.

La empresa implementa una estrategia que permita tomar decisiones de seguridad de manera oportuna, evitando la propagación de incidentes de seguridad y disminuyendo los daños de los activos de información y la pérdida de la disponibilidad de los tiempos establecidos en los acuerdos de nivel de servicios.

- **Contención**

Actividad que busca la detección de incidentes de seguridad que son identificados inmediatamente; con el objetivo de impedir la propagación del problema de seguridad presentado e impedir que genera más daños de la información y de la infraestructura de TIC, teniendo una estrategia de contención y prevención definida para tomar decisiones inmediatas cuando ocurre un incidente de seguridad.

Las estrategias y los métodos de contención establecidos por la empresa deben de variar según los incidentes de seguridad, todos los procesos deben de estar debidamente documentados y actualizados para facilitar la rápida toma de decisiones.

Los criterios que deben de ser tomados son los siguientes:

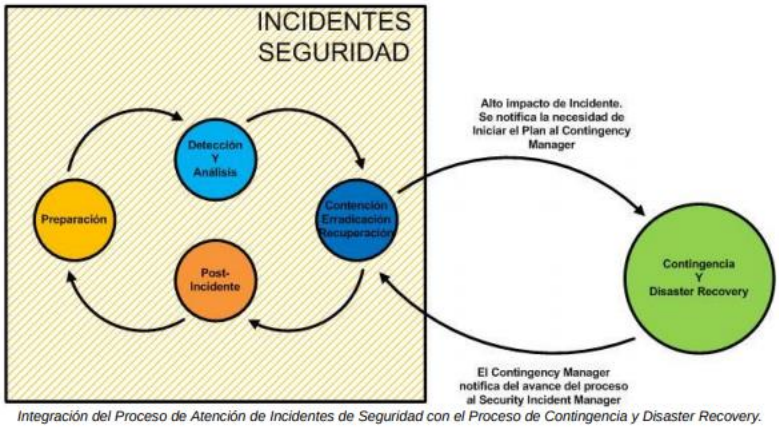
- Análisis forense
- Daños potenciales.
- Hurto de información y de activos.
- Preservación del debido proceso de la evidencia.
- Disponibilidad del servicio.
- Tiempo y recursos necesarios para la implementación de la estrategia.
- Efectividad de la estrategia en la contención de incidentes.
- Duración de la solución del incidente.

- **Erradicación y recuperación**

Al finalizar con la contención del incidente de seguridad, se realiza una erradicación y eliminación de cualquier rastro del problema presentado en los activos de información; con el fin de, estar seguros que no queda código malicioso en los activos de información o configuraciones que haya afectado el ataque, para no tener algún otro problema de seguridad en los activos de información.

La recuperación de los sistemas de información se puede realizar con la restauración de copias de seguridad e imágenes guardadas del servidor, restableciendo la totalidad de los activos afectados por el ataque, y luego de tener todos los sistemas operativos se realiza un endurecimiento de los servicios afectados, permitiendo prevenir los incidentes de seguridad similares en el futuro.

El proceso de gestión de incidentes genera a futuro dos procesos que permiten preservar la disponibilidad de los servicios de TI de la organización, en la implementación del BCP (Plan de continuidad del negocio) y el DRP (Plan de recuperación de desastres).



Integración del Proceso de Atención de Incidentes de Seguridad con el Proceso de Contingencia y Disaster Recovery.

9. Lecciones aprendidas.

Para el SGSI de GRUPO NETHEXA S.A.S lo más importante que puede suceder es poder identificar los errores cometidos en el sistema de gestión y mejorarlos cada vez que sea posible, con el propósito de llegar a un nivel de madurez que nos permita brindar un gran porcentaje de seguridad y disponibilidad de los servicios web prestados por la organización.

El equipo de seguridad informática evoluciona constantemente reflejando el conocimiento adquirido de las amenazas tras la solución de estas, adquiriendo un nivel de madurez que permitan reducir el tiempo de solución de los incidentes de seguridad y reducir las vulnerabilidades que posee los activos de información.

Mantener documentado el registro de todos los eventos ocurridos y como fueron solucionados, suministrando la documentación y enseñanza a todo el equipo de seguridad en la gestión del conocimiento de la organización, nos permite:

- Entender lo que sucedió en el incidente, desde el momento en que empezó el ataque y como el personal de seguridad informática gestiono el ataque.
- La documentación de procesos.
- Revisión de la toma de malas decisiones que podrían impedir la recuperación de los activos de información.
- Como se puede mejorar la gestión del personal en los tiempos de respuesta y de solución del incidente de seguridad.
- Realizar acciones correctivas que ayuden a solucionar problemas de seguridad que se pueden presentar en el futuro.
- Cuáles son las herramientas adicionales que se necesitan para detectar, analizar y mitigar los incidentes de seguridad que se pueden presentar en el futuro.

5. Bibliografía

MSPI (2016). Guía para la gestión y clasificación de incidentes de seguridad de la información, MINTIC. Recuperado: https://www.mintic.gov.co/gestionti/615/articles-5482_G21_Gestion_Incidentes.pdf. 20 de septiembre de 2018.

ANEXO 21

OSP-26 GESTIÓN DE DISPONIBILIDAD Y FIABILIDAD DE INFRAESTRUCTURA CRÍTICA

1. Descripción del proceso

Es un conjunto de medidas de seguridad basadas en la redundancia, diversidad y dispersión, con el fin de eliminar puntos de falla y reducir el impacto en la pérdida de la infraestructura crítica de seguridad. Cumpliendo con los niveles de servicios pactados, reduciendo el tiempo de indisponibilidad de los activos de información.

2. Objetivos y metas

Incorporación de resiliencia para fallas parciales o totales, mitigando los incidentes de seguridad críticos.

3. Métricas

- Porcentaje de tiempo de disponibilidad de servicio en el tiempo establecido.
- Cantidad de incidentes de falla de infraestructura crítica, afectando el tiempo establecido de los acuerdos de nivel se servicio.

4. Gestión de disponibilidad y fiabilidad de infraestructura crítica

El proceso de gestión de disponibilidad y fiabilidad de los productos web de la organización, tiene una influencia directa en la satisfacción de los clientes que hacen uso del servicio y la reputación de la empresa como proveedor de servicios web. La gestión de disponibilidad es un proceso básico que se tiene en cuenta en los diseños de infraestructura crítica de la organización, antes de ser implementada en los diferentes clientes.

La disponibilidad en infraestructuras críticas, comprenden todos los procesos del área de TIC al diseñar, implementar, evaluar, gestionar y mejorar los servicios de TIC y de los componentes, ayudando a la mejora continua de los productos web. La finalidad o el objetivo principal de los procesos es poder garantizar los niveles de servicios pactados con los clientes, cumpliendo con los niveles de seguridad de los servicios nuevos y actuales en producción.

Para mejorar la disponibilidad, el equipo de seguridad informática se apoya en los servicios de monitoreo, revisión de métricas y correlación de eventos

de seguridad, que permitan garantizar los niveles de seguridad a los servicios nuevos y actuales que posee la organización con los clientes.

5. Bibliografía

ITIL_V3 (2011). Gestión de disponibilidad, Diseño del servicio basada en ITIL V3. p. 33-34.

ANEXO 22

INFORME DE VALORACIÓN Y ANÁLISIS DEL RIESGO

El objetivo es poder informar en un resumen, las amenazas que puedan afectar a los activos de información en las plataformas web de e-learning y telefonía IP de la organización, valorando los riesgos que pueden causar las amenazas, a los activos información e identificar cuáles son los riesgos altos y medios a los que se realiza un tratamiento del riesgo. Los riegos bajos se deben de tener presentes, pero estos son aceptados por la organización por su baja probabilidad e impacto.

1. Activos de información evaluados

Son los activos de información extraídos del proceso de inventario de activos OSP-3, donde son tenidos en cuenta los activos con criticidad media y alta, ya que la criticidad baja es aceptada por la empresa.

Categoría	Etiqueta	Activos	Criticidad
Servicios	SRV-1	Apache + PHP	Alta
	SRV-2	Tomcat	Alta
	SRV-3	Asterisk	Alta
	SRV-4	MySQL	Alta
Aplicaciones	APP-1	Moodle	Alta
	APP-2	Queuemetrics	Alta
	APP-3	HexaDialer	Alta
	APP-4	HexaHud	Alta
	APP-5	FreePBX	Media
Sistemas operativos y plataformas de virtualización	SOP-1	Proxmox	Media
	SOP-2	VMWare	Media
	SOP-3	Debian 9	Alta
Plataformas Cloud	PCD-1	OVH	Alta
	PCD-2	AWS Amazon	Alta
Hardware	HWR-1	Servidor	Alta
	HWR-2	Red	Alta
	HWR-3	NAS	Media
Información del servicio	IFS-2	Datos de acceso	Alta
	IFS-3	Información de cursos	Media
	IFS-4	Información de llamadas	Alta

	IFS-5	Audios de llamadas	Alta
Intangibles	ITG-1	Credibilidad y buena imagen	Alta

2. Amenazas que afectan a los activos de información

Son las amenazas que pueden causar las vulnerabilidades y la falta de controles que poseen los activos de información, estas amenazas son investigadas y escaneadas directamente en los servicios, donde se encuentran vulnerabilidades, amenazas, problemas de desarrollo de aplicaciones y servicios desactualizados.

a. Amenazas investigadas

Se realiza un análisis con herramientas de escaneo como los son OWAS ZAP y Nessus, elegidas por la organización para analizar vulnerabilidades y amenazas conocidas que puedan afectar a los activos de información de las plataformas WEB, identificando cuáles son las amenazas que pueden afectar directamente a los servicios proporcionados en e-learning y telefonía IP.

Las amenazas y vulnerabilidades seleccionadas para realizar el cruce con los activos de información en la valoración del riesgo son:

- **Malware**

Es código o software maliciosos cuyo objetivo es sacar provecho de un sistema informático, causando mal funcionamiento, daño del sistema y extracción de información. El malware posee una gran cantidad de software malicioso que tienen funciones particulares en los sistemas de información y en la red de Internet, todas las variaciones están identificadas por las siguientes clases: Virus, Gusanos, troyanos, Spyware, Phishisng, Adware, Riskware, Rootkits, Spam, entre otros códigos que perjudiquen a los sistemas de información.

- **Exposición de directorios y datos sensibles**

Muchas de las aplicaciones web y APIs no protegen adecuadamente los directorios y los datos sensibles que contiene en la web, tales como código de desarrollo, información de datos personales, información de cursos e información de llamadas telefónicas en los servicios de la organización, estos problemas se pueden presentar por malos manejos en el desarrollo de las aplicaciones, ya que no se tiene un proceso establecido de desarrollo seguro en la empresa, que permita identificar y corregir estos problemas. Cuando se expone información en los sitios web, los atacantes pueden robar o modificar

estos datos que son protegidos adecuadamente llevando a cabo la materialización de la amenaza y la pérdida o modificación de la información.

- **Interceptación de información**

Es una amenaza común en todos los sistemas de información y comunicación en la red; debido a que, todas las comunicaciones de los servicios, aplicaciones y sistemas de red deben de ser cifrados, con el propósito de que un atacante que intercepte la comunicación no la pueda descifrar. En la actualidad todos los sistemas de información y comunicación poseen herramientas para cifrar la información transmitida y recibida, pero por malas prácticas de los administradores de los sistemas de información la comunicación es transmitida de texto plano.

- **DOS/DDOS**

Ataque de denegación de servicios y denegación de servicios distribuido, donde uno o más atacantes inundan de peticiones a un sistema de formación y de comunicación, afectando la accesibilidad de los servicios a los usuarios legítimos. Por lo general cuando se realizan estos ataques, los servicios pierden conectividad por el alto consumo de ancho de banda que genera las peticiones fraudulentas o afecta la sobrecarga de los recursos de los sistemas de información, impidiendo la prestación de los servicios.

- **Pérdida de autenticación y gestión de sesiones**

Ocurre cuando aplicaciones relacionadas con autenticación y gestión de sesiones no son implementadas correctamente, comprometiendo los usuarios y contraseñas, token de sesiones y el robo de identidades, permitiendo que usuarios malintencionados puedan ingresar a los activos de información.

- **Configuraciones de seguridad incorrectas**

Es un problema común en todas las organizaciones y se debe a que las personas humanas son las encargadas de establecer las configuraciones de seguridad de forma manual, ad hoc y por sesiones, dejando vulnerabilidades en los servicios y aplicaciones en los sitios web.

- **Deserialización insegura**

Es una vulnerabilidad de seguridad que ocurre cuando una aplicación recibe objetos serializados dañinos y estos objetos pueden ser manipulados o borrados por el atacante para realizar ataques de repetición, inyecciones y

levantar privilegios de ejecución. En el peor de los casos los atacantes podrían ejecutar código de manera remota directamente en los activos de información.

- **Uso de componentes de vulnerabilidades conocidas**

Vulnerabilidad que afecta a los componentes que utilizan bibliotecas, frameworks y módulos que se ejecutan con los mismos privilegios de la aplicación. Si se explota el componente vulnerable, un atacante puede provocar pérdida de información y tomar control del servidor. Todas las aplicaciones y las API que utilizan componentes vulnerables, debilitan las defensas de las aplicaciones permitiendo diferentes ataques e impactos.

- **Registro y monitoreo insuficiente**

El registro y monitoreo insuficiente; y la falta de respuesta a incidentes en las organizaciones, permiten que los atacantes puedan mantener los ataques en el tiempo, pivotar a otros sistemas y manipular, extraer o destruir los datos de los activos de información.

- **Phishing**

Es un ataque informático muy utilizado por los ciber-delincuentes, por lo general es un ataque que se realiza a través de un malware enviado por correo electrónico, redes sociales, SMS/MMS y por llamadas telefónicas que permite el ingreso a sitios fraudulentos a través de ingeniería social. El objetivo del ataque es estafar y obtener información confidencial como contraseñas e información bancaria de las víctimas.

- **SQL Inyección**

Las inyecciones SQL ocurren cuando un gestor de bases de datos SQL, NoSQL, OS o LDAP envía datos no confiables a un intérprete, como parte de un comando o consulta. Los datos del atacante pueden engañar al intérprete para que ejecute comandos involuntarios o acceda a los datos sin una debida autorización, permitiendo el robo de información sensible y escalamiento de privilegios en los servidores en la ejecución de comandos.

- **Buffer Overflow**

Es un error de software producido por un programa que no puede controlar adecuadamente la cantidad de datos que son copiados sobre el área de memoria reservada para su propio funcionamiento, generando que los bytes sobrantes son almacenados en zonas de memoria adyacentes, sobre

escribiendo su contenido original, generando problemas a las demás aplicaciones que ya tenían código almacenado.

- **Ataque día cero**

Son los ataques informáticos que se generan hacia un sistema o aplicación que tiene como objetivo la ejecución de malware gracias al conocimiento de vulnerabilidades que son desconocidas por los administradores de seguridad en el mundo.

- **Cross-site scripting**

Ataque llamado secuencia de comandos en sitios cruzados (XSS), el problema de seguridad ocurre cuando una aplicación toma datos no confiables y los envía al navegador web, sin ningún tipo de validación o codificación apropiada; permitiendo ejecutar comandos en los navegadores de las víctimas secuestrando la sesión de usuarios, modificación del sitio web o re direccionar a los usuarios a un sitio web malicioso. Estos ataques son utilizados en aplicaciones que corran JavaScript.

- **Ataque de fuerza bruta**

El ataque de fuerza bruta es la manera de recuperar contraseñas probando todas las combinaciones posibles que permita encontrar la contraseña que concede el acceso a un sistema de información y comunicación. Criptográficamente es un ataque que no debería de tener problemas de seguridad, pero las contraseñas que utilizan los usuarios son fáciles de detectar a través de la fuerza bruta, por este motivo es una vulnerabilidad importante que debe ser tenida en cuenta por toda la organización.

- **Robo de información**

La organización tiene presente el robo de datos sensibles de las plataformas web de la organización, la información que es generada por las aplicaciones y los servicios deben de ser almacenada en lugares externos; por este motivo, la información es respaldada y cubierta por controles de seguridad. Generalmente las organizaciones poseen controles de seguridad para muchas de las amenazas, pero los usuarios que poseen los permisos pueden extraer información sensible de las organizaciones sin ninguna restricción.

- **Man In The Middle**

El ataque de hombre en el medio consiste en interceptar e interactuar con dos sistemas de información que están estableciendo comunicación

lógicamente entre sí; con el fin de, hacerse pasar por uno de los dos puntos de comunicación, capturando el tráfico de la red entre los sistemas de información, con el propósito de descifrar la información y extraer datos sensibles que puedan ser aprovechados por el atacante.

- **CSRF**

El ataque informático cross-site request forgery, llamado en español falsificación de peticiones en sitios cruzados, es un exploit malicioso utilizados en sitios web, donde se transmiten comandos no autorizados por el navegador de un usuario autorizado a un sitio web vulnerable.

- **Envenenamiento de Cookies**

El objetivo del ataque es modificar el contenido de una cookie para saltarse los mecanismos de seguridad de los sitios y navegadores WEB que utilizan las sesiones con estos métodos; con el fin de, extraer información no autorizada, robo de identidad informática, robo de sesiones y modificación de datos.

- **Entidades XML (XXE)**

Muchos de los procesadores XML antiguos o mal configurados evalúan referencias de entidades externas en documentos XML. Estas entidades externas pueden ser utilizadas para revelar archivos internos mediante las URI o archivos internos de servidores no actualizados, escanear puertos en la red LAN, ejecutar malware de forma remota y realizar ataques de denegación de servicios.

b. Amenazas y vulnerabilidades Escaneadas

El objetivo de los escáneres de vulnerabilidades, es poder identificar qué amenazas y/o vulnerabilidades conocidas poseen los activos de información de la organización.

En la búsqueda se encontraron riesgos de información que comprometen algunas de las amenazas descritas anteriormente en la investigación; también se encuentran vulnerabilidades de código de desarrollo, malas prácticas en la información que puede proporcionar los servidores que contiene las plataformas web de la organización y vulnerabilidades por tener servicios desactualizados.

La finalidad de esta actividad es proporcionar dichas vulnerabilidades y amenazas para ser resueltas en la implementación de controles de seguridad

y corregir las configuraciones de los activos de información, dando una adecuada prioridad que se da en el análisis de riesgos en la valoración de las amenazas y activos.

El informe de los resultados los puede detallar en el siguiente enlace:

Resultados de escáner de amenazas y vulnerabilidades

3. Valoración del riesgo

En la valoración del riesgo se realiza un estudio de los activos de información que tiene una criticidad media y alta, estos activos son cruzados con las diferentes vulnerabilidades y amenazas detectadas e investigadas que pueden perjudicar la seguridad de los activos de información de las plataformas web de e-learning y telefonía IP de la organización, afectando la disponibilidad y la continuidad del funcionamiento de los servicios y aplicaciones. El riesgo es valorado a través de una matriz establecida por la empresa de probabilidad e impacto, donde son evaluadas las amenazas y vulnerabilidades que afectan a uno o varios activos de información, brindando la información de las amenazas que deben de ser tratadas para disminuir el riesgo informático y los riesgos que son aceptados por su baja probabilidad e impacto.

Se anexa la tabla de los resultados del análisis de la valoración del riesgo; con el objetivo de que las partes interesadas de la empresa puedan tomar decisiones en el tratamiento de riesgos, con el propósito de mejorar la seguridad en la prestación del servicio de las plataformas web de e-learning y telefonía IP.

Amenazas	Valoración Del Riesgo
Malware	Alto
Explosión de directorios y datos sensibles	Medio
Interceptación de información	Medio
DOS/DDOS	Alto
Pérdida de autenticación y gestión de sesiones	Bajo
Pérdida de control de acceso	Alto
Configuraciones de seguridad incorrectas	Alto
Deserialización insegura	Bajo
Uso de componentes con vulnerabilidades conocidas	Alto
Registro y monitoreo insuficiente	Alto
Phishing	Medio
SQL injection	Alto
buffer overflow	Medio
Ataque día cero	Medio

cross-site scripting	Alto
Ataque de fuerza bruta	Medio
Robo de Información	Bajo
Man In The Middle	Alto
CSRF	Bajo
Envenenamiento de cookies	Bajo
Entidades XML(XXE)	Medio

Analizando la tabla proporcionada por la valoración del riesgo, la empresa hace un tratamiento del riesgo de las amenazas con valoración del riesgo Alto y Medio; con el objetivo de, poder reducir el riesgo a un nivel bajo que pueda ser aceptable y tolerable para la organización, en la continuidad y disponibilidad de los servicios prestados en las plataformas web de e-learning y telefonía IP; ya que el mayor número de riesgos están en el nivel Medio y Alto como lo indica la siguiente tabla:

Valoración del Riesgo	Número
Alto	9
Medio	7
Bajo	5
Total	21

4. Bibliografía

OWASP (2017). OWASP Top 10 del 2017, Proyecto Abierto de Seguridad en Aplicaciones WEB. Recuperado: https://www.owasp.org/images/5/5e/OWASP-Top-10-2017-es.pdf. 23 de septiembre de 2018.

Nessus (2018). Aplicación de seguridad escaneo de vulnerabilidades, Tenable. Recuperado: https://www.tenable.com/downloads/nessus. 23 de septiembre de 2018.

ANEXO 23

ACTUALIZACIONES DE LOS ACTIVOS DE INFORMACIÓN

La aplicación de los parches de seguridad de los activos de información es de suma importancia, ya que la mayoría de aplicaciones y servicios que contienen los servidores y equipos en red, poseen una instalación predeterminada que no es probada lo suficiente. Luego los servicios y las aplicaciones cuando se encuentran en producción, los fabricantes y desarrolladores empiezan a detectar los errores y problemas que presentan estas plataformas, donde se empieza a corregir y refinar el código al detalle mejorando la seguridad y eficiencia de los servicios y aplicaciones; por este motivo, la importancia de las actualizaciones constantes de todas las plataformas web de la organización.

Cuando se descubren las vulnerabilidades de seguridad en los servicios y aplicaciones que utilizan las plataformas web de la organización, se programa una actualización del software afectado de manera masiva en todos los servidores. Al encontrar una falla de seguridad en Linux, por lo general siempre viene acompañada de un parche de seguridad que soluciona los inconvenientes presentados, todos los paquetes y actualizaciones de seguridad se pueden obtener desde la página oficial de debían, donde se encuentran todos los paquetes disponibles para las actualizaciones directas de los sistemas operativos.

Las actualizaciones de los activos de información son vitales para la reducción de riesgos identificados en el análisis realizado, mitigando riesgos críticos para la organización los cuales son:

- Malware.
- Uso de componentes con vulnerabilidades conocidas.
- Buffer Overflow.
- Ataques de fuerza bruta.
- Robo de información.

1. **Actualizaciones de paquetes.**

   Es de suma importancia descargar todos los paquetes de actualización directamente de la página oficial o de los repositorios autorizados por Debían, ya que es la única fuente confiable para hacer las descargas de todos los parques de seguridad que poseen los servicios y aplicaciones que corren bajo las plataformas web. De no descargar las actualizaciones de la página oficial puedes dañar el sistema muy fácilmente o instalar un malware que genere puertas traseras a personas mal intencionadas; perjudicando la seguridad de la organización, ya que el sistema operativo de los servidores

no podría detectar el software cuando es instalado con un paquete .deb directamente en el servidor.

2. Verificación de paquetes firmados.

La seguridad es muy importante, por este motivo es importante que todos las actualizaciones e instalaciones de servicios y/o aplicaciones que se generen en los servidores, deben de tener la garantía de que todos los paquetes utilizados sean provenientes de Debían, evitando que personas mal intencionadas intentan agregar código malicioso en los servidores de la empresa.

El sello que proporciona Debían a los paquetes a los que le pertenecen es una firma y una cadena de hash criptográficos, la firma siempre se encuentra en todos los archivos **Release**, el cual contiene todos los archivos **Packages** y los hashes (MD5, SHA1 y SHA256) de cada paquete, asegurando que los archivos no han sido modificados.

En Debían como distribución de Linux, la instalación y actualización de aplicaciones y servicios se utilizan a través de la administración por el paquete **apt** el cual contiene el programa **apt-key**, el cual contiene todas las llaves públicas GnuPG las cuales son utilizadas para la verificación de cada firma que contienen los paquetes proporcionados por debían.

3. Instalación de paquetes firmados.

Para la instalación y actualización de paquetes en los servidores tenemos que utilizar la herramienta **apt -get** y **apt-cache,** las cuales permiten obtener servicios y aplicaciones estables en las últimas versiones. La herramienta aptitude no es recomendable, ya que puede instalar o actualizar los servicios y aplicaciones que están en prueba; además, la utilización del comando elimina los paquetes que ya no son necesario colocando problemas en la devolución a las versiones actualizadas.

En la actualización de la distribución del sistema operativo Debían, podemos utilizar los comandos **apt full-upgrade** o **apt-get dist-upgrade,** los cuales permiten actualizar la versión del sistema operativo, cuanto es actualizado por una versión con mejoras considerables. También, debemos de tener en cuenta que es importante actualizar la versión de los sistemas operativos; ya que de no hacerlo; podemos terminar con servidores obsoletos al perder soporte de servicios y aplicaciones que ya no estén disponibles para las versiones anteriores de los sistemas operativos.

4. Aplicación de Cambios.

Al obtener todas las actualizaciones e instalaciones de los servicios y aplicaciones que proporcionan más seguridad en los servidores, es importante hacer un reinicio de los servicios actualizados e instalados; con el fin de, poder empezar a utilizar las nuevas versiones en el sistema operativo. El comando para reiniciar los servicios y/o aplicaciones es /etc/init.d/<Nombre del servicio> restart.

Tener presente que es necesario tener servidores de pruebas, con la finalidad de poder realizar las actualizaciones y cambios de seguridad en las plataformas que no se encuentran operando; con el propósito de, poder realizar las pruebas necesarios en los servicios y/o aplicaciones que corren en los servidores, verificando y analizando que las actualizaciones realizadas no afecten los servicios que están corriendo actualmente en producción; y finalmente, poder desplegar las actualizaciones a los servidores que se encuentran en operación con su adecuada ventana de mantenimiento generada por la gestión de cambios de la organización.

5. Bibliografía.

RedHat (2017). Guía de seguridad, Red Hat Enterprise Linux 6. Recuperado: https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/6/pdf/security_guide/Red_Hat_Enterprise_Linux-6-Security_Guide-es-ES.pdf, 11 de septiembre de 2018.

Debían (2018). Manual del Administración de Debían. Recuperado: https://debian-handbook.info/browse/es-ES/stable/sect.package-authentication.html, 7 de noviembre de 2018.

ANEXO 24

COPIAS DE SEGURIDAD Y CONTINUIDAD DE OPERACIONES

Para la organización es de vital importancia la continuidad de las operaciones de los activos de información de las soluciones de e-learning y telefonía IP de los productos desarrollados por GRUPO NETHEXA S.A.S. Como parte fundamental de la seguridad informática, es poder tener disponibles backups actualizados que permitan restablecer los servicios luego de sufrir un incidente de seguridad que dañe parcial o completamente los activos de información.

La empresa almacena un backup de la información y desarrollos que se realizan específicamente a los clientes que se les presta el servicio de e-learning y telefonía IP, ya que la información que se almacenan con el tiempo de operación de las plataformas es un recurso que se protege y se tiene siempre disponible a los usuarios que utilizan los servicios de la organización. Por este motivo, el almacenamiento es un factor crítico para los clientes, por lo que se realiza interna y externamente, dependiendo de la clase y el peso de su información, transportando los contenidos de manera segura.

Los siguientes controles de seguridad propuestos para la transferencia y realización de los backups de las plataformas de la organización, reducen los siguientes riesgos de seguridad encontrados en los activos de información:

- Exposición de directorios y datos sensibles.
- Interceptación de información.
- Robo de información.
- Malware.

1. Copias de seguridad de las máquinas en la nube

Las máquinas que se administran en la nube, son servidores que se encuentran creados en una instancia de la organización por un tercero en un datacenter que se encuentra en otro país, el cual es seleccionado al crear los servidores en la instancia desea de la nube. El backup de estas máquinas es diferente, ya que el proveedor de la nube tiene varios datacenter donde hace una réplica de todas las instancias que contiene los servidores creados en la nube, por lo que realizar backups a las máquinas completas es innecesario; ya que, al ocurrir un problema de pérdida de la máquina por un problema con el proveedor, esta puede ser recuperada en otro datacenter en tiempo real, para no afectar los servicios proporcionados.

Como sabemos, con solo tener el respaldo de toda la máquina en la nube no es suficiente, ya que podemos tener incidentes de seguridad que nos dañen la máquina y no pueda ser recuperada con Snapshot y copias de las máquinas, ya que el malware pudo estar durante el tiempo ejecutándose, teniendo el mismo resultado cuando es restaurada la máquina. Por este motivo, es necesario realizar copias de seguridad a la información importante y a los desarrollos realizados a cada cliente para poder ser restaurados en un servidor nuevo, si fuese necesario realizando la configuración de éste de manera rápida al tener toda la información almacenada en otro equipo que permita realizar el restablecimiento de la configuración y de la operación.

Las copias de seguridad que se deben de realizar son las siguientes:

- **E-learning**
  - Backup del desarrollo de la página web.
  - Backups de la configuración del Moodle.
  - Backups de todas las bases de datos creadas para el almacenamiento de información de los usuarios.
  - Backups de los cursos almacenados en el servidor.

- **Telefonía IP**
  - Backup de los desarrollos propietarios del PBX de los clientes.
  - Backups de las configuraciones de los archivos de configuración del Asterisk.
  - Backups de las configuraciones del FreePBX.
  - Backups de las bases de datos del Asterisk y del registro de llamadas en el CDR.
  - Backups de los audios de llamadas.

Nota: Las copias de seguridad se deben de almacenar en los mismos servidores, para tenerlas disponibles ante cualquier incidente de seguridad; pero también, deben de ser almacenadas en los activos de almacenamiento de la organización de manera externa a las plataformas en la nube, permitiendo tener la información disponible en dos partes diferentes evitando la pérdida de la información.

Teniendo toda la información necesaria de toda la configuración e información, se puede restablecer la operación de los clientes, ante una incidencia de seguridad que dañe de manera parcial o total los servidores que prestan los servicios.

2. Copias de seguridad de las máquinas virtuales

La infraestructura física es muy utilizada en empresas que poseen sus mismos datacenter y/ cuartos de telecomunicaciones, donde se administran todas las máquinas y dispositivos que permitan dar los servicios TIC de la organización. Por temas de disponibilidad de los servicios de TIC y recuperación de las aplicaciones en el menor tiempo posible, las máquinas físicas son administradas por plataformas de virtualización; la cuales permiten, crear múltiples servidores virtuales sobre las misma maquina en clúster y poder realizar backups que permiten el restablecimientos de servicios rápidamente, evitando la configuración de todo un servidor de manera manual al tener un incidente de seguridad o un incidente físico de la máquina.

Para tener una disponibilidad de los servicios ante un incidente se deben de realizar las siguientes configuraciones en las plataformas de virtualización, las cuales no permitirán restablecer los sistemas de una manera más rápida:

- Realizar copias de seguridad completa de toda la máquina virtual cada semana automáticamente en un horario que no estén laborando.
- Realizar Snapshot de las máquinas todos los días, con el propósito de devolver la configuración de manera rápida, ante cualquier eventualidad.
- Copiar la información de la máquina virtual en la unidad de almacenamiento local del cliente y realizar otra copia de la máquina virtual de manera externa en las instalaciones de la organización, cuando se realicen las debidas copias locales en los servidores.

Las copias de seguridad de la información de las aplicaciones y servicios deben de realizarse de manera independiente; con el fin de, tener la información disponible para poder ser restablecida en el menor tiempo posible, al poder utilizar las copias de las máquinas virtuales, las copias son las siguientes:

- **E-learning**
  - Backup del desarrollo de la página web.
  - Backups de la configuración del Moodle.
  - Backups de todas las bases de datos creadas para el almacenamiento de información de los usuarios.
  - Backups de los cursos almacenados en el servidor.

- **Telefonía IP**
  - Backup de los desarrollos propietarios del PBX de los clientes.

- Backups de las configuraciones de los archivos de configuración del Asterisk.
- Backups de las configuraciones del FreePBX.
- Backups de las bases de datos del Asterisk y del registro de llamadas en el CDR.
- Backups de los audios de llamadas.

Las copias de seguridad almacenadas nos permiten tener un plan de restablecimiento seguro de todos los activos de información, ante un incidente de seguridad, daño físico del servidor y errores humanos.

3. Alta Disponibilidad

Para la continuidad y disponibilidad de las operaciones de los servicios que son prestados a través de máquinas físicas como servidores, equipos de comunicación, equipos de seguridad informática, unidades de almacenamiento, etc. Es necesario tener infraestructura que posea redundancia de todos los equipos necesarios de TIC y de seguridad, que permitan el funcionamiento de las plataformas adecuadamente. Por este motivo, se deben de tener al menos dos dispositivos físicos a parte que permitan realizar balanceo de carga de alta disponibilidad, ya que al fallar uno de ellos, el otro dispositivo puede soportar toda la operación de manera automática sin que los usuarios lo puedan percibir.

Para las máquinas administradas en la nube, no es necesario tener alta disponibilidad porque esta es proporcionada por el proveedor de servicios en la nube.

4. Contingencia

Para la contingencia se deben de elaborar un plan de continuidad de las operaciones de las plataformas web de la organización, el cual permita tener un equipo similar adicional disponible ante cualquier incidente de seguridad que dañe o interrumpa de manera total o parcial los servicios que están activos.

La contingencia tiene que soportar toda la operación mientras se corrigen los problemas de seguridad y de TIC en los servidores y equipos de comunicación, Las contingencias deben de tener:

- Últimos Backups realizados a la plataforma web de la organización, para ser recuperados.
- Pruebas de recuperación satisfactorias de los backups realizados.

- Canales de comunicación adicionales que permitan la continuidad de las operaciones, al presentar una caída del canal principal de comunicaciones.
- Servidores adicionales en la infraestructura con la actualización automática de la réplica del servidor principal; con el fin, de ser habilitado ante cualquier eventualidad.
- Máquinas físicas disponibles para la sustitución ante una falla física de los dispositivos en operación.

5. Transferencia de copias de seguridad

Los Backups realizados a las máquinas virtuales y a la información de toda la operación de las plataformas web, es transferida a medios de almacenamiento externos que permitan la continuidad de las operaciones de los clientes.

Los backups realizados son transferidos de manera segura, por este motivo la información es transportada a través de una comunicación VPN cifrada segura y las copias de seguridad son cifradas de la información transportada, para evitar el robo de información sensible de los clientes.

6. Monitoreo

El monitoreo es muy importante para el equipo de soporte y seguridad de la organización, ya que permite reaccionar de manera proactiva ante cualquier falla o incidente de seguridad y TIC de las plataformas web, reduciendo el tiempo de indisponibilidad de las plataformas, atendiendo los problemas presentados en tiempo real.

Las plataformas necesarias para la identificación de problemas de los servicios y aplicaciones WEB de la organización son los siguientes:

- Monitoreo en tiempo real de los servicios prestados por los servidores web.
- Monitoreo en tiempo real de las nuevas vulnerabilidades descubiertas en los servidores web.
- Correlación de eventos de errores e inicios de sesión en las plataformas web.
- Patrones anómalos identificados en el escaneo y bloqueo de actividades de posible malware en los activos de información, que permita la erradicación.

Para concluir, las copias de seguridad nos facilitan el trabajo ante cualquier incidente de seguridad y TIC que se pueda presentar; por este motivo,

debemos realizar las tareas correspondientes de Backup cumplidamente, permitiendo la recuperación total de los activos de información de todos los clientes de la organización.

ANEXO 25

ENDURECIMIENTO DE ACTIVOS DE INFORMACIÓN

1. Escaneo de vulnerabilidades

a. Nmap

Nmap es la herramienta que podemos utilizar como primer paso para empezar a realizar el hardening de los servidores, con esta herramienta podemos sacar información de los puertos abiertos y los servicios de escucha que posee el servidor, donde podemos identificar los servicios y puertos que no son necesarios para cerrarlos.

b. Nessus

Es una herramienta de escaneo de vulnerabilidades completa, nessus permite a los administradores de TIC ajustar la seguridad de servicios y redes en las organizaciones, permitiendo tener una herramienta que es actualizada continuamente, permitiendo hacer escaneos de hosts y búsqueda de vulnerabilidades en tiempo real.

c. Owasp Zap

Es una herramienta de seguridad de escaneo de vulnerabilidades exclusivamente para servicios web, analizando todas las vulnerabilidades de los servicios, aplicativos y código de programación de las URL que son escaneadas. Permitiendo encontrar problemas de seguridad directamente en las plataformas web en la organización.

2. Servicios intrínsecamente inseguros

Son los servicios existentes que son inseguros a través de la red, que requieran transferir datos de autenticación y/o transferencia de información sensible para una organización en texto plano, permitiendo que ataques de Man in the Middle, interceptación de comunicación con sniffers y ataques de fuerza bruta, sean exitosos por tener servicios corriendo de los servidores y equipos de red de la organización que no realicen el proceso de cifrado de datos y de autenticación.

Los servicios comúnmente utilizados en la organización son el HTTP, FTP, Telnet, NTFS, Samba, etc. Los cuales son servicios que trabajan a través de la red y no proporcionan ningún tipo de cifrado en la transferencia y autenticación de datos.

La organización debe velar porque ningún servicio que no utilice conexiones seguras y cifradas pueda prestar servicios de conectividad en la red LAN y menos en la red de Internet al publicar servicios, porque se corre un riesgo muy grande de seguridad.

3. Vulnerabilidades y amenazas identificadas

En la gestión de riesgos realiza la identificación y el análisis de las vulnerabilidades y amenazas identificadas por el escaneo; adicional a esto, se hace una investigación de las amenazas que pueden presentarse en las plataformas web de la organización, donde se espera que con el hardening de los servidores pueda reducir el riesgo informático a los activos de información.

Las amenazas que reducirían los riesgos con el endurecimiento de los activos de información son las siguientes:

- Explosión de directorios y datos sensibles.
- Interceptación de Información.
- Pérdida de control de acceso.
- Configuraciones de seguridad incorrectas.
- Uso de componentes con vulnerabilidades conocidas.
- Ataque de fuerza bruta.
- Ataque de día cero.
- robo de información.
- Mand in the Middle.

Con el endurecimiento de los activos de información no es suficiente para reducir todo el riesgo que poseen, pero si es un control de seguridad eficiente que reduce el riesgo notablemente a las amenazas identificadas, ya que la organización espera reducir el riesgo a un nivel bajo y que sea aceptable.

4. Seguridad en el servidor

a. General

- **Instalación de sudo**

  Se debe instalar el **sudo,** para poder controlar el acceso de usuarios que pueden tener acceso como supe usuario root en los servidores.

  ```
  apt install sudo
  ```

- **configuración de usuarios requeridos**

Cuando se crea un usuario nuevo que necesite tener acceso a los permisos de súper usuario, el usuario es agregado al grupo sudo.

```
adduser usuario --ingroup sudo
```

Cuando el usuario no necesite los permisos de supe usuario, por seguridad no se puede agregar al grupo, por este motivo debemos de utilizar el siguiente comando.

```
adduser usuario
```

Cuando ya existe el usuario, pero se debe asignar al grupo sudo.

```
usermod -a -G sudo usuario
```

b. Configuración de Logs

En esta parte debemos de configurar el almacenamiento de logs del servicio Asterisk, ya que los servidores con la solución de Telefonía IP almacenan más logs de este servicio; por este motivo, se configura la rotación de logs y el directorio de almacenamiento.

Verificando las demás aplicaciones de los servidores, los logs quedan almacenados el directorio **/var/log/**, donde cada servicio crea por defecto su directorio y los archivos donde se almacenan las líneas de logs.

- **Logrotate asterisk**

Creamos o editamos el archivo **/etc/logrotate.d/asterisk**
Debe contener el siguiente código que se encarga de definir las políticas de rotación para los archivos de log.

```
/var/spool/mail/asterisk
/var/log/asterisk/freepbx_debug.log
/var/log/asterisk/messages
/var/log/asterisk/event_log
/var/log/asterisk/full
/var/log/asterisk/dtmf
/var/log/asterisk/security{
        su asterisk asterisk
        daily
        missingok
        rotate 15
```

```
        compress
        notifempty
        sharedscripts
        create 0640 asterisk asterisk
        postrotate
        /usr/sbin/asterisk -rx 'logger reload' > /dev/null 2> /dev/null
        endscript
}
```

- **Asterisk logger**

  Editamos el archivo /etc/asterisk/logger_logfiles_custom.conf En este vamos a configurar las políticas de registro de eventos, en que archivo se guardará cada tipo de evento (security, warning, error, verbose, debug, dtmf).

```
full => verbose,debug,notice
messages => warning,error
security => security
dtmf => dtmf
```

  Luego de esto se recarga la configuración de Asterisk

```
asterisk -rx 'logger reload'
```

- **Apache logger**

  Cuando se instala el servicio apache, el paquete de instalación realiza la configuración de los logs en el servidor de manera automática, solamente tenemos que verificar que la instalación de los logs sea correcta.

```
/var/log/apache2/access.log
/var/log/apache2/error.log
/var/log/apache2/domains/$domain.log
/var/log/apache2/domains/$domain.error.log
```

- **Tomcat Logger**

  Tomcat en un servicio WEB de Java que genera una gran cantidad de logs, por este motivo es necesario configurar la rotación de logs en el

servidor, que nos genere seguridad y disponibilidad.

En el contenedor de tomcat se encuentra el fichero de logs **/usr/share/tomcat7/logs**. En el directorio de logs podemos observar que tenemos varios logs que son generados por el servicio del tomcat los cuales son los siguientes:

Catalina.out: En este archivo se guarda todo lo escrito en system.out/System.err de las aplicaciones que son ejecutadas en el contenedor de tomcat.

catalina.YYYY-MM-DD.log: Es la salida que se graba en catalina.out también se graba en estos ficheros, los cuales se les aplica una rotación de un día.

localhost_access_log.YYYY-MM-DD.txt: Es el fichero encargado de almacenar todos los logs de acceso a las aplicaciones que utilizan el contenedor de tomcat.

localhost.YYYY-MM-DD.log: Fichero de eventos de log de las aplicaciones que corren en el contenedor.
manager.YYYY-MM-DD.log: Fichero de los log de eventos del manager del tomcat.

host_manager.YYYY-MM-DD.log: Fichero de los log de eventos del host_manager de tomcat.

- **Logrotate Tomcat**

Creamos el fichero /etc/logrotate.d/tomcat con el siguiente contenido:

```
/usr/share/tomcat7/logs/catalina.out {
   copytruncate
   daily
   dateext
   rotate 14
   compress
   missingok
   size 20M
   }
```

Con esta configuración, realizamos la rotación diaria del fichero comprimiendo el fichero del día anterior, manteniendo los últimos 14 ficheros. Con un tamaño inferior de 20 MBytes. De esta manera se

eliminará y se comprimieron los log de catalina, evitando el almacenamiento excesivo de logs.

- **MySQL Logger**

  Para activar los logs del MySQL debemos de configurarlos, ya que si no se realiza la configuración adecuada podemos perder la información de logs de la base de datos, es de suma importancia tener todos los logs que genera la base de datos, ya que si la base de datos se daña podremos recuperar la información que no posee el backup realizado a las bases de datos perjudicadas.

  Para activar los logs del MySQL debemos de editar el archivo de configuración:

```
vim /etc/mysql/mysql.conf.d/mysqld.cnf
```

  Buscamos las siguientes líneas y las des comentamos:

```
#general_log_file       = /var/log/mysql/mysql.log
#general_log            = 1
```

  Luego de realizar el cambio, debemos de reiniciar el servicio para que pueda ser aplicado:

```
/etc/init.d/mysql restart
```

c. SSH Server

SSH en un servicio de acceso remoto a los sistemas linux, el cual nos permite acceder de manera remota y segura a los servidores de la organización, aunque el servicio de ssh sea cifrando bajo SSL/TLS, debemos de cambiar las configuraciones por defecto y dar los permisos de acceso solo a los usuarios autorizados.

El archivo de configuración del servicio **/etc/ssh/sshd_config** donde vamos a realizar los siguientes cambios:

- **Cambio de puerto por defecto:**
  Buscamos la línea que dice Port y cambiamos el puerto que trae por defecto (**22**) por el **9911**.

```
# What ports, IPs and protocols we listen for
Port 9911
```

- **Deshabilitar acceso root remoto:**
  Buscamos la línea que dice PermitRootLogin y nos aseguramos que esté saeteada en "**no**"

```
PermitRootLogin no
```

- **Limitar usuarios con conexión SSH:**
  Se edita o agrega la línea **AllowUsers nethexa**

```
AllowUsers nethexa
```

d. FAIL2BAN

Es una aplicación que previene la intrusión de intrusos en las aplicaciones en red que provee el servidor, denegando el acceso de ataques de fuerza bruta que se intente realizar a las aplicaciones en los servidores automáticamente, bloqueando a través del firewall interno del servidor la IP de donde provienen las amenazas.

A continuación, se detallan los pasos de instalación y configuración del aplicativo fail2ban.
Sirve para agregar una capa más de seguridad de nuestro servidor permitiendo configurar reglas de bloqueo por intentos fallidos de conexión o registró en los servicios.

- Se actualiza la lista de repositorios del sistema e instalamos Fail2Ban.

```
apt update
apt install fail2ban
```

Editamos el archivo de configuración **/etc/fail2ban/jail.conf**

- Agregamos las redes que vamos a omitir para que no bloquee intentos fallidos desde la red interna. (cada red se separa con un espacio en blanco).

ignoreip = 127.0.0.1 192.168.0.0/16 172.16.0.0/12 10.0.0.0/8

- Definimos el tiempo de bloqueo para las IP. (10 días)

bantime = 864000

- Definimos la cantidad de intentos fallidos para proceder a bloquear la IP donde la organización definió que deben ser tres.

  maxretry = 3

- Habilitamos los filtros que queremos usar.

  Para el SSH definimos los puertos **9911, 22** y nos cercioramos que esté en modo **enabled = true.**

```
[ssh]

enabled  = true
port     = 9911,22
filter   = sshd
logpath  = /var/log/auth.log
maxretry = 3
```

  El SSH-DDoS nos permite bloquear ataques de denegación de servicios.
  También seleccionamos los puertos **9911, 22** y nos cercioramos que esté en modo **enabled = true**

```
[ssh-ddos]

enabled  = true
port     = 9911,22
filter   = sshd-ddos
logpath  = /var/log/auth.log
maxretry = 3
```

  El APACHE nos permite bloquear por intentos fallidos en los servicios WEB que soportan todas las aplicaciones de E-learning y Telefonía IP.
  Seleccionamos los puertos **80, 443** o por servicios **http, https** y nos cercioramos que esté en modo **enabled = true**

```
[apache]

enabled  = true
port     = http,https
filter   = apache-auth
logpath  = /var/log/apache*/*error.log
maxretry = 6
```

Creamos el filtro para Asterisk

```
[asterisk-iptables]
enabled = true
filter = asterisk
action = iptables-multiport[name=ASTERISK, port="5060,4569",
protocol=udp]
                sendmail-whois[name=ASTERISK-{CLIENTE},
                dest=soporte@nethexa.com, sender=alertas@nethexa.com]
        logpath = /var/log/asterisk/security
        maxretry = 3
        bantime = 864000
```

***Nota**: El parámetro "action" va en una sola línea*

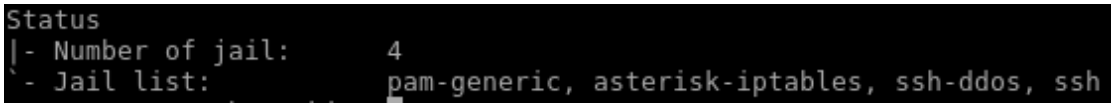
```
[asterisk-iptables]
enabled = true
filter = asterisk
action = iptables-multiport[name=ASTERISK, port="5060,4569", protocol=udp]
sendmail-whois[name=ASTERISK-{CLIENTE}, dest=soporte@nethexa.com, sender=alertas@nethexa.com]
logpath = /var/log/asterisk/security
maxretry = 3
bantime = 864000
```

En MySQL nos permite denegar los intentos fallidos que se realizan al puerto de la base de datos del servidor.

```
[mysql] enabled = true
port = 3306 filter = mysqld-auth
logpath = /var/log/mysql/error.log
maxretry = 3
```

Verificamos que los filtros estén listos

```
fail2ban-client status
```



e. IPTABLES

Es una aplicación de firewall, que permite establecer un firewall local en los servidores; con el fin de, poder permitir y rechazar los puertos habilitados en los servidores WEB. También, es una herramienta importante que trabaja en conjunto de FAIL2BAN para denegar el acceso a los atacantes que atacan a los servidores.

En esta parte se configura el firewall a nivel de servidor, esto evita que se pueda escanear o acceder a los servicios configurados.

Primero debemos instalar y configurar el módulo GeoIP del iptables.

```
apt install libtext-csv-xs-perl xtables-addons-common xtables-addons-dkms

cd /usr/lib/xtables-addons/

./xt_geoip_dl

mkdir -p /usr/share/xt_geoip/LE

/usr/lib/xtables-addons/xt_geoip_build -D /usr/share/xt_geoip/
GeoIPCountryWhois.csv
```

Para tener una referencia de estos procesos, se debe leer el manual de este enlace: https://openwebinars.net/geoip-para-iptables-con-xtables_addons-en-gnulinux-ubuntu-13/

Se descarga desde el servidor el script de iptables. http://nethexa.com/pkgs/iptables-nethexa.sh

Se guarda en la ruta **/usr/sbin/**

Se crea una entrada llamando al script en el archivo **/etc/rc.local** antes de la línea **"exit 0"** para que el script se ejecute cada que el servidor inicie.

```
bash /usr/sbin/iptables-nethexa.sh

exit 0
```

Luego procedemos a ejecutar el script manualmente para que las reglas queden aplicadas.

```
bash /usr/sbin/iptables-nethexa.sh
```

NOTA: Si el servidor maneja servicios adicionales como Tomcat, conexión de AMI u otros, estos se deberán agregar en el script para permitir su acceso.

Además, si el servidor es accedido desde zonas diferentes a Colombia se deben agregar dichas zonas en las reglas del iptables separado por comas en la parte:

“-m geoip --src-cc CO”
Ej: Para permitir Colombia, USA, España, Perú.
-m geoip --src-cc CO, US, ES,PE

La regla completa quedaría así:
/sbin/iptables -A INPUT -p tcp -m state --state NEW -m tcp --dport 80 -m geoip --src-cc CO,US,ES,PE -j ACCEPT

f. MOTD

Banner de inicio de sesión, el cual nos brinda información relevante del estado del servidor, con el propósito de brindar información adicional que sea útil para el equipo de soporte y el mensaje de propiedad de la organización.

Editamos el siguiente archivo:
/usr/local/bin/systemstats.sh

Dentro del archivo ingresan el siguiente código completo.

```
#!/bin/bash
CPUTIME=$(ps -eo pcpu | awk 'NR>1' | awk '{tot=tot+$1} END {print tot}')
CPUCORES=$(cat /proc/cpuinfo | grep -c processor)
UP=$(echo `uptime` | awk '{ print $3 " " $4 }')
echo "
```

```
Estado del Sistema
Actualizado a: `date`
- Nombre del Servidor       = `hostname`
- IP Publica               = `wget http://ipecho.net/plain -O - -q ; echo`
- Versión de Debian         = `cat /etc/debian_version`
- Promedio de Carga         = `cat /proc/loadavg`
- Tiempo al Aire            = `echo $UP`
- Datos de plataforma       = `uname -orpi`
- Uso de CPU (promedio)     = `echo $CPUTIME / $CPUCORES | bc`%
- Memoria disponible (real)  = `free -m | head -n 2 | tail -n 1 | awk {'print $4'}` Mb
- Memory disponible (cache)  = `free -m | head -n 3 | tail -n 1 | awk {'print $3'}` Mb
- Swap en uso               = `free -m | tail -n 1 | awk {'print $3'}` Mb
- Espacio de disco Usado    = `df -h / | awk '{ a = $4 } END { print a }'` - `df -h / | awk '{ a = $5 } END { print a }'`
-------------------------
Powered by Grupo Nethexa
soporte@nethexa.com
-------------------------
" > /etc/motd
# End of script
```

Se hace que el archivo sea ejecutable
chmod +x /usr/local/bin/systemstats.sh

Agregamos en el crontab el comando para que se ejecute cada 5 minutos.

 # Status Script
***/5 * * * * root /usr/local/bin/systemstats.sh > /dev/null 2>&1**

Ejecutamos el script manualmente para validar que no tenga errores.
/usr/local/bin/systemstats.sh

5. Seguridad de los servicios WEB

a. Apache2

Servicio que administra las páginas web de e-learning y telefonía IP de la organización de código abierto. A continuación, se detallan los pasos de configuración de la seguridad en el web server apache.

- Debemos cambiar la ruta por defecto para alojar los sitios web que se implementen en los servidores.

  Crear una nueva ruta en el directorio **/opt**, donde se almacenan todas las aplicaciones de terceros en Linux.

  ```
  mkdir -p /opt/www/html
  ```

  Realizar los cambios en el archivo de configuración de apache **/etc/apache2/apache2.conf**, para que empiece a apuntar al nuevo directorio.

  ```
  <Directory /opt/www/html/>
          Options -Indexes -FollowSymLinks -ExecCGI
  +SymLinksIfOwnerMatch
          AllowOverride None
          Require all granted
  </Directory>
  ```

  Configurar la ruta del nuevo directorio en los sitios configurados en el servicio web, por ejemplo:**/etc/apache2/sites-enabled/000-default.conf**.

  ```
  DocumentRoot /opt/www/html
  ```

  Se deben de realizar los cambios del punto de montaje del directorio **/opt** en el servidor, habilitando las siguientes opciones que nos proporcionan limitaciones de seguridad de la información contenida en el directorio:
  -nodev: Impide la interpretación de los dispositivos especiales o de bloques del sistema de archivos.
  -nosuid: Bloquea el funcionamiento de suid, y sgid bits. Suid permite a los usuarios comunes ejecutar binarios con privilegios concedidos temporalmente.
  -noexec: No permite la ejecución de binarios que se encuentren en el sistema de archivos.

  Se anexa ejemplo de cómo se realiza la configuración en el archivo de montaje /etc/fstab

  ```
  UUID=82feb5e0-6c7c-4df5-9e9d-8cf2f5e0191b /opt   ext4
  nodev,nosuid,noexec 0 2
  ```

- Evitar la búsqueda de DNS para que los equipos se puedan registrar en el servidor. Editamos el archivo **vim /etc/apache2/apache2.conf**.

  Buscamos y realizamos el siguiente cambio:

```
HostnameLookups Off
```

- Se establecen parámetros para que la información relevante como el sistema operativo, versiones, etc. no sea visible públicamente desde el escaneo del servicio.

  Editamos el archivo de configuración de seguridad de apache, el cual se encuentra en la ruta **vim /etc/apache2/conf-enabled/security.conf**.

  Luego editamos la siguiente configuración; con el fin de, ocultar la información de versión del servidor:

```
#Deshabilitar la firma de páginas web por el servicio
Apache
ServerSignature Off

#No mostrar todos los datos del verbose mode en apache
ServerTokens Prod
```

  Desactivamos las peticiones de seguimiento HTTP del servidor:

```
# Set to one of:On|Off|extended
TraceEnable Off
```

  Deshabilitar las etiquetas de información en la caché de la WEB:

```
#Desactivar las Etags
FileETag None
```

  Restringir el acceso al directorio raíz (/):

```
<Directory />
        Order
deny,allow
        Deny from all
        Options None
```

```
<IfModule ssl_module>
      Listen 0.0.0.0:443
</IfModule>

<IfModule mod_gnutls.c>
      Listen 0.0.0.0:443
</IfModule>
```

```
      AllowOverride
None
  </Directory>
```

- **Options None:** No permitir ninguna de las características adicionales opcionales.
- **Order deny, allow:** Proceso de “negar” primero.
- **Deny from all:** Denegar cualquier solicitud al directorio raíz.
- **AllowOverride None:** Denegar el uso del archivo .htaccess

Nota: Las opciones “**Order deny, allow**” y “**Deny from all**” pueden ser sustituidas en apache 2.4 por “**Require all denied**”

- Desactivar la escucha por direccionamiento ipv6, si no se está utilizando en el servidor. Editamos el archivo **vim /etc/apache2/ports.conf**.

Realizamos el siguiente cambio en el archivo de configuración:

```
Listen 0.0.0.0:80
```

Si estamos utilizando SSL, que sería lo ideal debemos de configurar los siguiente:

- Mitigación de ataques de denegación de servicios en el servicio WEB.

Activamos el módulo **sudo a2enmod reqtimeout**:

```
Enabling module reqtimeout.
To activate the new configuration, you need to run:
```

```
service apache2 restart
```

Activamos el módulo headres **sudo a2enmod headers**:

```
Enabling module headers.
To activate the new configuration, you need to run:
 service apache2 restart
```

Desactivar el módulo status sudo a2dismod status:

- Revisamos y cambiamos los permisos del código que se colocará en el servidor WEB.

```
find /web/httpd/htdocs -perm 777 -type f
```

```
find /web/httpd/htdocs -type f -name '*.php' -exec chmod
644 {} \;
```

- En el servidor se instala el certificado digital SSL para cifrar toda la información de acceso a las aplicaciones WEB, esta información es proporcionada por el sitio oficial de Apache.

  Al tener las llaves del certificado “llave privada, clave pública y el certificado generado por la CA”, se deben de agregar en el servidor en el directorio donde se va a realizar el almacenamiento de esta.

  Habilitar el módulo de ssl del servicio WEB de Apache

```
a2enmod ssl
service apache2 restart
```

  Copiamos la configuración del sitio que estamos utilizando y la renombramos con el identificador SSL.

```
cp 000-default.conf 000-default.conf-ssl
```

  Ingresar al sitio WEB habilitado y realizar la configuración del <VirtualHost> para habilitar el cifrado del sitio WEB.

```
/etc/apache2/sites-enabled/000-default.conf-ssl
```

Primero cambiamos el puerto del 80 al 443, el cual corresponde al protocolo HTTPS:

```
<VirtualHost *:443>
```

Luego cambiamos los archivos de los logs, agregando los archivos de los del sitio SSL:

```
ErrorLog /var/log/apache2/000-default.conf-ssl-error.log
CustomLog /var/log/apache2/000-default.conf-ssl-
access.log combined
```

Configuramos dentro de la sección <VirtualHost> los certificados que vamos a utilizar en el sitio WEB.

```
SSLEngine on

      SSLCertificateFile
/etc/letsencrypt/live/web.nethexa.com/cert.pem
      SSLCertificateKeyFile
/etc/letsencrypt/live/web.nethexa.com/privkey.pem
```

Se configura HSTS para obligar que todas las conexiones al servidor dean a través de HTTPS:

```
Header always set Strict-Transport-Security "max-
age=4838400; includeSubdomains;"
```

Luego de realizar la configuración, se procede a habilitar el sitio WEB y a reiniciar los servicios para recargar la configuración:

```
/etc/apache2/sites-available# a2ensite 000-default.conf-
ssl
Enabling site 000-default.conf-ssl.
To activate the new configuration, you need to run:
 service apache2 reload
```

```
/etc/apache2/sites-available# service apache2 reload
[ ok ] Reloading web server config: apache2.
```

b. Tomcat

Para asegurar el contenedor de aplicaciones WEB en Java de Apache, con el fin de evitar proporcionar información a los usuarios o a los atacantes de los servicios que están corriendo los servidores WEB, debemos de realizar un aseguramiento mínimo del servicio que permita aumentar la disponibilidad de las aplicaciones que corren bajo el servicio.

- Primero debemos de ocultar los detalles del producto y el encabezado de conexión del servidor, para esto entramos a editar el archivo de configuración **vim /etc/tomcat/server.xml**. En el archivo de configuración añadimos en **connector port** la línea de configuración **Server =" "**, como se muestra en la configuración:

```
<Connector port="8080" protocol="HTTP/1.1"
connectionTimeout="20000"
Server =" "
redirectPort="8443" />
```

  Luego guardamos el archivo y reiniciamos el tomcat para cargar la configuración, cuando realizamos esto el servidor ya lo proporciona el encabezado del servidor.

- Ejecutar tomcat como administrador de seguridad, iniciando el tomcat con Security Manager, para proteger las aplicaciones de una Applet (Componente de aplicación que se puede ejecutar en otro programa). Todo lo que tenemos que hacer es ejecutar el tomcat con **-security**:

```
./startup.sh -security
```

- Al habilitar el uso de SSL/TLS en el Apache como medida de seguridad por obligación, debemos de configurar el tomcat para que se pueda acceder por HTTPS y poder asegurar la información entre el cliente servidor. En el archivo de configuración **vim /etc/tomcat/server.xml**, en el campo **connector port** añadimos la siguiente línea de configuración:

```
SSLEnabled = "true" scheme = "https" keystoreFile =
"/etc/letsencrypt/live/web.nethexa.com/cert.pem "
```

```
keystorePass =
"/etc/letsencrypt/live/web.nethexa.com/privkey.pem"
clientAuth = "false" sslProtocol = "TLS"
```

Asegurar que el acceso solo se permite por HTTPS, impidiendo que puedan romper la aplicación y tener acceso por HTTP. Para realiza el cambio debemos de ir al directorio de configuración del tomcat y editar el archivo de configuración **vim web.xml** y agregamos las siguientes líneas de configuración antes de la sintaxis **</web-app>:**

```
<security-constraint>
<web-resource-collection>
<web-resource-name>Protected Context</web-
resource-name>
<url-pattern>/*</url-pattern>
</web-resource-collection>
<user-data-constraint>
<transport-guarantee>CONFIDENTIAL</transport-
guarantee>
</user-data-constraint>
</security-constraint>
```

Guardamos el archivo y reiniciar el tomcat para que pueda cargar las configuraciones.

- Agregar el marcador de seguridad y HTTPOnly a la cookie, impidiendo la manipulación de la aplicación WEB y las cookies. Esto lo realizamos en el archivo de configuración **web.xml** y agregamos las siguientes líneas en **session-config**:

```
<cookie-config>
<http-only> true </http-only>
<secure> true </secure>
</cookie-config>
```

Guardamos y reiniciamos el tomcat.

- Ejecutar tomcat desde una cuenta no privilegiada; con el objetivo de, proteger otros servicios que están corriendo en el servidor en caso de que alguna de las cuentas del tomcat se vea comprometida.

Creamos los usuarios tomcat:

```
useradd tomcat
```

Luego detenemos el comcat y asignamos la propiedad del directorio /tomcat a los usuarios creados:

```
chown -R tomcat:tomcat tomcat/
```

Reiniciamos el tomcat y verificamos que esté corriendo con los usuarios tomcat.

- Debemos de eliminar las aplicaciones predeterminadas y no necesarias en el entorno de producción; con el fin de, tener el contenedor lo más limpio posible y evitar cualquier riesgo de tomcat que se encuentre por defecto en el servicio.

  Los archivos por defecto son:

  - **ROOT:** Página de bienvenida por defecto.
  - **Docs:** Documentación Tomcat.
  - **Ejemplos**: JSP y servlets para demostración.
  - **Manager, host-manager:** administración de Tomcat.

  Están disponibles en el directorio **$tomcat/webapps**.

- Cambiar el puerto y comando shutdown, ya que de forma predeterminada tomcat está configurado para apagarse en el puerto 8005. Esta configuración es cambiada porque es un riesgo alto de seguridad para el servicio y las aplicaciones, debido a que un telnet a la ip:8005 con el comando shutdown apaga el servicio y las aplicaciones dejarían de funcionar.

  Como recomendación se cambia el puerto predeterminado y el camino de apagado en el archivo de configuración del tomcat **server.xml.**

  ```
  <Server port="8005" shutdown="SHUTDOWN">
  ```

  Cambiar el puerto por uno no utilizado y cambiar el comando por una palabra más difícil.

- Por último, debemos de reemplazar y/o cambiar las alertas de error por defecto que son 403, 404 y 500, ya que este error nos muestra la información de la versión del tomcat que está utilizando el servidor.

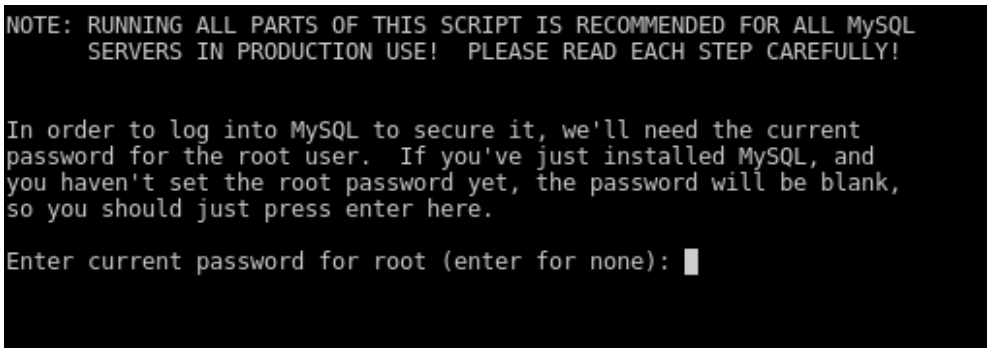
c. MySQL

Para configurar mejor el servicio de acceso y permisos de usuarios en la base de datos, es recomendable ejecutar el script que trae el sistema para mejorar la seguridad del servicio:

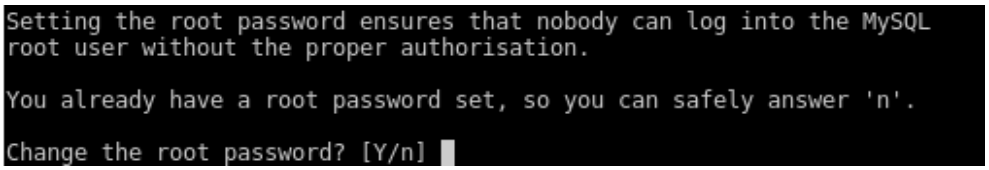
mysql_secure_installation

El sistema nos arroja una serie de preguntas para aplicarlos cambios que requerimos en la base de datos.:

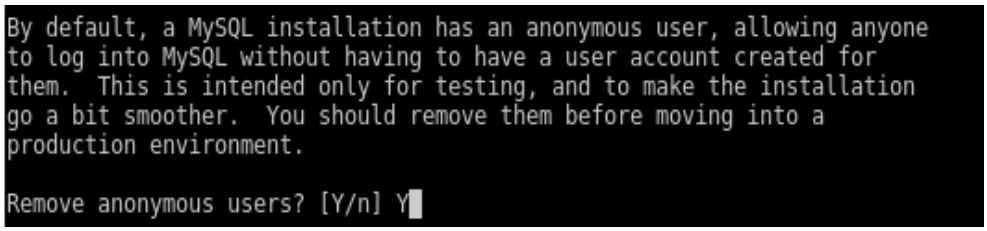
Primero nos pide la contraseña de acceso del usuario root. La ingresamos y presionamos **ENTER**.



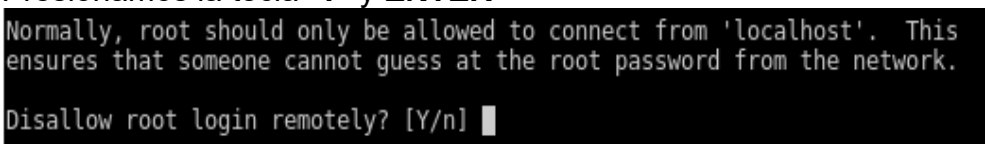
Nos pregunta si queremos cambiar el password del root de MySQL. Si se requiere hacer la actualización presionamos la tecla "**Y**", si no se omite el paso presionando la tecla "**N**"



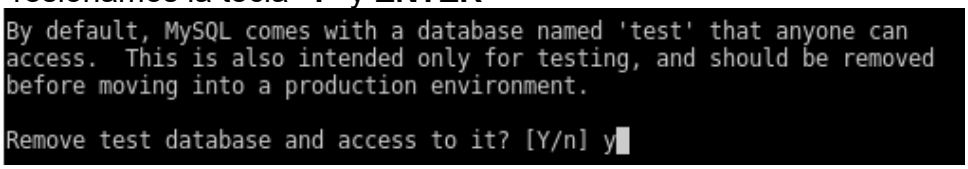
Luego el sistema nos pregunta si queremos eliminar usuarios anónimos.
Presionamos la tecla "**Y**" y **ENTER**



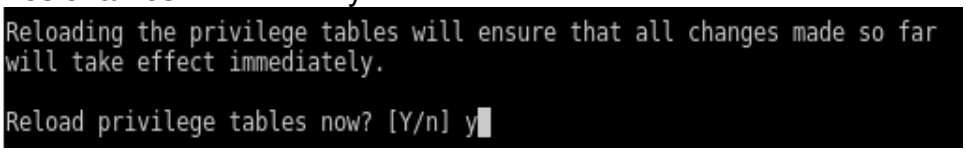
A continuación, podemos deshabilitar el acceso remoto con usuario root, generalmente se debe hacer, solo en casos especiales se permite este acceso.
Presionamos la tecla "**Y**" y **ENTER**



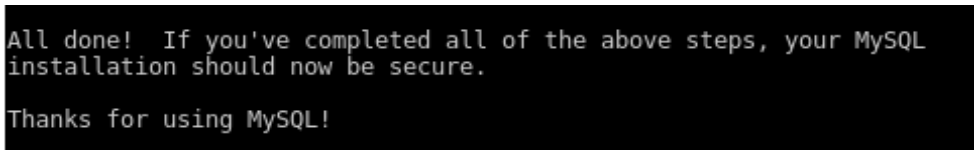
Eliminamos la base de datos "**test**" y su usuario de acceso.
Presionamos la tecla "**Y**" y **ENTER**



Recargamos la tabla de privilegios para que los cambios se apliquen.
Presionamos la tecla "**Y**" y **ENTER**



Si todo finalizó correctamente, nos muestra un aviso como el que se ve a continuación.



d. Asterisk

A continuación, se detallan los pasos de configuración de la seguridad en asterisk, servicio que nos permite establecer una PBX en el servidor.

- En esta parte se establecen parámetros para que la información relevante del sistema no sea visible públicamente y pueda bloquear a nivel de aplicación accesos no autorizados.

  Editamos el archivo **/etc/asterisk/sip_general_custom.conf** y agregamos o modificamos los siguientes parámetros.

```
useragent=XXXXXXXXXX
sdpsession=XXXXXX
sdpowner=XXXXXX
alwaysauthreject=yes
allowguest=no
language=es
```

- **Administradores del sistema AsteriskNow**

  En la sección **Admin** => **Administrators**
  Nos cercioramos que no exista un usuario **“admin”.**
  Debe existir un usuario **“nethexa”** con la contraseña que se maneja en la compañía.
  Si el cliente requiere de un usuario, se debe procurar limitar los permisos.

- **Plan de numeración**

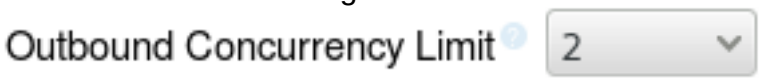
  De ser posible las extensiones deben ser de mínimo 4 dígitos, esto con el fin de dificultar el escaneo de extensiones válidas por software malicioso.

- **Limitar concurrencia por extensiones**

  Limitamos el número máximo de llamadas concurrentes por extensión.
  Este valor se establecerá por defecto cuando se crea una nueva extensión.
  En la sección **Settings** => **Advanced Settings**
  Buscamos el parámetro **“Extension Concurrency Limit”**
  Configuramos este en “2”.

  NOTA: Si la extensión ya está creada se deberá modificar manualmente para cada extensión.
  Por defecto deben ser 2 llamadas concurrentes para extensiones normales, para extensiones con telefono

secretarial se debe configurar en 6.



- **Contraseñas seguras para extensiones**

  En la sección **Admin** => **Module Admin**.
  Buscamos el módulo **"Weak Password Detection"** y nos cercioramos de que esté instalado.
  Luego en el apartado **Reports** => **Weak Password Detection**
  Podemos observar el reporte de extensiones con configuraciones de contraseña débiles.
  Se deben modificar aquellas que allí estén reportadas.

  Las contraseñas deben contar con un mínimo de 12 caracteres alfanuméricos.
  Se pueden generar contraseñas seguras en http://password.es/
  Adicional se deben seguir las recomendaciones del módulo.

  Weak Password Detection

Type	Name	Secret	Message
Extension	1111	1111ofic	Secret has consecutive digit 1
Extension	2222	2222vib3	Secret has consecutive digit 2
Extension	11117	11117ofic	Secret has consecutive digit 1

  Como se ve en la imagen, las extensiones no deben tener el mismo caracter 2 o más veces de forma consecutiva.

6. Bibliografía.

RedHat (2017). Guía de seguridad, Red Hat Enterprise Linux 6. Recuperado: https://access.redhat.com/documentation/es-es/red_hat_enterprise_linux/6/pdf/security_guide/Red_Hat_Enterprise_Linux-6-Security_Guide-es-ES.pdf, 11 de septiembre de 2018.

Linux_Trucepei_Blog (2017). Aseguramiento de servidor WEB apache. Recuperado: https://juantrucupei.wordpress.com/2017/05/24/seguridad-apache-tips/, 8 de noviembre de 2018.

Linuxito (2016). Cómo asegurar SSl en Apache. Recuperado: https://www.linuxito.com/seguridad/664-como-configurar-ssl-en-apache-debian, 8 de noviembre de 2018.

C. Kumar (2018). Apache Tomcat Hardening and Security Guide. Recuperado: https://geekflare.com/apache-tomcat-hardening-and-security-guide/, 8 de noviembre de 2018.

ANEXO 26

SEGURIDAD DEL TRÁFICO EN LA RED

Define los controles de seguridad que se realiza a nivel perimetral de la red, los cuales obedecen a las políticas creadas en el SGSI. La finalidad de la seguridad perimetral del tráfico de red, es poder tener una estandarización del tráfico que es permitido y rechazado en el establecimiento de la comunicación de los servicios de los usuarios y las plataformas web de cada cliente.

El objetivo principal es poder otorgar seguridad, estabilidad, disponibilidad y eficiencia en la comunicación hacia los servicios web de las plataformas de los clientes, generando mayor seguridad y monitoreo de todas las conexiones que son realizadas a los servidores mitigando los siguientes riesgos identificados por la organización:

- Malware.
- Interceptación de información.
- Ataques de DoS/DDoS.
- Pérdida de control de acceso.
- Configuraciones de seguridad incorrectas.
- Uso de componentes con vulnerabilidades conocidas.
- Registro y monitoreo insuficiente.
- Ataques de fuerza bruta.
- Ataques de día cero.

Reduciendo los riesgos anteriores, la organización puede dar mayor confiabilidad de los clientes y puede aceptar el riesgo informático crítico que tenía presente. Para mitigar los riesgos se generan controles en la administración de seguridad del tráfico de red, que se pueden evidenciar en el diseño de red de las plataformas de la organización y en la descripción de los controles.

Los controles de seguridad para las dos soluciones son los mismos, lo único que cambia es la estructura de seguridad en la comunicación, ya que e-learning solo tiene dos segmentos de red, un segmento DMZ y un segmento WAN que permite la comunicación con los demás aplicativos internos y la comunicación de la plataforma con los usuarios externos. En cambio, la telefonía IP tiene muchos más segmentos de red, ya que los usuarios que utilizan el servicio son internos, por lo que se realizan segmentos adicionales los cuales pertenecen a equipos de cómputo, telefonía, red inalámbrica, etc. Los cuales corresponden al segmento LAN.

Figura 1: Diagrama de red de e-learning

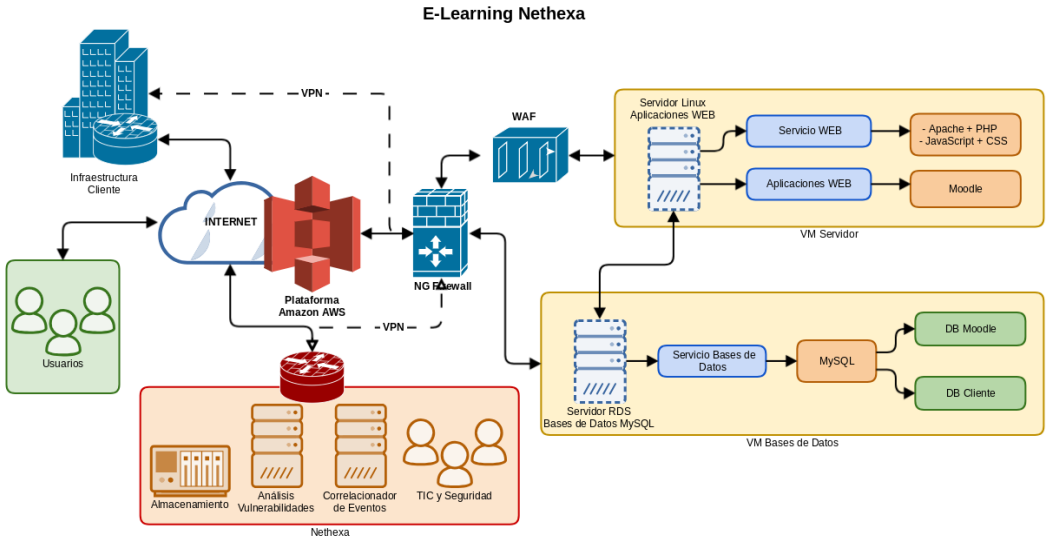
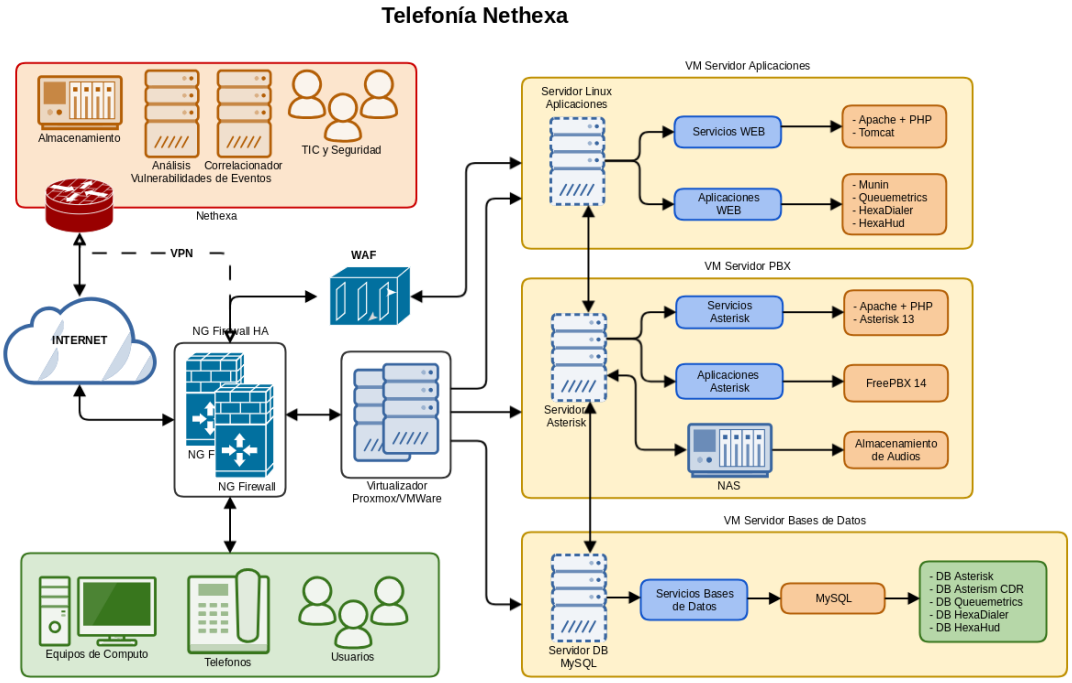


Figura 2: Diagrama de red de telefonía IP



1. Segmentación de red y enrutamiento

La segmentación de red es proporcionada por la capa de acceso a la red y el enrutamiento es proporcionado por la capa de Internet. El objetivo principal

de este control es poder realizar una separación lógica de los servidores, usuarios, administradores de TIC y seguridad, plataformas de monitoreo y seguridad, teléfonos, equipos de cómputo, etc. Permitiendo administrar mejor las políticas de seguridad del tráfico de red a través de zonas de seguridad, las cuales nos permiten realizar una adecuada separación de los segmentos de red y enrutamiento de red, mejorando la administración de políticas de seguridad que se aplican en la red perimetral.

Las zonas que se utilizan para las soluciones son las siguientes:

- Zona WAN: Son los segmentos de red proporcionados por los proveedores de servicios que interconectan a través de un canal de Internet los servicios web de la organización.
- Zona DMZ: Es el segmento de red donde se encuentran todos los servidores que permiten el funcionamiento de las plataformas web administradas por la organización.

- Zona LAN: Segmento de red donde se encuentran conectados los equipos de cómputo, telefonía IP, redes inalámbricas, etc. Redes que son internas en las organizaciones de los clientes.

- Zona VPN: Es la comunicación con otros segmentos de red que posee un dispositivo de red remoto, permitiendo la comunicación de un segmento local con un segmento remoto, con direccionamiento privado.

- Zona VPN SSL: Comunicación de los equipos de cómputo que poseen el permiso de conectarse directamente a la red local a través de una red pública, estableciendo una conexión cifrada cliente servidor de manera directa al computador.

Las zonas permiten establecer las políticas de tráfico de red seguro de la conexión de los usuarios y segmentos de red permitidos, reduciendo el riesgo cerrando los puertos de comunicación innecesarios interna y externamente de las plataformas web administradas por la organización.

Segmentos que poseen los servicios en la nube son: Zona WAN, Zona DMZ, Zona VPN y Zona VPN SSL.

Segmentos que poseen los servicios de telefonía IP son: Zona WAN, Zona LAN, Zona DMZ, Zona VPN y Zona VPN SSL.

2. Balanceo de carga

Es un servicio de red que nos permite realizar un control de alta disponibilidad y contingencia de la comunicación de las plataformas de la organización de los clientes, el cual nos permite utilizar canales de Internet simultáneos redundantes y nos permite distribuir las cargas de conexión en los servidores, distribuyendo el tráfico a los diferentes servicios que proveen el servicio de manera redundante. El control nos permite tener alta disponibilidad de las plataformas web que son administradas por la organización.

3. Políticas de firewall

El firewall permite otorgar los permisos del tráfico entrante y saliente a las plataformas web de la organización, implementando políticas de acceso a todos los puertos necesarios para que el servicio pueda funcionar en el tiempo y pueda ser debidamente administrado. El firewall por defecto tiene que tener la política de denegación de servicio de todo el tráfico hacia todas las zonas de seguridad perimetral, con el objetivo de aceptar todo el tráfico necesario para el funcionamiento de los servicios y plataformas web.

Como mencionamos anteriormente, en la segmentación de servicios, es mucho más fácil la administración de las políticas de seguridad, para iniciar con la restricción de acceso en la red, la cual es un control de seguridad esencial para la prestación de servicios perimetral en la red, vamos a definir las reglas autorizadas de aceptación del tráfico , toda regla creada en el firewall es documentada y comentada para futuros soportes y resolución fácil de problemas que se puedan presentar en el bloqueo del tráfico de red.

Las políticas definidas para los servicios de e-learning son los siguientes:

- **WAN > WAN**
  Es el tráfico de comunicación del firewall hacia la red de Internet.

    - Aceptar el puerto de administración HTTPS [3344] del firewall desde la red de origen publica de GRUPO NETHEXA S.A.S, para su administración.
    - Aceptar el tráfico desde cualquier origen al firewall por el puerto UDP 123, para la sincronización automática horaria.
    - Aceptar el tráfico de origen del fabricante del firewall, para las actualizaciones automáticas de los servicios que presta.
    - Aceptar el tráfico del servicio VPN SSL [4433], para el establecimiento de la VPN de los usuarios autorizados para la administración de los servidores de las plataformas de e-learning.

- Aceptar el tráfico del servicio IPSec [500] UDP, para el establecimiento de VPN con la infraestructura de los clientes y la administración de TIC y seguridad en GRUPO NETHEXA S.A.S.
- Bloquear desde cualquier origen a cualquier destino todos los servicios y/o puertos tcp y udp, impidiendo el ingreso de las demás solicitudes.

- **WAN > DMZ**
  Es el tráfico de todos los usuarios que acceden a los cursos de e-learning desde la red de Internet.

  - Aceptar desde cualquier origen al dispositivo de seguridad WAF por el servicio HTTPS [443], el cual realiza balanceo y análisis de seguridad del tráfico entrante hacia los servidores web de e-learning, el cual es el encargado de proporcionar el servicio web a los usuarios desde Internet.
  - Aceptar el tráfico desde cualquier origen al firewall por el puerto UDP 123, para la sincronización automática horaria.
  - Aceptar el tráfico de origen del fabricante del WAF, para las actualizaciones automáticas de los servicios que presta.
  - Bloquear desde cualquier origen a cualquier destino todos los servicios y/o puertos tcp y udp, impidiendo el ingreso de las demás solicitudes.

- **DMZ > WAN**
  Es el tráfico de navegación permitido hacia Internet de los servidores de la organización.

  - Aceptar el tráfico HTTP [80], HTTPS [443] y HTTPS segundario [8443] hacia Internet, para la búsqueda de y descarga de actualizaciones de los servidores.
  - Aceptar el acceso al puerto UDP 123 para la sincronización automática de la zona horaria de los servidores.
  - Aceptar el siguiente tráfico TCP de salida, para el envío de correos cifrados seguros de los servidores, los servicios son los siguientes: TCP_TLS_SMTP [587], TCP_SSL_SMTP [465] y TCP_SSL_IMAP [993].
  - Aceptar el tráfico saliente TCP para el envío de correos de los servidores, los servicios son los siguientes: SMTP [25], POP3 [110] y IMAP [143].
  - Aceptar el servicio DNS [53] en los protocolos TCP y UDP, para la resolución de nombres en Internet.

- Bloquear desde cualquier origen a cualquier destino todos los servicios y/o puertos tcp y udp, impidiendo el ingreso de las demás solicitudes.

- **VPN > DMZ**
  Comunicación de los segmentos de red autorizados de la infraestructura del cliente y los segmentos de red de soporte de GRUPO NETHEXA S.A.S.

  - Aceptar el tráfico del protocolo ICMP desde la red de la infraestructura del cliente y la red de soporte nethexa, para realizar las validaciones correspondientes de conectividad.
  - Aceptar el tráfico de UDP del puerto 161 para el registro del servidor de monitoreo.
  - Aceptar todos los puertos y servicios disponibles para el registro de los servicios de escaneo de vulnerabilidades y correlación de eventos.
  - Aceptar el puerto TCP 9911 desde las redes remotas, que permita la conexión de acceso SSH a los servidores para su administración desde la red remota de nethexa.
  - Aceptar los puertos y servicios HTTP [80] y HTTPS [443], para el ingreso a las plataformas de e-learning para la administración desde las redes de nethexa y el cliente.
  - Aceptar el puerto TCP 3306 para el ingreso remoto al servidor de bases de datos, para la administración y mantenimiento de estas desde la red remota de nethexa.
  - Aceptar los puertos TCP de los servicios LDAP [389], LDAPS [636] y Single Sing On [2258], hacia la infraestructura del cliente, para el registro de los usuarios en el directorio activo del servidor y del firewall.
  - Aceptar el puerto de administración HTTPS [3344] del firewall desde la red de GRUPO NETHEXA S.A.S, para su administración.
  - Bloquear desde cualquier origen a cualquier destino todos los servicios y/o puertos tcp y udp, impidiendo el ingreso de las demás solicitudes.

- **DMZ > VPN**
  Comunicación del segmento de red de los servidores con la infraestructura autorizada del cliente y del segmento de red del equipo de soporte de GRUPO NETHEXA S.A.S.

- Aceptar el tráfico del protocolo ICMP desde la red de los servidores, para realizar las validaciones correspondientes de conectividad desde la red del cliente y de nethexa.
- Aceptar el tráfico de UDP del puerto 161 para el registro del servidor de monitoreo.
- Aceptar todos los puertos y servicios disponibles para el registro de los servicios de escaneo de vulnerabilidades y correlación de eventos.
- Aceptar el puerto TCP 9911 desde el segmento de servidores, que permita la conexión de acceso SSH los equipos de la red de soporte de nethexa.
- Aceptar el puerto TCP 3306 para la comunicación y establecimiento de comunicación de bases de datos alojadas en el segmento de equipos de soporte de nethexa.
- Aceptar los puertos TCP de los servicios LDAP [389], LDAPS [636] y Single Sing On [2258], desde la red de servidores, para el registro de los usuarios en el directorio activo del servidor y del firewall.
- Aceptar el puerto de administración HTTPS [3344] del firewall desde la red de Grupo Nethexa, para su administración.
- Bloquear desde cualquier origen a cualquier destino todos los servicios y/o puertos tcp y udp, impidiendo el ingreso de las demás solicitudes.

- **VPN SSL > DMZ**
  Comunicación cifrada segura a los servidores de la DMZ, desde un computador en una red pública para su administración y soporte cuando no se encuentran en las instalaciones de la empresa.

  - Aceptar el tráfico del protocolo ICMP desde el cliente VPN de soporte Nethexa, para realizar las validaciones correspondientes de conectividad.
  - Aceptar el puerto TCP 9911 desde el cliente VPN de soporte Nethexa, que permita la conexión de acceso SSH a los servidores para su administración remotamente.
  - Aceptar los puertos y servicios HTTP [80] y HTTPS [443], para el ingreso a las plataformas de e-learning para la administración desde la red otorgada al cliente VPN de soporte Nethexa.
  - Aceptar el puerto TCP 3306 para el ingreso remoto del servidor de bases de datos, para la administración y mantenimiento de estas desde el cliente VPN de soporte Nethexa.
  - Aceptar el puerto de administración HTTPS [3344] del firewall desde la red cliente VPN de soporte Nethexa para su administración segura.

- Bloquear desde cualquier origen a cualquier destino todos los servicios y/o puertos tcp y udp, impidiendo el ingreso de las demás solicitudes.

- **DMZ > VPN SSL**
  Comunicación cifrada segura de los servidores de la DMZ a al segmento de red de clientes VPN de soporte Nethexa, desde un computador en una red pública para su administración y soporte cuando no se encuentran en las instalaciones de la empresa.

  - Aceptar el tráfico del protocolo ICMP desde el segmento DMZ de servidores, para realizar las validaciones correspondientes de conectividad.
  - Aceptar el puerto TCP 9911 desde el segmento DMZ de servidores, que permita la conexión de acceso SSH a los servidores para su administración remotamente.
  - Aceptar los puertos y servicios HTTP [80] y HTTPS [443], para el ingreso a las plataformas de e-learning para la administración desde la red DMZ de servidores.
  - Aceptar el puerto TCP 3306 para el ingreso remoto del servidor de bases de datos, para la administración y mantenimiento de estas desde la red DMZ de los servidores.
  - Aceptar el puerto de administración HTTPS [3344] del firewall desde la red DMZ de los servidores.
  - Bloquear desde cualquier origen a cualquier destino todos los servicios y/o puertos tcp y udp, impidiendo el ingreso de las demás solicitudes.

Las políticas definidas para los servicios de telefonía IP son los siguientes:

- **WAN > WAN**
  Es el tráfico de comunicación del firewall hacia la red de Internet.

  - Aceptar el puerto de administración HTTPS [3344] del firewall desde la red de origen publica de GRUPO NETHEXA S.A.S, para su administración.
  - Aceptar el tráfico desde cualquier origen al firewall por el puerto UDP 123, para la sincronización automática horaria.
  - Aceptar el tráfico de origen del fabricante del firewall, para las actualizaciones automáticas de los servicios que presta.
  - Aceptar el tráfico del servicio VPN SSL [4433], para el establecimiento de la VPN de los usuarios autorizados para la administración de los servidores de las plataformas de telefonía IP.

- Aceptar el tráfico del servicio IPSec [500] UDP, para el establecimiento de VPN con la infraestructura de los clientes y la administración de TIC y seguridad en GRUPO NETHEXA S.A.S.
- Bloquear desde cualquier origen a cualquier destino todos los servicios y/o puertos tcp y udp, impidiendo el ingreso de las demás solicitudes.

- **WAN > DMZ**
  Es el tráfico entrante que es generado desde la red de Internet hacia los servidores directamente.

  - Aceptar el tráfico desde cualquier origen al firewall por el puerto UDP 123, para la sincronización automática horaria.
  - Aceptar el tráfico de origen del fabricante del WAF, para las actualizaciones automáticas de los servicios que presta.
  - Bloquear desde cualquier origen a cualquier destino todos los servicios y/o puertos tcp y udp, impidiendo el ingreso de las demás solicitudes.

- **WAN > LAN**
  Es el tráfico entrante que es generado desde la red de Internet hacia el usuario, equipos de cómputo, teléfonos, etc. Desde la red de internet.

  - Aceptar el tráfico desde cualquier origen al firewall por el puerto UDP 123, para la sincronización automática horaria.
  - Bloquear desde cualquier origen a cualquier destino todos los servicios y/o puertos tcp y udp, impidiendo el ingreso de las demás solicitudes.

- **DMZ > WAN**
  Es el tráfico de navegación permitido hacia Internet de los servidores de la organización.

  - Aceptar el tráfico HTTP [80], HTTPS [443] y HTTPS segundario [8443] hacia Internet, para la búsqueda de y descarga de actualizaciones de los servidores.
  - Aceptar el acceso al puerto UDP 123 para la sincronización automática de la zona horaria de los servidores.
  - Aceptar el siguiente tráfico TCP de salida, para el envío de correos cifrados seguros de los servidores, los servicios son los siguientes: TCP_TLS_SMTP [587], TCP_SSL_SMTP [465] y TCP_SSL_IMAP [993].

- Aceptar el tráfico saliente TCP para el envío de correos de los servidores, los servicios son los siguientes: SMTP [25], POP3 [110] y IMAP [143].
- Aceptar el servicio DNS [53] en los protocolos TCP y UDP, para la resolución de nombres en Internet.
- Bloquear desde cualquier origen a cualquier destino todos los servicios y/o puertos tcp y udp, impidiendo el ingreso de las demás solicitudes.

- **DMZ > LAN**
  Es el tráfico permitido desde la red servidores hacia los segmentos de red internos como los usuarios, equipos de cómputo, teléfonos, etc.

  - Aceptar el tráfico HTTP [80], HTTPS [443] y HTTPS segundario [8443] hacia las redes locales, para la navegación web de las aplicaciones de telefonía IP.
  - Aceptar el tráfico UDP de los servicios SIP [5060-5063] y RTP [10000-20000] para el registro de las extensiones en el PBX y el establecimiento del tráfico de las llamadas.
  - Bloquear desde cualquier origen a cualquier destino todos los servicios y/o puertos tcp y udp, impidiendo el ingreso de las demás solicitudes.

- **DMZ > VPN**
  Comunicación del segmento de red de los servidores con el segmento de red del equipo de soporte de GRUPO NETHEXA S.A.S.

  - Aceptar el tráfico del protocolo ICMP desde la red de los servidores, para realizar las validaciones correspondientes de conectividad desde la red de nethexa.
  - Aceptar el tráfico de UDP del puerto 161 para el registro del servidor de monitoreo.
  - Aceptar todos los puertos y servicios disponibles para el registro de los servicios de escaneo de vulnerabilidades y correlación de eventos.
  - Aceptar el puerto TCP 9911 desde el segmento de servidores, que permita la conexión de acceso SSH los equipos de la red de soporte de nethexa.
  - Aceptar el puerto TCP 3306 para la comunicación y establecimiento de comunicación de bases de datos alojadas en el segmento de equipos de soporte de nethexa.
  - Aceptar el tráfico UDP de los servicios SIP [5060-5063] y RTP [10000-20000] para el registro de las extensiones en el PBX y

el establecimiento del tráfico de las llamadas, para realizar pruebas de telefonía.
    - Aceptar el puerto de administración HTTPS [3344] del firewall desde la red de GRUPO NETHEXA S.A.S, para su administración.
    - Bloquear desde cualquier origen a cualquier destino todos los servicios y/o puertos tcp y udp, impidiendo el ingreso de las demás solicitudes.

- **DMZ > VPN SSL**
  Comunicación del segmento de red de los servidores con el segmento de red del cliente VPN de GRUPO NETHEXA S.A.S, para el soporte de los servidores desde redes públicas.

    - Aceptar el tráfico del protocolo ICMP desde la red de los servidores, para realizar las validaciones correspondientes de conectividad desde la red de nethexa.
    - Aceptar el puerto TCP 9911 desde el segmento de servidores, que permita la conexión de acceso SSH los equipos de la red de soporte de nethexa.
    - Aceptar el puerto TCP 3306 para la comunicación y establecimiento de comunicación de bases de datos alojadas en el segmento de equipos de soporte de nethexa.
    - Aceptar el tráfico UDP de los servicios SIP [5060-5063] y RTP [10000-20000] para el registro de las extensiones en el PBX y el establecimiento del tráfico de las llamadas, para realizar pruebas de telefonía.
    - Aceptar el puerto de administración HTTPS [3344] del firewall desde la red de GRUPO NETHEXA, para su administración.
    - Bloquear desde cualquier origen a cualquier destino todos los servicios y/o puertos tcp y udp, impidiendo el ingreso de las demás solicitudes.

- **LAN > WAN**
  Es el tráfico de navegación permitido hacia Internet de los usuarios, equipos de cómputo, teléfonos, etc. de la organización.

    - Aceptar el tráfico HTTP [80], HTTPS [443] y HTTPS segundario [8443] hacia Internet, para la búsqueda de y descarga de actualizaciones de los servidores.
    - Aceptar el acceso al puerto UDP 123 para la sincronización automática de la zona horaria de los servidores.
    - Aceptar el siguiente tráfico TCP de salida, para el envío de correos cifrados seguros de los servidores, los servicios son los

siguientes: TCP_TLS_SMTP [587], TCP_SSL_SMTP [465] y TCP_SSL_IMAP [993].
    - Aceptar el tráfico saliente TCP para el envío de correos de los servidores, los servicios son los siguientes: SMTP [25], POP3 [110] y IMAP [143].
    - Aceptar el servicio DNS [53] en los protocolos TCP y UDP, para la resolución de nombres en Internet.
    - Bloquear desde cualquier origen a cualquier destino todos los servicios y/o puertos tcp y udp, impidiendo el ingreso de las demás solicitudes.

- **LAN > DMZ**
  Es el tráfico permitido desde la red local de la organización del cliente hacia el segmento de servidores, para el establecimiento de la comunicación y operación de las plataformas de telefonía IP.

    - Aceptar el tráfico HTTP [80], HTTPS [443] y HTTPS segundario [8443] hacia el segmento de los servidores, para la navegación web de las aplicaciones de telefonía IP.
    - Aceptar el tráfico UDP de los servicios SIP [5060-5063] y RTP [10000-20000] para el registro de las extensiones en el PBX y el establecimiento del tráfico de las llamadas.
    - Bloquear desde cualquier origen a cualquier destino todos los servicios y/o puertos tcp y udp, impidiendo el ingreso de las demás solicitudes.

- **LAN > VPN**
  Comunicación de los segmentos de red locales del cliente hacia la red de soporte de GRUPO NETHEXA S.A.S.

    - Aceptar el tráfico del protocolo ICMP desde la red de los servidores, para realizar las validaciones correspondientes de conectividad desde la red de nethexa.
    - Aceptar el puerto de administración HTTP [80] y HTTPS [443] para la administración de los teléfonos IP.
    - Aceptar el puerto TCP de control remoto [3389] para el ingreso a los equipos de cómputo, con el propósito de brindar soporte a sophones y revisión de acceso a las plataformas web de la telefonía IP.
    - Bloquear desde cualquier origen a cualquier destino todos los servicios y/o puertos tcp y udp, impidiendo el ingreso de las demás solicitudes.

- **LAN > VPN SSL**

Comunicación de los segmentos de red locales del cliente hacia la red de VPN cliente de soporte de GRUPO NETHEXA S.A.S, para el soporte desde redes públicas.

- Aceptar el tráfico del protocolo ICMP desde la red de los servidores, para realizar las validaciones correspondientes de conectividad desde la red de nethexa.
- Aceptar el puerto de administración HTTP [80] y HTTPS [443] para la administración de los teléfonos IP.
- Aceptar el puerto TCP de control remoto [3389] para el ingreso a los equipos de cómputo, con el propósito de brindar soporte a sophones y revisión de acceso a las plataformas web de la telefonía IP.
- Bloquear desde cualquier origen a cualquier destino todos los servicios y/o puertos tcp y udp, impidiendo el ingreso de las demás solicitudes.

- **VPN > DMZ**
  Comunicación del segmento de red de soporte de GRUPO NETHEXA S.A.S con el segmento de red de los servidores.

  - Aceptar el tráfico del protocolo ICMP desde la red de soporte de GRUPO NETHEXA S.A.S, para realizar las validaciones correspondientes de conectividad desde la red de nethexa.
  - Aceptar el tráfico de UDP del puerto 161 para el registro del servidor de monitoreo.
  - Aceptar todos los puertos y servicios disponibles para el registro de los servicios de escaneo de vulnerabilidades y correlación de eventos.
  - Aceptar el puerto TCP 9911 desde la red de soporte de GRUPO NETHEXA S.A.S, que permita la conexión de acceso SSH los servidores.
  - Aceptar el puerto TCP 3306 para la comunicación y establecimiento de comunicación de bases de datos alojadas en el segmento de servidores.
  - Aceptar el tráfico UDP de los servicios SIP [5060-5063] y RTP [10000-20000] para el registro de las extensiones en el PBX y el establecimiento del tráfico de las llamadas, para realizar pruebas de telefonía.
  - Aceptar el puerto de administración HTTPS [3344] del firewall desde la red de GRUPO NETHEXA S.A.S, para su administración.
  - Bloquear desde cualquier origen a cualquier destino todos los servicios y/o puertos tcp y udp, impidiendo el ingreso de las demás solicitudes.

- **VPN > LAN**
  Comunicación de los segmentos de red del equipo de soporte de GRUPO NETHEXA S.A.S con las redes locales del cliente.

    - Aceptar el tráfico del protocolo ICMP desde la red de soporte de GRUPO NETHEXA S.A.S, para realizar las validaciones correspondientes de conectividad desde la red de Nethexa.
    - Aceptar el puerto de administración HTTP [80] y HTTPS [443] para la administración de los teléfonos IP.
    - Aceptar el puerto TCP de control remoto [3389] para el ingreso a los equipos de cómputo, con el propósito de brindar soporte y revisión de acceso a las plataformas web de la telefonía IP.
    - Bloquear desde cualquier origen a cualquier destino todos los servicios y/o puertos tcp y udp, impidiendo el ingreso de las demás solicitudes.

- **VPN SSL > DMZ**
  Comunicación del segmento de red del cliente VPN de GRUPO NETHEXA S.A.S con el segmento de red de los servidores.

    - Aceptar el tráfico del protocolo ICMP desde la red del cliente VPN de GRUPO NETHEXA S.A.S, para realizar las validaciones correspondientes de conectividad desde la red de Nethexa.
    - Aceptar el puerto TCP 9911 desde el cliente VPN de Grupo Nethexa, que permita la conexión de acceso SSH a los equipos de la red de soporte de Nethexa.
    - Aceptar el puerto TCP 3306 para la comunicación y establecimiento de comunicación de bases de datos alojadas desde la red cliente VPN de GRUPO NETHEXA S.A.S.
    - Aceptar el tráfico UDP de los servicios SIP [5060-5063] y RTP [10000-20000] para el registro de las extensiones en el PBX y el establecimiento del tráfico de las llamadas, para realizar pruebas de telefonía.
    - Aceptar el puerto de administración HTTPS [3344] del firewall desde la red de GRUPO NETHEXA S.A.S, para su administración.
    - Bloquear desde cualquier origen a cualquier destino todos los servicios y/o puertos tcp y udp, impidiendo el ingreso de las demás solicitudes.

- **VPN SSL > LAN**
  Comunicación de los segmentos de la red de VPN cliente de soporte de GRUPO NETHEXA S.A.S hacia las redes locales del cliente, para el soporte desde redes públicas.

    - Aceptar el tráfico del protocolo ICMP desde la red VPN cliente de soporte de GRUPO NETHEXA S.A.S, para realizar las validaciones correspondientes de conectividad desde la red de Nethexa.
    - Aceptar el puerto de administración HTTP [80] y HTTPS [443] para la administración de los teléfonos IP.
    - Aceptar el puerto TCP de control remoto [3389] para el ingreso a los equipos de cómputo, con el propósito de brindar soporte y revisión de acceso a las plataformas web de la telefonía IP.
    - Bloquear desde cualquier origen a cualquier destino todos los servicios y/o puertos tcp y udp, impidiendo el ingreso de las demás solicitudes.

4. NAT

Es la traducción de direcciones IP, el cual es utilizado como control de seguridad en la publicación de servicios web hacia Internet. La publicación de los servicios se realiza en asignar una dirección IP del pool público otorgado por el proveedor de servicios al firewall y es traducido a la dirección privada y puerto del servicio HTTPS; con el fin de, que las redes de Internet no puedan acceder directamente al dispositivo que proporciona la página web y poder hacer un análisis de las peticiones realizadas por el firewall.

5. Control de aplicaciones

Nos permite tener un control de las aplicaciones que pueden ser utilizadas en las zonas del firewall, permitiendo y denegando el acceso a las aplicaciones establecidas por las políticas de la organización. Para la solución de e-learning y telefonía IP, los servidores solo pueden tener permitido la descarga de contenidos .deb, .sql, tar.gz, .gz, .zip, etc. Que sean validados para la actualización e instalación de nuevos contenidos e aplicaciones en los servidores Linux de la empresa.

Las reglas del control de contenido para las redes locales del cliente, son establecidas por el propio cliente donde se anexan las aplicaciones que son permitidas a los equipos de cómputo, celulares, Tablet, etc.

6. Calidad de servicio

La calidad de servicio es importante para la estabilidad y mejora de la latencia de los servicios por causa de los canales de Internet o el uso de tráfico de otras aplicaciones de alto consumo de tráfico en la red. Para la solución de e-learning y telefonía IP, damos una prioridad en las reglas que se crearon para el acceso a los servicios web y el tráfico UDP de la telefonía IP con una prioridad alta, la cual permite contestar las solicitudes de red del firewall en tiempo real, minimizando la latencia que pueda ocurrir por saturación de los canales de Internet y de la red local.

7. Bloqueo de países

Este control es importante para la seguridad de la red de los servidores y de las organizaciones, ya que el bloqueo de los países a los que no vamos a tener algún tipo de conexión le podemos bloquear el acceso a los activos de información; con el objetivo, de reducir los riesgos de ataques informáticos de países potenciales en seguridad informática y que posiblemente pueden realizar ataques informáticos que afecten el funcionamiento de los activos de información de la organización.

La política de la organización es bloquear todos los países y permitir el ingreso a los pocos países que utilizan los servicios web prestados a través de Internet.

8. Conexión segura VPN IPSec.

IPSec es el protocolo de seguridad sobre Internet, el cual es el encargado de asegurar las comunicaciones sobre la red de Internet, autenticando y cifrando los paquetes que son establecidos por un transmisor y un receptor.

IPSec es utilizado para crear túneles seguros cifrados entre las organizaciones, permitiendo la comunicación de las redes Internas con sitios remotos, agregando seguridad en el flujo de datos que son transmitidos entre dos sedes. Por este motivo, la VPN cifrada es importante en la seguridad perimetral que comunica los activos de información con sitios remotos, los cuales poseen la administración y la conexión de los demás servicios en red para la operatividad de las plataformas web de la organización.

La VPN posee dos Fases de seguridad, las cuales deben de coincidir perfectamente, ya que se configuran los parámetros de red que deben de ser cumplidos en toda VPN establecida por la organización; con el objetivo de, impedir que un ataque en el medio pueda extraer la información y descifrar en el menor tiempo posible.

Fase	Propiedades del Tunnel	Local	Remoto
Fase 1	Peer	IP Pública Local	IP Publica Remota
	Encryption Domain	Red Local	Red Remota
	VPN Device Description	Site to Site	Site to Site
	Authentication Method	Preshare-key	Preshare-key
	Diffie-Hellman Group	2	2
	Encryption Algorithm	AES128	AES128
	Hashing Algorithm	SHA1	SHA1
	Main or Aggressive Mode	Main	Main
	Lifetime	86400	86400
	Diffie-Hellman Group	modp1024	modp1024
Fase 2	Encapsulation (ESP or AH)	ESP	ESP
	Encryption Algorithm	AES128	AES128
	Hashing Algorithm	SHA1	SHA1
	Lifetime	86400	86400

El cifrado utilizado es el adecuado, ya que es el cifrado más liviano y seguro que se puede utilizar para la seguridad de las comunicaciones de red, permitiendo una seguridad de los datos transmitidos y recibidos por más de un billón de años y los equipos de seguridad perimetral pueden bajar el

procesamiento del tráfico cifrado al no colocar un cifrado más alto a estos dispositivos, debido a que no es necesario.
Nota: Por ningún motivo se utilizan VPN's con cifrados que no son suficiente fuertes que puedan comprometer la seguridad de los datos transportados, no se pueden utilizar protocolos como PPTP y L2TP que no contengan cifrado SSL.

9. Conexión segura VPN SSL

Es una VPN particular, la cual permite establecer conexiones seguras sobre redes públicas que proporcionen Internet; con el objetivo de poder acceder a los servidores de manera segura por parte del personal de Nethexa, el cual es el encargado de acceder a los activos de información en un tiempo de disponibilidad por fuera del horario laboral, el cual permite acceder los computadores de la organización directamente a la administración de las plataformas web.

La ventaja principal de la VPN es la portabilidad de esta a todo lugar, desde que tenga la aplicación y los accesos a esta, la cual puede soportar los diferentes sistemas operativos.

10. Protección de ataques de DoS y DDoS

Los equipos perimetrales poseen un servicio de seguridad básico que permite la identificación y erradicación de los ataques de denegación de servicios a nuestros equipos y también a los sistemas perimetrales.

Todos los servidores, equipos de comunicación y equipos perimetrales, deben de tener habilitado la identificación y erradicación de los ataques de nivel de servicios.

11. Cifrado de tráfico de red DPI-SSL

Inspección profunda de paquetes que ingresan y salen de la red de datos de la organización, el cual contiene los servicios de Antivirus, Antispyware e IPS sobre HTTPS, permitiendo identificar, analizar y restringir el tráfico denegado o que comprometa la seguridad de los activos de información que se están protegiendo en la red de datos.

Los activos de información deben de estar siempre protegidos por los servicios de DPI-SSL con el objetivo de detectar y denegar ataques informáticos como ataques informáticos dirigidos y malware que pueda afectar los las plataformas web de la organización.

ANEXO 27

PROTECCIÓN CONTRA MALWARE Y ATAQUES DIRIGIDOS

Con el crecimiento de las TIC en el mundo, también se está reflejando los problemas de ciberseguridad en los activos de información que poseen las diferentes organizaciones, GRUPO NETHEXA S.A.S no se puede quedar atrás en la seguridad de los activos de información que proporcionan la seguridad de las plataformas web.

La protección contra código malicioso es vital para los activos de información, ya que se deben de mitigar todos los ataques de malware que lleguen a las plataformas web, mitigando o reduciendo el riesgo identificado en el análisis de riesgo.

Los riesgos que se deben de tratar en los controles de protección contra malware son:

- Malware
- Interceptación de información
- DOS/DDOS
- Pérdida de control de acceso
- Configuraciones de seguridad incorrectas
- Registro y monitoreo insuficiente
- Phishing
- SQL Injection
- Buffer Overflow
- Ataques de día cero
- Cross-site Scripting
- Ataques de fuerza bruta
- Man in the Middle
- CSRF
- Entidades XML (XXE)

La finalidad de este documento, es poder informar de la necesidad de los controles descritos en esta sección que tiene como objetivo fundamental, reducir el riesgo informático de los activos de información que puede ser causados por las amenazas descritas anteriormente. Los siguientes controles permiten implementar una seguridad más organizada, jerárquica y eficaz al momento de sufrir un incidente de seguridad.

1. **IPS/IDS, Gateway Antivirus y Antispyware**

   Son los controles de seguridad en red que permiten la detección y prevención de intrusos en red, el cual puede ofrecer un motor de inspección de paquetes

profundo y de alto rendimiento, en la protección de servicios claves para la organización como los son las aplicaciones web, correo electrónico, transferencia de archivos desde los servidores, servicios Linux y DNS. La protección del control es creada para proteger los activos de información vulnerabilidades de las aplicaciones y malware que permita dañar o robar información confidencial de los servicios web de la organización.

La empresa necesita un control licenciado que contenga los servicios de seguridad, que permitan ser actualizados constantemente con las firmas o parámetros que permiten detectar y prevenir automáticamente los ataques informáticos que son conocidos por todos los fabricantes de seguridad, permitiendo detener y mitigar todos los ataques de red informáticos que pueden ser utilizados hacia los activos de información.

El firewall perimetral debe contener estos controles, permitiendo investigar a fondo los protocolos que están ingresando a los servidores de las plataformas web, examinado la información de la capa de aplicación, defendiéndose contra ataques dirigidos a las vulnerabilidades que puede poseer las aplicaciones web.

Los controles permiten:

- Contener un motor de antivirus en tiempo real, teniendo la capacidad de rastrear en la red virus, gusanos, troyanos y las demás amenazas en Internet identificadas en las firmas.
- Bloquear la instalación de spyware malicioso e interrumpir las comunicaciones establecidas por el spyware.
- Protección contra una gran variedad de amenazas que pueden ser realizadas sobre la red, como gusanos, troyanos u otro código que sea malicioso.
- Inteligencia y control de aplicaciones sobre el firewall del dispositivo de seguridad perimetral, proporcionando la información necesaria para el refuerzo de aplicaciones y políticas.
- Base de datos de firmas y comportamientos anormales de manera automática, proporcionando protección contra las amenazas.

El IPS/IDS analiza todo el tráfico entrante y saliente en todas las zonas establecidas por el firewall, analizando el siguiente tráfico y detectando las amenazas en la red que se encuentren en todas las categorías de firmas de la base de datos.

El Gateway antivirus, inspecciona y vigila todos los protocolos HTTP, FTP, IMAP, SMTP, POP3, CIFS/Netbios y TCP Stream, verificando todo el tráfico entrante y saliente de las diferentes zonas del firewall, impidiendo el acceso

a los virus que se infiltran en la red que contengan los protocolos anteriores, cotejando la información que posee en las firmas bloqueando el contenido e informando a los administradores de seguridad de la organización.

El Antispyware se encarga de analizar el tráfico de red entrante y saliente de las diferentes zonas del firewall, detectando y previniendo los spyware que ingresan a la red a través de los protocolos HTTP, FTP, IMAP, SMTP y POP3. Permitiendo dar seguridad a los usuarios y a los servidores en la red.

2. Sandboxing

Sistema de protección contra amenazas avanzadas con soluciones de multimotor en la nube, control que tiene la capacidad de detener ataques de día cero, ransomware y ataques persistentes avanzados, analizando los paquetes que ingresan a la red en tiempo real permitiendo detectar y bloquear el malware que no se encuentra en las firmas creadas por los diferentes fabricantes, previniendo los diferentes ataques de malware que no muestran un comportamiento malicioso u oculta el código malicioso mediante cifrado, dirigido a las activos de información de las aplicaciones web.
La empresa adquiere estos controles en el firewall de seguridad perimetral, que fortalezca la seguridad en la red, impidiendo el ingreso de ataques de ciberseguridad potenciales a las plataformas web de la organización, reduciendo los riesgos y el impacto generado por un incidente de seguridad.

3. Filtro de contenido

Es un control esencial para la organización, cuyo objetivo es impedir la navegación indebida en los servidores de las plataformas web, reduciendo los problemas de seguridad reforzando las políticas del uso del Internet y bloqueo del contenido dañino, el cual puede causar infecciones y ataques informáticos.

El filtro de contenido implementado deniega toda la navegación de las plataformas web de la organización, permitiendo solo el tráfico de la prestación del servicio y el tráfico de navegación de las páginas autorizadas que debían ser realizar este tipo de actualizaciones e implementaciones.

Además, la organización controla todo el tráfico HTTPS que pasa por el firewall de la organización e impedir la descarga de archivos que pueden ser perjudiciales para la estabilidad de las plataformas de aplicaciones web.

Para todo servidor, es necesario bloquear toda la navegación web y solo se deben abrir las páginas necesarias para la descarga y actualización de los

servicios y aplicaciones de las plataformas web, bloqueando todas las categorías que posee el firewall.

4. EndPoint

Para los servidores Linux, es poco usado las aplicaciones cliente de antivirus y EndPoint, ya que al ser una plataforma que se puede asegurar con los mismos recursos Open Source en servicios y aplicaciones que son fundamentales para la seguridad de las plataformas web, los fabricantes no desarrollan mucho en estas áreas.

La seguridad en las plataformas es vital para la disponibilidad y seguridad de los servicios web de la organización, pero no podemos olvidar el eslabón más débil en la cadena de la seguridad los cuales son los diferentes usuarios que utilizan las plataformas web en las diferentes organizaciones, por lo que es de suma importancia tener un control como el EndPoint que nos permite tener una protección avanzada contra malware con interfaces unificadas que poseen motores contra código malicioso de nueva generación.

La organización tiene que buscar y seleccionar un EndPoint que permita conectarse con la solución de seguridad perimetral, la cual pueda unificarse con los reportes de amenazas y vulnerabilidades que fueron afectadas en toda la compañía, permitiendo una seguridad que sea centralizada y que pueda brindar seguridad dentro y fuera de la empresa. Por este motivo se selecciona como un control de seguridad fundamental para los usuarios que utilizan las plataformas web de la organización, permitiendo tener una información adecuada de la herramienta como lo son:

- Visualizar reportes de seguridad.
- Visualización del ataque informático.
- Antivirus de nueva generación basado en comportamiento, bajando el consumo de los recursos de los equipos de cómputo de los usuarios.
- Integración con Sandbox de seguridad perimetral.
- Hacer cumplir las políticas de seguridad de la empresa dentro y fuera de la red corporativa.
- Atender los incidentes de seguridad y remediarlos lo más pronto posible.
- Detectar las amenazas provenientes de canales cifrados.
- Detener ataques persistentes Avanzados y Ransomware.
- Detección de malware sin tener archivos asociados.

Finalmente, poder tener una seguridad centralizada de los usuarios que permitan tener un panorama general de las amenazas que sufren todos lo usuarios, permitiendo mitigar los ataques dirigidos a los activos de

información y forzar las políticas creadas por la organización a todos los usuarios de la compañía.

5. WAF

Para la protección oportuna especializada en servicios web de seguridad es necesario implementar un Firewall de aplicaciones web, permitiendo analizar todo el tráfico en la capa de aplicación proporcionando seguridad en tiempo real de ataques entrantes dirigidos a las plataformas web de la organización.

El WAF es un software que es instalado en la nube a través de máquinas establecidas en las plataformas Cloud y en la infraestructura interna de la organización se puede manejar como una máquina virtual que se puede instalar en un virtualizador. WAF brinda seguridad en la fuga de información, balanceo de cargas, ataques de DDoS en las plataformas HTTPS, prevención contra ataques y exploit a través de comportamientos lógicos anómalos, manejo del cifrado HTTPS y protección contra los principales ataques del Top 10 del proyecto de seguridad de OWASP.

El firewall de aplicación también puede ser implementado de las siguientes maneras, dependiendo del escenario y de la seguridad que se vaya a brindar a los servidores web:

- Implementación como proxy reverso por defecto, recibiendo el tráfico de una sola interfaz.
- Implementación de disposición, donde es encargado de filtrar el tráfico web detrás de un firewall.
- Implementación en clúster, en implementación de múltiples WAF.
- Implementación de inspección SSL, donde inspecciona todo el tráfico cifrado de las aplicaciones web.

WAF es esencial para la administración de la seguridad WEB de las plataformas de la organización en e-learning y Telefonía IP, ya que se acomoda a los dos escenarios sin ningún inconveniente, ya que el software del firewall de aplicación se adquiere directamente en la nube y se puede instalar sobre un sistema de virtualización. Además; es un servicio de seguridad especializado que puede proteger los ataques directos a las vulnerabilidades y las amenazas descubiertas por el análisis de riesgos en la empresa.

6. Correlación de eventos

En la conformación de la seguridad informática de las plataformas web de e-learning y telefonía IP, se evidencia la necesidad de tener un software que permite analizar todos los eventos de seguridad que pueden ser tomadas a través de diversas aplicaciones que se encuentran en sobre la red, prestando los servicios web de la organización.

La finalidad de la correlación de eventos es poder analizar los datos e identificar las relaciones entre ellos, correlacionado todos los eventos de seguridad y adelantándose a los incidentes de seguridad que se puedan presentar en la empresa, reduciendo el impacto de las amenazas al tener una correlación y monitoreo de las aplicaciones que conforman las plataformas web, determinando las causas del problema y resolverlo rápidamente minimizando el impacto y pérdida del negocio.

La correlación de eventos permite evidenciar los eventos antes de que lleguen, a través de un syslog de los sistemas de información, centralizando toda la información y correlacionando entre sí para encontrar eventos de seguridad que pueden ser mitigados por el área de seguridad, realizando las siguientes actividades en el control:

- Inteligencia de datos.
- Apoyo a las operaciones.
- Análisis de causa raíz del problema.
- Detección de fraude.

La correlación de eventos posee unos grandes beneficios para la organización, con el objetivo de poder tomar decisiones sobre qué hacer con la seguridad de las aplicaciones web, investigando y respondiendo todas las alertas de seguridad detectadas en la herramienta. Algunos beneficios son los siguientes:

- Visibilidad de amenazas en tiempo real.
- Vigilancia de seguridad en la red de datos.
- Informes de cumplimiento.
- Reducción de costos operativos.
- Mejora de la gestión del tiempo en la organización.

7. Bibliografía

SonicWall (2018).Recursos de soporte de seguridad. Recuperado: https://www.sonicwall.com/en-us/support, 8 de noviembre de 2018.

Innova Secure (2017). Qué es la correlación de eventos. Recuperado:

https://innovasecure.com/que-es-la-correlacion-de-eventos/, 8 de noviembre de 2018.

ANEXO 28

ANTEPROYECTO

Maestría en Tecnologías de la Información y la Comunicación

Formulación del Proyecto de Grado

Sistema de Gestión Integral de Seguridad Informática en servicios WEB de e-learning y Telefonía IP en Grupo Nethexa S.A.S

Participantes

Datos del Estudiante			
Nombre	Sebastián Restrepo Marín		
Correo electrónico	Sebastianrpo1991@gmail.com		
ID Usuario (cédula)	1035390130	ID UPB	000359573

Datos del Director	
Nombre	John Fernando Vargas Buitrago
Correo electrónico	Johnfdo.vargas@upb.edu.co
ID Usuario (cédula)	000022763
Facultad/Institución/Empresa	Facultad de Ingeniería en TIC - UPB

Datos Asesor Metodológico	
Nombre	Juan Camilo Estrada
Correo electrónico	jcestrada@nethexa.com
Profesión	Ingeniero Informático
Facultad/Institución/Empresa	Grupo Nethexa S.A.S

Datos Asesor Técnico	
Nombre	Julián Gutierrez
Correo electrónico	jgutierrez@nethexa.com
Profesión	Ingeniero en Telecomunicaciones
Facultad/Institución/Empresa	Grupo Nethexa S.A.S

Universidad Pontificia Bolivariana

Escuela de Ingenierías
Facultad de Ingeniería en Tecnologías de la Información y la Comunicación
Medellín, 2017-12-01

1 Título

Sistema de Gestión Integral de Seguridad Informática en servicios WEB de e-learning y Telefonía IP en Grupo Nethexa S.A.S

2 Resumen

2.1 Español

El proyecto consiste en implantar un sistema de gestión integral de seguridad informática, que permita analizar y mitigar las vulnerabilidades críticas que poseen los servicios WEB de e-learning y telefonía IP transversalmente en Grupo Nethexa S.A.S. Creando actividades interrelacionadas a través de acciones específicas, que permitan definir e implementar lineamientos de seguridad informática, adaptando estándares que permitan aumentar la seguridad, disponibilidad y la continuidad de los servicios WEB en la organización. Se propone en el trabajo de maestría se realice un sistema de gestión integral que apoye la detección de vulnerabilidades existentes en los servicios WEB de la organización que afecten la confiabilidad, integridad y autenticidad de la información en los servidores que contienen las aplicaciones WEB. Con el fin de informar y corregir las vulnerabilidades críticas, protegiendo los datos de información que circulan en la red desde las plataformas WEB, ayudando a aumentar el manejo seguro en la prestación del servicio, disminuyendo el hurto de información e identidad, divulgación de información sensible, escalamiento de privilegios, entre otros datos que afecte la continuidad de los servicios de las empresas que lo utilizan.

2.2 Inglés

The project consists of implementing a comprehensive information security management system that allows analyzing and mitigating the critical vulnerabilities that the e-learning and IP telephony WEB services have transversally in Grupo Nethexa S.A.S. Creating interrelated activities through specific actions that allow the definition and implementation of computer security guidelines, adapting standards that increase the security, availability and continuity of WEB services in the organization. It is proposed in the master's work to carry out an integral management system that supports the detection of existing vulnerabilities in the WEB services of the organization that affect the reliability, integrity and authenticity of the information in the servers that contain the WEB applications. In order to inform and correct critical vulnerabilities, protecting the information data circulating in the network from the WEB platforms, helping to increase the safe handling in the provision of the service, reducing the theft of information and identity, disclosure of sensitive information, escalation of privileges, among other data that affects the continuity of the services of the companies that use it.

3 Palabras clave

3.1 Español
SSL/TLS, HTTP, HSTS, Educación Virtual, VoIP.

3.2 Inglés
SSL/TLS, HTTP, HSTS, e-learning, VoIP.

4 Tema

El proyecto consiste en implementar un sistema de gestión integral que permita establecer procesos de análisis de seguridad informática, con el fin de evaluar y mitigar las vulnerabilidades existentes que poseen los servicios WEB que contienen las aplicaciones internas de educación virtual y de soluciones de VoIP en Grupo Nethexa S.A.S. Contribuyendo con la mejora continua de los servicios y desarrollos propietarios de la organización en el ámbito de seguridad informática.

La relación del contenido de investigación del proyecto y/o trabajo de grado con el programa de formación de la maestría en tecnologías de la información y la comunicación, es la orientación a la aplicación del conocimiento adquirido en la línea de formación de seguridad informática definida por el estudiante como objeto de formación, realizando un reto empresarial que ayudará a ampliar los conocimientos adquiridos en la institución en un ambiente organizacional, que permita mejorar los procesos de seguridad informática en la línea de investigación en la empresa Grupo Nethexa S.A.S.

5 Problema

El uso de los sistemas de información crea la necesidad y la dependencia de la utilización de los medios informáticos de navegación HTTP para realizar la mayoría de los trámites en la red, reduciendo tiempo y dinero al gestionar la mayoría los deberes desde cualquier sitio con acceso a Internet. Por ende, es importante proteger los datos críticos de los usuarios que en su mayoría es tráfico HTTP; por este motivo el tráfico es asegurado bajo los protocolos de seguridad SSL/TLS, que brindan confiabilidad, integridad y autenticidad (Rodríguez,2013). Los protocolos SSL/TLS han presentado grandes vulnerabilidades en la red de datos, proporcionando una brecha de seguridad para plataformas de navegación HTTP y de transferencia de archivos en la red. Un gran número de vulnerabilidades han sido descubiertas en los protocolos SSL/TLS.

Para reducir los problemas de los protocolos de seguridad SSL/TLS, se desarrolló el mecanismo de seguridad llamado HSTS que obliga a que las peticiones realizadas desde un navegador WEB sean forzadas, para la utilización de los protocolos SSL/TLS navegando de manera segura con HTTPS, pero este mecanismo HSTS es inseguro, ya que existen ataques informáticos que aprovechan

vulnerabilidades en los navegadores y de los aplicativos HTTP, burlando el mecanismo de seguridad, realizando ataques de MITM afectando la integridad de los datos.

Grupo Nethexa S.A.S tiene presente todos los problemas de seguridad que poseen los protocolos HTTP, SSL/TLS y el mecanismo de seguridad HSTS, que afectan la integridad de los servicios de e-learning y Telefonía IP publicados en Internet, los cuales contienen servicios WEB que son fundamentales para la continuidad del negocio de la compañía. Además; los servidores WEB de la organización son vulnerables porque poseen problemas de seguridad en los protocolos de los servicios que manejan y no se tiene un modelo de gestión de seguridad informática, que permita evaluar e implementar controles de seguridad constantemente con los nuevos ciberataques que aparecen con el tiempo al descubrir nuevas vulnerabilidades en las aplicaciones WEB, careciendo de seguridad informática para el debido funcionamiento de todos los servicios HTTP ofrecidos a los clientes. Se necesita reducir los problemas de seguridad que se tienen en el hurto de información, escalamiento de privilegios, suplantación de identidad, afectación de la disponibilidad del servicio WEB, etc. Afectando finalmente a la empresa con la degradación de la imagen corporativa a nivel tecnológico en la prestación de servicios informáticos.

La organización requiere implantar controles en seguridad informática que ayude a mitigar los problemas de seguridad de las plataformas WEB de e-learning y Telefonía IP, que tenga la posibilidad de adaptarse a un sistema de gestión integral que facilite la evaluación de las vulnerabilidades de todas los servicios HTTP que posee la organización transversalmente, con el fin de reducir los ataques informáticos WEB existentes que afectan la confiabilidad, integridad, autenticidad y continuidad de los servicios. En el trabajo de grado de maestría, se investigará la manera de implantar un sistema de gestión integral de seguridad informática para los servicios WEB de e-learning y Telefonía IP en Grupo Nethexa S.A.S; mediante la adaptación de metodologías de seguridad informática, análisis de vulnerabilidades de seguridad WEB, integración de técnicas de escaneo y ataques informáticos HTTP, que faciliten la identificación y mitigación de los problemas de seguridad existentes que presentan las aplicaciones HTTP que operan en la empresa.

6 Justificación

En el entorno actual de las tecnologías de la información, se encuentra que cada día se depende de los sistemas informáticos, que son accedidos desde hogares y organizaciones por medio de la red de Internet, generando el crecimiento de aplicaciones, plataformas y entretenimiento de manera remota. Creando la necesidad de proteger los datos de personas con altos conocimientos informáticos, los cuales buscan beneficiarse económicamente extrayendo información sensible

que afecte la confiabilidad, integridad, autenticidad y disponibilidad de los servicios de navegación WEB de los usuarios.

La idea del Sistema de gestión integral de seguridad informática en servicios WEB en Grupo Nethexa S.A.S; es identificar las vulnerabilidades y los problemas de seguridad proporcionados por las malas prácticas en controles de seguridad y los problemas que contienen los protocolos y/o mecanismos de seguridad en aplicaciones HTTP, que pueden ser aprovechadas exitosamente por técnicas de ataques informáticos, permitiendo quebrantar el nivel de seguridad de los sitios de navegación WEB. Así, adaptar controles de seguridad que permitan mitigar los riesgos de seguridad identificados, que exponen la integridad de la información de la navegación en servidores WEB.

Finalmente, poder informar a la empresa de los problemas de seguridad encontrados y de los controles que deben ser implementados en las aplicaciones HTTP analizadas en el trabajo de grado, contribuyendo con la mejora continua en la protección de los sistemas de información en la navegación WEB de los usuarios que utilizan los servidores de la organización. Con el fin de reducir los ataques informáticos que proporciona la navegación WEB; y así, mejorar la disponibilidad de los servicios WEB, disminuyendo el hurto de información crítica y suplantación de identidad, previniendo anticipadamente el escalamiento de privilegios y la degradación de imagen corporativa, etc.

7 Marco referencial

7.1 Marco contextual

El trabajo de grado de maestría busca solucionar los problemas de seguridad que presenta la empresa Grupo Nethexa S.A.S. Gutiérrez (2017), La organización es líder en la operación y prestación de servicios de telecomunicaciones, contando con la capacidad técnica de atender requerimientos informáticos en el área de Telefonía IP, e-learning, redes de datos, seguridad perimetral, consultoría y optimización de infraestructura.

La empresa se enfoca en la prestación de servicios de comunicación IP e infraestructura, que parten desde el análisis, diseño, implementación, optimización y operación de soluciones innovadoras que buscan optimizar los recursos aportando valor agregado a los clientes. Brindando soluciones personalizadas que aportan al Core del negocio de cada uno de los clientes, gracias a la permanente innovación de servicios, ya que se poseen desarrollos de productos propietarios y se realiza seguimiento de estratégico de los objetivos de los clientes.

Los servicios ofrecidos son los siguientes:

- Educación virtual y contenidos
- Señalización digital y distribución de audio
- Servidores, Servicios en la nube y Virtualización
- Soluciones IaaS para retail
- Soluciones VoIP – IP PBX Básico
- Soluciones VoIP Para Call Center
- Soluciones Inalámbricas

El trabajo consiste en implementar un sistema de gestión integral de seguridad informática en los servicios WEB de e-learning y Telefonía IP en la empresa Grupo Nethexa S.A.S; que permita auditar la seguridad WEB transversalmente en las aplicaciones HTTP de la organización. Adaptando metodologías de gestión ágiles que permitan establecer políticas y procesos de seguridad que ayuden a identificar y mitigar los problemas de seguridad críticos en la organización, en un escenario de pruebas de los servicios internos de e-learning y Telefonía IP.

Se busca con el sistema de gestión integral que permita apalancar las políticas de seguridad informática establecidas en la organización, incorporando nuevos procesos que son necesarios en la auditoría constante, aportando en la evaluación y en la mejora continua de la seguridad del servicio WEB de las aplicaciones internas de educación virtual y soluciones de VoIP, con el fin de mejorar la disponibilidad de los diferentes servicios que son ofrecidos a los clientes de la organización.

Con el objetivo de Informar a los clientes y a la organización los reportes de las vulnerabilidades encontradas y de los controles establecidos aplicados en los servicios, permitiendo resolver los problemas de seguridad identificados, con el propósito de contribuir con el cumplimiento de buenas prácticas de seguridad informática que son adaptadas por la empresa, ayudando a disminuir el impacto de ataques informáticos en las aplicaciones WEB.

7.2 Marco conceptual

Dado que el trabajo se centrará en evaluar y mitigar la existencia de vulnerabilidades detectadas en los servicios WEB de e-learning y Telefonía IP en Grupo Nethexa S.A.S, se suministra la información relevante de las áreas de investigación abarcadas. En la primera sección se presenta los fundamentos básicos de las aplicaciones WEB, la segunda se analiza los protocolos de seguridad SSL/TLS y HSTS y, por último, se describen los servicios de e-learning y Telefonía IP.

7.2.1 Aplicaciones HTTP

Es un conjunto de herramientas que contiene un servidor WEB, red, y navegador, los cuales son encargados de prestar un servicio de navegación a los usuarios cliente-servidor en la red desde la intranet e Internet. El protocolo HTTP es el protocolo que soporta toda la comunicación en la navegación en aplicaciones WEB, el cual fue diseñado para proporcionar robustez y tolerancia a fallas prestando un rendimiento confiable en la comunicación en la Word Wide WEB.

Berners-Lee, Fielding y Frystyk (1996), el protocolo de transferencia de hipertexto (HTTP) tiene sus inicios en el año 1996 y está plasmado en la RFC 1945, donde es publicada la versión HTTP/1.0 y es la base fundamental para el desarrollo del área de ingeniería de software, para la creación de aplicaciones ligeras accedidas por los navegadores WEB de los usuarios, sin importar los sistemas operativos que hacen las peticiones del servicio. El protocolo realiza una transferencia de datos básica a través de Internet permitiendo la trasferencia de mensajes en formato MIME, conteniendo la información de los mensajes transferidos y modificados en las peticiones y respuestas de los usuarios.

Fielding, Gettys, Mogul, Frystyk, Masinter, Leach y Berners-Lee (1999), en 1990 proponen un nuevo protocolo HTTP/1.1 en la RFC 2068 y es mejorada en el año 1999 por la RFC 2616. Esta versión incluye unas seria de mejoras del protocolo de comunicación anterior como: jerarquía de proxys, almacenamiento en cache, conexiones persistentes, anfitriones virtuales, etc. La mejora del protocolo se diferencia al anterior por contener requisitos estrictos en la comunicación, mejorando el servicio entre usuarios y servidores Proxy, uso de cookies y puertas de acceso a otros sistemas de Internet con los protocolos SMTP, NNTP, FTP, Gopher y WAIS.

Nielsen, Leach, y Lawrence (2000), en el año 2000 el protocolo es actualizado nuevamente a HTTP/1.2 y comunicado en la RFC 2774, donde se resuelven los problemas presentados en la versión anterior HTTP/1.1, donde no se puede cumplir con el dialogo y de la coordinación de las extensiones de las aplicaciones. Este protocolo realiza una extensión genérica para el funcionamiento de las aplicaciones en el protocolo HTTP.

Belshe, Peon, y Thomson (2015), finalmente, en el 2015 es actualizada la última versión del protocolo llamada HTTP/2.0 y que es informado en la RFC 7540, donde se describe una versión optimizada del protocolo HTTP, permitiendo mejor eficiencia en los recursos de red y reducción en la cabecera comprimiendo los datos, reduciendo la percepción de latencia de los usuarios en la utilización del protocolo en la navegación y permitiendo intercambios simultáneos en el uso de la conexión. El protocolo HTTP/2.0 se encarga de optimizar la semántica del protocolo de conexiones subyacentes, mejorando el comportamiento de las solicitudes en velocidad y rendimiento. También, el protocolo mejoro el rendimiento de los

recursos en procesamiento, a través del encuadre de mensaje binario mejorando la eficiencia de los mensajes transmitidos en la red.

Las aplicaciones WEB manejan diferentes lenguajes de programación como PHP, Java, JavaScript, Ruby, Python, etc. Que facilitan el desarrollo y la estructura de la página WEB en el servidor, estructurando toda la comunicación en la aplicación con bases de datos, diseño de la página y ejecución del desarrollo para el funcionamiento de todos los campos que posee la página WEB en la red, estas aplicaciones se encargan de procesar la información que visualiza el usuario en código HTML en el protocolo HTTP.

7.2.2 SSL/TLS

El protocolo SSL (Secure Sockets Layer) y su sucesor TLS (Transport Layer Security) son protocolos de seguridad criptográficos que trabajan sobre la capa de transporte, encargados de proporcionar comunicaciones seguras en toda la red de comunicaciones.

El protocolo HTTPS es esencial en una sesión HTTP, a través de una conexión segura SSL/TLS. Las sesiones se establecen usando una combinación de protocolos criptográficos de claves simétricas y asimétricas, el protocolo de clave asimétrica se utiliza inicialmente para las modulaciones de intercambio del protocolo de calve simétrica. Lugo, el protocolo de clave simétrica se utiliza para proteger el tráfico. Con el fin de prevenir ataques a las claves públicas, las claves públicas se entregan en un certificado X.509, que contiene varios campos adicionales que se utilizan para verificar que la clave pública es válida y pertenezca realmente al sitio (Benton, Jo y Kim, 2011).

(Rodríguez,2013), señalan que el protocolo de seguridad SSL/TLS brinda confiabilidad, integridad y autenticación en el uso de servicios en la red como la navegación WEB, correo electrónico, mensajería instantánea, voz sobre IP, etc.

Los protocolos SSL/TLS se encuentra ubicados en la capa de transporte, entre las capas de red y la capa de aplicación, encargado de transferir toda la información de manera segura a través de las capas de seguridad Handshake Y Record.

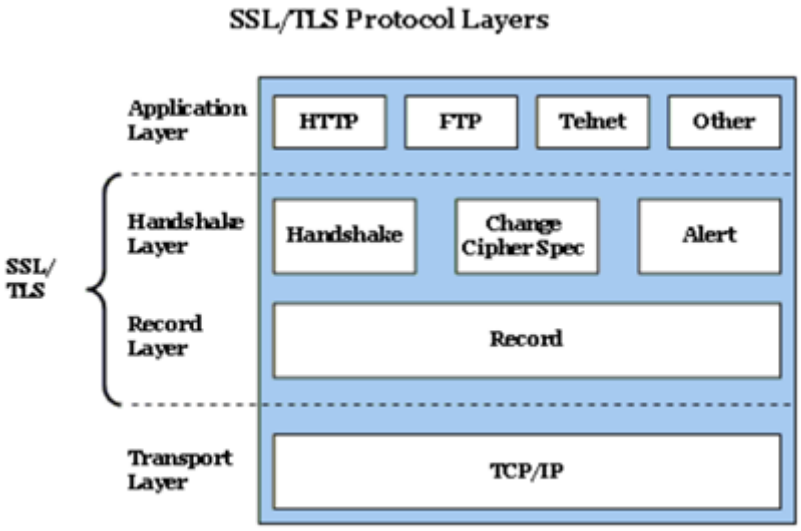


Figura 1. Capas del protocolo SSL/TLS. (Rodríguez,2013).

EL protocolo se encuentra dividido por dos capas:

- Handshake Layer

En la fase de negociación Handshake realiza la negociación de los algoritmos, luego realiza la autenticación de los servidores y genera el secreto compartido. El protocolo Alert gestiona las sesiones SSL, los mensajes de errores y todas las advertencias y Change Ciphersuite Protocol es usado para indicar que una parte va a cambiar en Ciphersuite se ha negociado recientemente. Un Ciphersuite es un nombre usado para la combinación de la autenticación, encriptación y Message Authentication Code (MAC) (Rodríguez,2013).

- Record Layer

Es utilizado para encapsular los protocolos de mejor nivel, proporcionando una comunicación más segura y tomar los mensajes que llegan a esta capa, codificando los algoritmos de encriptación de llave simétrica aplicando una AMC (Message Authentication Code) (Rodríguez,2013).

Wang, et al. (2015), los protocolos criptográficos SSL y TLS fueron diseñados para proporcionar seguridad en las comunicaciones en toda la red de datos, encriptando los datos en la capa de aplicación y en las demás capas subyacentes. SSL/TLS es un protocolo de registro, cuyo funcionamiento se establece a través de un apretón de manos, el cual encapsula los datos en la capa de aplicación; Luego el protocolo de registro completa una serie de funciones, las cuales incluyen paquetes de fragmentación y desfragmentación, comprensión y descomprensión, autenticación y cifrado, con el fin de asegurar los mensajes de manera confiable y persistente.

“El protocolo de registro SSL/TLS trabaja de tres maneras diferentes, dependiendo de los algoritmos de cifrado con los que es configurado.
…
1. Primero se calcula el HMAC y luego cifra todos los datos con el algoritmo CBC-Modo.
2. Primero se calcula el HMAC y luego usa el cifrado de flujo RC4 para cifrar todos los datos.
3. Autenticación a través del cifrado de datos asociado CCM-Modo o Modo GCM-(AEAD).”

7.2.3 HTTP Strict Transport Security (HSTS)

Es el mecanismo de seguridad utilizado para realizar conexiones seguras HTTP y que está presente en la RFC 6797, cuyo objetivo es impedir que atacantes puedan convertir el trafico HTTPS a HTTP. El mecanismo utiliza el navegador del usuario para inspeccionar la conexión con el servidor, con el fin de inspeccionar si ocurre algún error durante la comunicación segura SSL/TLS. La idea principal del mecanismo no es solo forzar las conexiones HTTPS, sino que también el objetivo fundamental es proporcionar seguridad al usuario al navegar en Internet, muestreando las conexiones donde están ingresando son cifradas con los protocolos de seguridad SSL/TLS.

El protocolo de navegación HTTP puede ser utilizado en diversos medios de transporte, generalmente estas conexiones se realizan bajo el protocolo TCP, el cual no proporciona integridad y confiabilidad en la transferencia de datos en la red. Por este motivo, son utilizados los protocolos de seguridad SSL/TLS y el mecanismo de seguridad HSTS, impidiendo que se realicen ataques de MITM en la red.

Jackson y Barth (2008), HSTS tiene sus comienzos en el año 2008 cuando Collin Jackson y Adam Barth difunden el prototipo de seguridad WEB ForceHTTPS, mecanismos utilizado para que los usuarios puedan navegar en la WEB de manera segura, mitigando las vulnerabilidades generadas por la red en navegadores cuando se establecen peticiones HTTP de manera estricta utilizando los protocolos SSL/TLS. (Hodges, Jackson y Barth (2012), en septiembre de 2009 Jeff Hodges de PayPal, Collin Jackson y Adam Barth lanzan una versión actualizada del mecanismo de seguridad ForceHTTPS, llamada Strict Transport Security (STS) donde es adoptada por navegadores reconocidos como Firefox, Google Chrome, entre otros. Finalmente, el mecanismo de seguridad STS se convierte en estándar de la IETF en noviembre del 2012 llamado HTTP Strict Transport Security (HSTS) y es encontrado en la RFC 6797.

7.2.4 Educación Virtual

Barhoum y Muhsen (2013), la educación viene evolucionando y acomodándose a las necesidades de empresas y personas, realizando cambios radicales en los diferentes métodos de aprendizaje en todos los sectores de educación a nivel mundial, con el fin de reducir costos y tiempos, proporcionar fácil accesibilidad desde cualquier lugar y ofrecer material de educación siempre disponible, dando lugar a la educación virtual desde plataformas interactivas de educación que son accedidas desde sitios de navegación WEB. e-Learning se ha catalogado como una herramienta de educación que brinda calidad a todos los estudiantes que están matriculados en la plataforma, ofreciendo servicios importantes como: permitir interactividad de los canales de comunicación de educación, procesos de aprendizaje diversos para todos los estilos de los estudiantes, variedad de multimedia, descarga e impresión de material de estudio desde la WEB y crear medios de interacción la colaboración, conversación e intercambio de ideas.

Gutiérrez (2017), Grupo Nethexa S.A.S viene adaptando y madurando su portafolio de servicios con la educación virtual (e-learning) tomando como base sus conocimientos de tecnología abierta (Open Source) y la integración de la plataforma de educación Moodle con todos sus desarrollos, construyendo soluciones de alta calidad y posibilidades ilimitadas de cara al cliente orientando el manejo eficiente del conocimiento de las compañías y sus integrantes, generando y administrando la información que debe ser transmitida, compartida y mantenida en el tiempo. La solución de educación virtual entra a tener un papel importante para las organizaciones en mantener la documentación y medir el nivel actual de los empleados de la planta laboral.
La solución del servicio está compuesta por 4 fases importantes para los clientes de la organización, con la finalidad de administrar y soportar toda la infraestructura; y desarrollo de toda la plataforma de e-Learning, brindado todas las soluciones posibles con los siguientes ítem:

1. Infraestructura Física: Implementación de plataformas con infraestructura en la nube, garantizando calidad, compatibilidad, estabilidad e integración a los clientes.
2. Software de educación virtual: Desarrollo, actualización e integración de plataformas de educación virtual.
3. Generación de contenidos: Desarrollo y diseño, multimedia, transformación de contenidos académicos y adecuación a estándares internacionales.
4. Administración y soporte: Soporte 24X7

Figura 2. Educación Virtual y contenidos (Gutiérrez, 2017).

7.2.5 VoIP

Baz, Bonilla, Gorrotxategi, Ibarra, Santamaría y Ruiz (2009), Voz sobre IP (VoIP) es un servicio que permite establecer llamadas sobre Internet, permitiendo la comunicación de voz y video desde diferentes redes que sean convergentes. Esta técnica es llamada Telefonía IP, la cual brinda calidad, fiabilidad y bajo costo de inversión para las organizaciones, ya que manejar diferentes códecs de audio y video que pueden facilitar el consumo de ancho de banda, facilita la integración en la administración y de seguridad por la integración sobre redes LAN.

Gutiérrez (2017), Grupo Nethexa S.A.S implementa, desarrolla y soporta infraestructuras VoIP bajo la comunidad de software libre Asterisk a todos sus clientes, contando con diferentes servicios de IP-PBX y soluciones de VoIP para Call Center que trabajan y son administrados sobre plataformas WEB, con los que es reconocido en el mercado por sus desarrollos propietarios en herramientas de salida y entrada de llamadas, campañas automáticas, características especiales y administración avanzada, donde posee productos novedosos como los es HexaDialer y HexaHUD que poseen grandes ventajas en la automatización de procesos, administración de reportes avanzados y en disponibilidad del servicio; algunas de las ventajas destacadas son:

- **Escalabilidad:** Los recursos están disponibles de la manera y en el momento en que el cliente los necesita, por lo que desaparecen los tiempos de espera

a la hora de ampliar la capacidad y no se desaprovecha la que no se esté utilizando.

- **Compatibilidad:** A diferencia de la telefonía tradicional la VoIP permite integrar en una sola infraestructura varias tecnologías, esto facilita el crecimiento futuro y la integración con infraestructuras ya existentes o futuras.
- **Flexibilidad:** Los servicios basados en VoIP permiten desarrollar soluciones integradas, que hacen uso de la telefonía pero que en esencia no pertenezca esta, como sistemas de cobro, CRM, consulta automatizada entre otros.
- **Independencia de la localización:** Por lo general, se puede acceder al servicio desde cualquier lugar, siempre y cuando se disponga de una conexión a Internet y enrutamiento adecuado.
- **Seguridad física en los centros de datos:** Los servicios disponibles a través de una infraestructura VPN que permite asegurar y controlar las comunicaciones entre los puntos de venta y la infraestructura central del cliente.
- **Soporte y Servicio:** La posibilidad de tener infraestructura no administrable en sitio facilita enormemente la capacidad de respuesta a la hora de fallos y contingencias, así como la posibilidad de realizar cambios y adaptaciones en menos tiempo.

Todas las plataformas VoIP de la organización son implementadas y desarrolladas en Asterisk. Herramienta de código abierto que proporciona: la disponibilidad del código fuente que garantiza a la continuidad del negocio, compatibilidad y escalabilidad por tener la facilidad de correo sobre hardware genérico lo que permite a la empresa no depender de un único fabricante de hardware y seguridad ya que Asterisk es fiable que cualquier otro sistema de comunicaciones comerciales debido a que el código es visible, cualquier detección de algún fallo de seguridad, es rápidamente publicado y su solución aparece en cuestión de horas.

Asterisk posee grandes beneficios, donde ofrece funciones de plantas telefónicas convencionales y avanzadas, añadiendo las opciones y características de VoIP, igualando las características que ofrecen los grandes sistemas de plantas telefónicas propietarias. Contando con un sistema de comunicaciones completo ofreciendo cualquier servicio asociado a telefonía que se pueda imaginar, brindando la integración con otros servicios expandiendo la posibilidad de soluciones.

Figura 3. Soluciones VoIP- IP-PBX (Gutiérrez, 2017).

7.2.6. Seguridad en plataformas de e-learning

La educación virtual se ha convertido en una herramienta esencial en el desarrollo de procesos de enseñanza y aprendizaje, por este motivo los entornos educativos se encuentran expuestos a riesgos tecnológicos que deben de ser identificados y mitigados de manera apropiada, debido a que tener vulnerabilidades puede afectar la seguridad de las plataformas educativas.

Se aconseja que la seguridad en las plataformas de e-learning adopte como mínimo las medidas necesarias para proteger los servicios que tiene alojados en el servicio WEB, como lo son: implementación de firewall en el servicio, acceso a través del certificado de seguridad HTTPS, adecuados permisos de acceso por FTP y bases de datos, cifrado en usuarios y contraseñas; y permisos en directorios.

La seguridad mínima de los servicios WEB de e-learning no es suficiente, debido que al transcurrir el tiempo los servicios manejados en las plataformas de e-learning son vulnerables al estar expuestos a Internet, debido a que los servicio deben de ser actualizados, monitoreados, auditados y asegurados constantemente a través de servicios de seguridad complementarios que permiten mitigar ataques informáticos realizados. Por este motivo, la importancia de regir las normas y los estándares de gestión en seguridad y riesgos informáticos, que poseen la finalidad de preservar la disponibilidad, continuidad e integridad de los servicios WEB de las plataformas virtuales; con el fin de, controlar y mitigar ataques informáticos como lo son: acceso no autorizado, abuso de privilegios, suplantación de identidad, hacking,

divulgación o fuga de información, entre otros; que pueden degradar el servicio y la imagen corporativa de la empresa o institución (Santiso, Koller y Bisaro, 2016).

7.2.7. Seguridad en plataformas de VoIP

La voz sobre IP posee ciertos inconvenientes con el desarrollo o el funcionamiento de la telefonía IP, que puede ser catalogada en tres conceptos diferentes, como lo son: seguridad, fiabilidad y calidad de servicio. Desde el punto de vista de seguridad informática, las llamadas de VoIP son transmitidas por Internet o por redes que son potencialmente inseguras, las cuales poseen riesgos de privacidad y seguridad que no poseen los sistemas telefónicos tradicionales.

VoIP es vulnerable, ya que puede verse degradada por la infección de virus, gusanos y malware que circula en la red de Internet, ataques de SPAM y debilidades en los dispositivos de red en la transmisión de voz, afectando la capa de transporte UDP en los protocolos que presta el servicio como lo son el SIP, IAX y RTP.

El servicio de VoIP no funciona por sí solo, este servicio necesita de un sistema operativo que albergue las aplicaciones complementarias como lo son los servicios WEB y bases de datos, las cuales facilitan la administración y la extracción de reportes de llamadas de la telefonía IP.

La VoIP es una tecnología que se apoya en las capas y protocolos existentes en las redes de datos, heredando los problemas de seguridad de las capas y los protocolos existentes, siendo algunas de estas las amenazas más importantes de VoIP, problemas clásicos que afectan directamente a la red de datos. Por lo que el servicio de telefonía IP posee varias capas de seguridad que deben ser protegidas, las cuales son:

- Seguridad en aplicaciones y protocolos VoIP.

  Control y mitigación de ataques contra Fraudes, SPAM, Phishing, Fuzzing, Floods, secuestro de sesiones, Intercepción, Redirección de llamadas y reproducción de llamadas.

- Seguridad en el sistema operativo.

  Protección contra Buffer Overflows, Gusanos, Virus, Malware y Malas configuraciones.

- Seguridad en los servicios.

  Protección contra injecciòn SQL, Denegación de DHCP y Denegación de servicios.

- Seguridad de Red.

Mitigación de Denegación de servicios distribuidos, ataques ICMP, SYN Floods, TCP Floods y UDP Floods.

- Seguridad Física.

Protección de dispositivos físicos sensibles, Reinicio de máquinas y denegación de servicios.

- Políticas y procedimientos.

Control ante contraseñas débiles, implementación errada de políticas de privilegios y accesos permitidos a datos que pueden ser comprometidos.

Todos los ataques de VoIP tienen un objetivo en específico, el cual es el robo de información confidencial de llamadas telefónicas, degradación de la calidad del servicio de telefonía IP, alteración de la información de llamadas entrantes y salientes, interceptación y secuestro de llamadas, reproducción de conversaciones, robo de identidad e incluso realizar llamadas gratuitas por todo el mundo. Por este motivo la importancia de implementar seguridad constante en el servicio de VoIP, ya que los servidores, sistemas operativos, protocolos con los que trabajan y la infraestructura de red VoIP es susceptible en todo momento de ser atacada (Gutiérrez, 2010).

7.3 Marco legal

El marco legal del proyecto de implantación del sistema de gestión integral de seguridad informática, que permita analizar y mitigar las vulnerabilidades críticas que poseen los servicios WEB de e-learning y Telefonía IP transversalmente en Grupo Nethexa S.A.S, debe tener presente la ley Colombiana y las normas Nacionales e Internacionales de gestión de seguridad informática, protección de datos, delitos informáticos, derechos de autor y divulgación de información confidencial, que puedan apalancar la solución del problema de la organización, por este motivo debemos de tener las siguientes normas presentes:

Decisión 351 (1993), Acuerdo de Cartagena y la ley 23 de 1982 establecen las leyes sobre los derechos de autor.

La ley informa sobre la Régimen común sobre derechos de autor y derechos conexos, protección de los derechos de autor, identificación del alcance; y aporta elementos de los sistemas de la información, encontrando aportes importantes en los siguientes artículos:

“Artículo 1. Las disposiciones de la presente Decisión tienen por finalidad reconocer una adecuada y efectiva protección a los autores y demás titulares de derechos, sobre las obras del ingenio, en el campo literario, artístico o científico, cualquiera

que sea el género o forma de expresión y sin importar el mérito literario o artístico ni su destino.
...
Artículo 7. Queda protegida exclusivamente la forma mediante la cual las ideas del autor son descritas, explicadas, ilustradas o incorporadas a las obras.
...
Artículo 9. Una persona natural o jurídica, distinta del autor, podrá ostentar la titularidad de los derechos patrimoniales sobre la obra de conformidad con lo dispuesto por las legislaciones internas de los Países Miembros.
...
Artículo 11. El autor tiene el derecho inalienable, inembargable, imprescriptible e irrenunciable de:

a) Conservar la obra inédita o divulgarla;
b) Reivindicar la paternidad de la obra en cualquier momento; y,
c) Oponerse a toda deformación, mutilación o modificación que atente contra el decoro de la obra o la reputación del autor.

...
Artículo 52. La protección que se otorga a las obras literarias y artísticas, interpretaciones y demás producciones salvaguardadas por el Derecho de Autor y los Derechos Conexos, en los términos de la presente Decisión, no estará subordinada a ningún tipo de formalidad. En consecuencia, la omisión del registro no impide el goce o el ejercicio de los derechos reconocidos en la presente Decisión."

Ley 1450 (2011), control de los derechos de autor.
"Artículo 28. Propiedad intelectual obras en cumplimiento de un contrato de prestación de servicios o de un contrato de trabajo. El artículo 20 de la Ley 23 de 1982 quedará así:
Artículo 20. En las obras creadas para una persona natural o jurídica en cumplimento de un contrato de prestación de servicios o de un contrato de trabajo, el autor es el titular originario de los derechos patrimoniales y morales; pero se presume, salvo pacto en contrario, que los derechos patrimoniales sobre la obra han sido transferidos al encargado o al empleador, según sea el caso, en la medida necesaria para el ejercicio de sus actividades habituales en la época de creación de la obra. Para que opere esta presunción se requiere que el contrato conste por escrito. El titular de las obras de acuerdo con este artículo podrá intentar directamente o por intermedia persona acciones preservativas contra actos violatorios de los derechos morales informando previamente al autor o autores para evitar duplicidad de acciones."

Ley 599 (2000), código Penal, establece las sanciones contra los derechos de autor y daño por divulgación de información confidencial.
"Artículo 270. Violación a los derechos morales de autor. Incurrirá en prisión de dos (2) a cinco (5) años y multa de veinte (20) a doscientos (200) salarios mínimos legales mensuales vigentes quien:

1. Publique, total o parcialmente, sin autorización previa y expresa del titular del derecho, una obra inédita de carácter literario, artístico, científico, cinematográfico, audiovisual o fonograma, programa de ordenador o soporte lógico.
2. Inscriba en el registro de autor con nombre de persona distinta del autor verdadero, o con título cambiado o suprimido, o con el texto alterado, deformado, modificado o mutilado, o mencionando falsamente el nombre del editor o productor de una obra de carácter literario, artístico, científico, audiovisual o fonograma, programa de ordenador o soporte lógico.
3. Por cualquier medio o procedimiento compendie, mutile o transforme, sin autorización previa o expresa de su titular, una obra de carácter literario, artístico, científico, audiovisual o fonograma, programa de ordenador o soporte lógico."

Ley 222 (1995), la información puede ser confidencial

"Artículo 23. Los administradores deben obrar de buena fe, con lealtad y con la diligencia de un buen hombre de negocios. Sus actuaciones se cumplirán en interés de la sociedad, teniendo en cuenta los intereses de sus asociados. Donde en el cumplimiento de todo administrador es de abstenerse de utilizar indebidamente información privilegiada, preservando la confidencialidad de la información de la organización."

Ley 1712 (2014), ley de la transparencia y acceso a la información pública

"El objeto de la presente ley es regular el derecho de acceso a la información pública, los procedimientos para el ejercicio y garantía del derecho y las excepciones a la publicidad de información.

...

Artículo 7. Disponibilidad de la Información. En virtud de los principios señalados, deberá estar a disposición del público la información a la que hace referencia la presente ley, a través de medios físicos, remotos o locales de comunicación electrónica. Los sujetos obligados deberán tener a disposición de las personas interesadas dicha información en la Web, a fin de que estas puedan obtener la información, de manera directa o mediante impresiones. Asimismo, estos deberán proporcionar apoyo a los usuarios que lo requieran y proveer todo tipo de asistencia respecto de los trámites y servicios que presten.

…

Artículo 8. Criterio diferencial de accesibilidad. Con el objeto de facilitar que las poblaciones específicas accedan a la información que particularmente las afecte, los sujetos obligados, a solicitud de las autoridades de las comunidades, divulgarán la información pública en diversos idiomas y lenguas y elaborarán formatos alternativos comprensibles para dichos grupos. Deberá asegurarse el acceso a esa información a los distintos grupos étnicos y culturales del país y en especial se adecuarán los medios de comunicación para que faciliten el acceso a las personas que se encuentran en situación de discapacidad."

Ley 1581 (2012), Disposiciones Generales para la Protección de Datos Personales

"Artículo 1. Objeto. La presente ley tiene por objeto desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma.

...

Artículo 2. Ámbito de aplicación. Los principios y disposiciones contenidas en la presente ley serán aplicables a los datos personales registrados en cualquier base de datos que los haga susceptibles de tratamiento por entidades de naturaleza pública o privada. La presente ley aplicará al tratamiento de datos personales efectuado en territorio colombiano o cuando al responsable del Tratamiento o Encargado del Tratamiento no establecido en territorio nacional le sea aplicable la legislación colombiana en virtud de normas y tratados internacionales.

El régimen de protección de datos personales que se establece en la presente ley no será de aplicación:

a) A las bases de datos o archivos mantenidos en un ámbito exclusivamente personal o doméstico.
b) A las bases de datos y archivos que tengan por finalidad la seguridad y defensa nacional, así como la prevención, detección, monitoreo y control del lavado de activos y el financiamiento del terrorismo;
c) A las Bases de datos que tengan como fin y contengan información de inteligencia y contrainteligencia;
d) A las bases de datos y archivos de información periodística y otros contenidos editoriales;
e) A las bases de datos y archivos regulados por la Ley 1266 de 2008;
f) A las bases de datos y archivos regulados por la Ley 79 de 1993."

Ley 1273 (2009), Delitos Informáticos

"Artículo 269A. Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

...

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios

mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.
...
Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.
...
Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
...
Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.
...
Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.
...
Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.
...
Artículo 269I: Hurto por medios informáticos y semejantes. El que, superando medidas de seguridad informáticas, realice la conducta señalada en el artículo 239 manipulando un sistema informático, una red de sistema electrónico, telemático u otro medio semejante, o suplantando a un usuario ante los sistemas de autenticación y de autorización establecidos, incurrirá en las penas señaladas en el artículo 240 de este Código.
...
Artículo 269J: Transferencia no consentida de activos. El que, con ánimo de lucro y valiéndose de alguna manipulación informática o artificio semejante, consiga

la transferencia no consentida de cualquier activo en perjuicio de un tercero, siempre que la conducta no constituya delito sancionado con pena más grave, incurrirá en pena de prisión de cuarenta y ocho (48) a ciento veinte (120) meses y en multa de 200 a 1.500 salarios mínimos legales mensuales vigentes. La misma sanción se le impondrá a quien fabrique, introduzca, posea o facilite programa de computador destinado a la comisión del delito descrito en el inciso anterior, o de una estafa."

SGSI (2017), Modelo de Seguridad Colombiano: Sistemas de Gestión de la Seguridad de la Información

"El Ministerio de Tecnologías de la Información y las Comunicaciones - MinTIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones; pública El Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión. "Colombia establece un modelo de seguridad y de privacidad que es actualizado periódicamente de las buenas prácticas de seguridad de la información adoptadas de la norma internacional ISO 27001 del 2013, la cual permite la confidencialidad, el aseguramiento e integridad de los datos e información que son procesados informáticamente.

El MSPI cuenta con una metodología importante que posee que con una serie de guías que ayudan a las organizaciones colombianas puedan evaluar los riesgos y puedan aplicar controles de seguridad puedan eliminarlos o mitigarlos. "La implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, en la Entidad está determinado por las necesidades objetivas, los requisitos de seguridad, procesos, el tamaño y la estructura de la misma, todo con el objetivo de preservar la confidencialidad, integridad, disponibilidad de los activos de información, garantizando su buen uso y la privacidad de los datos."

7.4 Estado del arte

Es necesario comprender la finalidad de la seguridad informática para plataformas de navegación WEB, por el motivo de que el proyecto de maestría está enfocado en la mitigación de vulnerabilidades en plataformas informáticas que trabajan bajo los protocolos HTTP que proporcionan aplicaciones WEB a todos los usuarios que utilizan los servicios de VoIP y de e-learning en Grupo Nethexa S.A.S. Es importante poder conocer qué vulnerabilidad presentan los protocolos de seguridad, los tipos de ataques informáticos que se utilizan actualmente, tipos de herramientas utilizadas para detección de vulnerabilidades y que se ha hecho para mejorar o descubrir los problemas de seguridad en aplicaciones WEB. Por lo que hablaremos un poco de los antecedentes importantes que se han extraído con un estudio de la literatura.

El mecanismo de seguridad de navegación HSTS es creado con el objetivo de obligar a que todos los usuarios que están explorando sitios WEB puedan navegar de manera segura, este mecanismo exige que el navegador negocie la conexión del cliente y el servidor de manera segura a través de los protocolos de seguridad SSL y TLS; evitando que un atacante en la red pueda interceptar los datos de comunicación de la conexión en texto plano, forzando a que los usuarios se conecten por el protocolo seguro de navegación HTTPS en vez del protocolo menos seguro HTTP.

Hodges, Jackson y Barth (2012), el protocolo de navegación HTTP puede ser utilizado en diversos medios de transporte, generalmente estas conexiones se realizan bajo el protocolo TCP, el cual no proporciona integridad y confiabilidad en la transferencia de datos en la red. Por este motivo, son utilizados los protocolos de seguridad Secure Sockets Layer (SSL), y su sucesor, Transport Layer Security (TLS) que fueron creados para dar seguridad de transferencia de información en la red con el protocolo TCP. Los protocolos SSL/TLS no estaba proporcionada seguridad en la comunicación WEB de los usuarios en la red, ya que diferentes ataques pasivos y activos pueden burlar el uso de la navegación WEB segura forzando que la conexión sea insegura, con el propósito de recolectar información en texto plano, este inconveniente es solucionado con el mecanismo HTTP Strict Transport Security (HSTS).

Jackson y Barth (2008), HSTS tiene sus comienzos en el año 2008 cuando Collin Jackson y Adam Barth difunden el prototipo de seguridad WEB Force HTTPS, mecanismos utilizado para que los usuarios puedan navegar en la WEB de manera segura, mitigando las vulnerabilidades generadas por la red en navegadores cuando se establecen peticiones HTTP de manera estricta utilizando los protocolos SSL/TLS. Hodges, Jackson y Barth (2012) En septiembre de 2009 Jeff Hodges de PayPal, Collin Jackson y Adam Barth lanzan una versión actualizada del mecanismo de seguridad Force HTTPS, llamada Strict Transport Security (STS) donde es adoptada por navegadores conocidos como Firefox, Google Chrome, entre otros. Finalmente, el mecanismo de seguridad STS se convierte en estándar de la IETF en noviembre del 2012 llamado HTTP Strict Transport Security (HSTS) y es encontrado en la RFC 6797.

El propósito de HSTS es beneficiar a los usuarios en la seguridad de la navegación HTTP, estableciendo la conexión HTTPS entre el usuario y el servidor a través del navegador; forzando la conexión obligando utilizar las diferentes versiones de los protocolos SSL/TLS. Como punto de partida los protocolos de seguridad de navegación HTTP han presentado vulnerabilidades que son importantes para la investigación del trabajo de maestría, por este motivo se analiza las debilidades de los protocolos de seguridad que pueden ayudar a encontrar las vulnerabilidades, que pueden afectar directa e indirectamente el mecanismo de seguridad HSTS en servicios WEB.

Brooks y Deng (2010), indican que la mayoría de los sitios de Internet utilizan SSL/TLS como mecanismo de confianza, el cual ha presentado una serie de debilidades en seguridad presentando problemas en la criptografía que maneja, permitiendo ser vulnerables a través de servicios que establecen funciones importantes en la red, como la resolución de nombres de dominio (DNS), enrutamiento sobre Internet, envenenamiento de caché ARP, la destitución de cifrados, errores de programación, la usabilidad del navegador y en ocasiones el criptoanálisis. Presentando lecciones importantes para diseños e implementaciones de nuevos servicios que deben de poseer confianza, por la inseguridad que presentan los ataques MITM para los usuarios en la red.

Mavrogiannopoulos, Vercauteren, Velichkov y Preneel (2012), demuestran que el protocolo SSL/TLS es vulnerable a través de los ataques Wagner y Schneier, el cual utiliza curvas elípticas con parámetros claros en el cifrado Diffie-Hellman, firmados por servidores y que pueden ser interceptados fácilmente por los usuarios. Dacosta, Ahamad, y Traynor (2012), proponen utilizar el certificado de validación DVCert, modelo de confianza que propone la validación de certificados fuertes y alta detección de los ataques informáticos MITM. El método funciona con el establecimiento de secretos de doble vía con servicios web importantes, estos secretos son validados por los usuarios y el servicio para dar autenticidad, evitando ataques MITM que está aprovechando las debilidades del método certificación CA desde la red. Los cambios hechos en el protocolo TLS por DVCert, proporcionan una mejora de rendimiento y simplicidad de la seguridad, sin afectar PAK el cual es el método encargado del intercambio de claves del protocolo de seguridad TLS.

Sugavanesh, Prasath y Selvakumar (2013), informan que el protocolo TLS es inseguro, porque para todo usuario al momento de realizar la primera conexión a un sitio WEB, no se encuentra protegido, ya que al hacer la primera solicitud en texto plano devuelve al usuario los datos de conexión segura (HTTPS), lo que da lugar a que un atacante suplante la conexión con un MITM y el usuario acepte el certificado incorrecto proporcionado por el atacante. Se plantea la utilización de HSTS, el cual emplea un método de inicio de confianza utilizando STS, donde realiza la primera conexión en el navegador que posee un filtro o control forzando de conexión segura, HSTS forzó la primera solicitud como los métodos HTTPS Lock y Force HTTPS, evitando ataques de MITM en el inicio de sesión de una conexión WEB, aunque las vulnerabilidades persisten en el apretón de manos del protocolo TLS, permitiendo que la conexión pueda ser atacada con éxito.

Eldewahi, Sharfi, Mansor y Mohamed (2015), los protocolos SSL/TLS han presentado grandes vulnerabilidades en la red de datos, el cual no está exhibiendo la confiabilidad, integridad y autenticidad, enseñando una brecha de seguridad para plataformas de navegación y de transferencia de archivos en la red, por sus debilidades que aprovechan los atacantes y las limitaciones que poseen las actuales contramedidas. Un gran número de vulnerabilidades han sido descubiertas en los protocolos SSL/TLS, en las cuales se destacan ataques como: Cipher Suites

Rollback, ChangeCipherSpec Message Drop, ataque Bleichenbacher en PKCS#1, ataques de temporización remota OpenSSL, DoS, ataques sobre el almacenamiento de datos MAC, ataques CBC-Modo, ataques en algoritmos de comprensión, ataque al algoritmo RC4, Ataque Lucky 13, entre otros. Los cuales han sido satisfactorios y que proporciona inseguridad en la red de datos. Dowling, Günther, Fischlin y Stebila (2015), estudian la seguridad criptológica del protocolo TLS 1.3 y la autenticación Diffie-Hellman, el cual actualiza y mejora la seguridad de las anteriores versiones de los protocolos de seguridad TLS 1.1 y 1.2 de las vulnerabilidades que poseen, los cuales son aprovechados por la ciberseguridad con ataques conocidos como: BESTIA, Lucky 13, CANICHE, etc., comprometiendo la integridad y confiabilidad de los datos de las aplicaciones Web y correo electrónico.

Han, Kwon, Hahn, Koo, y Hur (2016), SSL/TLS utiliza certificados para mitigar los ataques MITM, entre la CA que emite un certificado de confianza garantizando la identidad del servidor. Pero al comprometerse el certificado CA, con certificados falsos y la caducidad de los certificados, todos estos métodos del protocolo de seguridad no son suficientes para detectar y prevenir los ataques de MITM. Por estas vulnerabilidades que posee el protocolo de seguridad, se realiza un análisis de ataques de MITM en el apretón de manos de SSL/TLS, se hace pasar por un usuario legítimo, demostrando que la seguridad del protocolo es vulnerable y que no puede mitigar todos los ataques de MITM.

La información investigada ayuda a aclarar que los protocolos de seguridad SSL/TLS que son utilizados en la actualidad son vulnerables; sin embargo, a pesar de que el protocolo seguridad es actualizado y mejorado, persisten las debilidades que pueden ser aprovechadas por ataques informáticos. Como punto de partida ante las vulnerabilidades encontradas en los protocolos de seguridad y de comunicación, se encuentra diferentes procedimientos de pentesting que ayudan a retroalimentar el trabajo de maestría planteado, tomando en cuenta las investigaciones y desarrollos de seguridad informática actuales que pueden apoyar a evidenciar las vulnerabilidades existentes en los servicios WEB de Grupo Nethexa S.A.S.

LeonardoNev (2015), SSLStrip2, DNS2Proxy, Delorian, MITMF y BeterCap, son herramientas que proporcionan ataques informáticos de MITM que nacen del investigador Leonardo Nve, estas herramientas son nuevas versiones de ataques informáticos. Orientados a la navegación HTTPS, que contienen características importantes con el fin de evitar el mecanismo de protección HSTS. El propósito fundamental de estas herramientas es cambiar el tráfico HTTPS a HTTP y el nombre de la máquina en el código HTML, con el fin de evitar el mecanismo HSTS, capturando el tráfico en texto plano entre la conexión del cliente y el servidor.

Romero (2015), también, existen herramientas metodológicas que están encargadas de automatizar análisis de pentesting en aplicaciones WEB, proyectos

enfocados en escanear, atacar e informar los problemas de seguridad de los servicios que trabajan bajo el protocolo HTTP como: OWASP, Nessus, Metasploit, Arachni, Burp, OpenVast, w3af, Acunetix, entre otras. OWASP (2013), estos proyectos poseen cualidades importantes en cross-site scripting (XSS), inyección de SQL, OS y LDAP, pérdida de autenticación y gestión de sesiones, referencias directas de objetos inseguros, exposición de datos sensibles, ausencia de control de acceso a funciones, Cross-site request forgery (CSRF), utilización de componentes con vulnerabilidades conocidas, redirección y reenvió no válidos, denegación de servicios, entre otros. Informando los problemas de seguridad, el nivel de riesgo que posee y documentación de las posibles soluciones.

Revisando la literatura se observa que existen vulnerabilidades en los protocolos de seguridad WEB que pueden ser identificadas por herramientas de pentesting y que son aprovechadas por ataques informáticos automatizados que son desarrollados por científicos, con la finalidad de realizar ataques informáticos que pueden afectar la disponibilidad del servicio WEB de las plataformas que posee Grupo Nethexa S.A.S, por lo que la organización identifica la necesidad de tener un plan de gestión de seguridad informática que integre y cubra los servicios WEB de plataformas de e-learning y de Telefonía IP, con el propósito general de poder mitigar o minimizar el riesgo informático que poseen todas las aplicaciones WEB de la organización, por lo que se realiza un proyecto de seguridad que permite gestionar constantemente los riesgos de seguridad encontrados.

Existen métodos y normas de buenas prácticas de seguridad de la información, que orientan a las organizaciones a gestionar el riesgo informático a través de la administración de políticas y procesos informáticos que se alinean a las estrategias y al gobierno de las empresas, cuya prioridad es asegurar y tener disponibilidad de todos los sistemas de información TIC que mantienen la continuidad del negocio de toda organización que Grupo Nethexa desea adaptar. En la investigación se encuentran diferentes metodologías Nacionales e Internacionales que pueden ser adaptadas por Grupo Nethexa S.A.S como lo son el Modelo de Seguridad y Privacidad de la Información Colombiano (MSPI), MAGERIT, OCTAVE, CRAMM, EBIOS, MAHARI Y O-ISM3, orientando a las organizaciones en la implementación de gestión de análisis de riesgos y en la gestión de los sistemas de información, siguiendo los lineamientos de las normas ISO 27001:2013 y la ISO/IEC 27005:2008.

Torres y Rojas (2017), OCTAVE es una metodología utilizada para la evaluación y gestión de riesgos con el propósito de que las organizaciones puedan realizar gestión de activos, conocer posibles amenazas y evaluar las vulnerabilidades que poseen, garantizando la seguridad de los sistemas de información siguiendo los lineamientos del estándar internacional ISO 27001. Octave utiliza un enfoque de tres fases cuyo objetivo es disminuir las falsas creencias en seguridad informática y presentar principios básicos en la estructura de mejores prácticas internacionales que guían la gestión de riesgos de seguridad.

MEHARI (2010), MEHARI proporciona un método de evaluación y gestión de los riesgos cualitativos y cuantitativos, siguiendo los requerimientos de la norma ISO/IEC 27005:2008, proporcionado un conjunto de herramientas y bases de datos de conocimiento necesarios para la adaptación del método. Las bases de datos de conocimiento y los procedimientos automatizados dan un enfoque a MEHARI para la evaluación de los factores que caracterizan cada uno de los riesgos identificados, permitiendo evaluar su nivel de criticidad. Además, el método proporciona asistencia para la selección de los planes de tratamiento adecuados.

EBIOS (2003), EBIOS es un método que permite apreciar e identificar los riesgos de seguridad en los sistemas de información (SSI), proporcionando las justificaciones necesarias en la toma de decisiones como una herramienta de negociación. No se trata solo de un método de SSI, sino también de una herramienta de software libre que ayuda al diseño de proyectos asociados al campo de gestión de riesgos informáticos. Este método permite identificar los objetivos y requerimientos de seguridad tras una apreciación de riesgos, construyendo con los esquemas de dirección de SSI, políticas de seguridad, planes de accesión de SSI y; en la adaptación y justificación de proyectos de seguridad.

Torres y Rojas (2017), MAGERIT es una metodología de análisis y gestión de riesgos de los sistemas de información relacionados con la seguridad de las TIC, elaborado por el Consejo Superior de Administración Electrónica para dar respuesta a las necesidades de administración de TIC que depende de la seguridad, con el propósito de que la sociedad tenga un crecientemente de las tecnologías de la información y pueda cumplir con la misión de los deberes personales y empresariales, beneficiando a las organizaciones que lo implementan minimizando los riesgos seguridad adaptando medidas que generen confianza. La metodología está dirigida todas las personas que trabajan con información digital y sistemas informáticos, brindado la posibilidad de saber cuánto valor se está jugando la organización ayudando a protegerlos.

CRAMM (2002), CRAMM es una herramienta utilizada para el análisis y gestión de riesgos cualitativos desarrollados por la Agencia Central de Computación y Telecomunicaciones del Gobierno del Reino Unido en 1985, proporcionado a departamentos gubernamentales un método para la supervisión de seguridad en los sistemas de información. CRAMM puede ser utilizado en todo tipo de organización, con el fin de justificar las inversiones de seguridad y de contingencias en sistemas de información y redes de telecomunicaciones, demostrando la importancia de realizar gestión con resultados cuantificables y contramedidas a implementar luego del análisis de riesgos, dando cumplimento al estándar Británico BS7799 identificando y valorando los activos de la organización, identificando amenazas y vulnerabilidades, calculando los riesgos y priorizando e identificando las contramedidas.

MSPI (2017), Modelo de seguridad y privacidad de la información colombiano (MSPI) se encuentra alineado con el marco referencial de Arquitectura de TI soportando transversalmente los componentes estratégicos en servicios de TIC, gobierno Abierto de TIC y Gestión de TIC. El modelo está acorde con los lineamientos de buenas prácticas de seguridad y es actualizado periódicamente con las mejoras que se van adquiriendo, reuniendo los cambios que se realizan en la norma ISO 27001:2013, la legislación de ley en la protección de datos personales, transparencia y acceso de la información pública, las cuales son importantes para la gestión de la información. El MSPI cuenta con una serie de guías anexas que ayudan a todas las entidades en cumplir las buenas prácticas de seguridad de la información, permitiendo abordar cada una de las fases que brinda el modelo, buscando comprender los resultados a obtener y cómo desarrollarlos, incluyendo los nuevos lineamientos que permitan la adopción del protocolo de enrutamiento IPv6 en todo el estado colombiano. La implementación del modelo MSPI en las organizaciones permite determinar las necesidades objetivas, requisitos de seguridad, procesos, tamaño y estructura de la entidad, con el objetivo de preservar la confidencialidad, integridad y disponibilidad de los activos de información, garantizado el uso de la información y la privacidad de los datos, contribuyendo con la transparencia de la gestión pública, promoviendo el uso de buenas prácticas de seguridad de la información aplicando los conceptos de seguridad digital.

O-ISM3 (2017), O-ISM3 es un estándar de madurez que define los procesos de seguridad, con el fin administrar el sistema de gestión de seguridad de la información (ISMS) de las organizaciones. O-ISM3 asigna las responsabilidades al negocio empresarial en definir los objetivos de seguridad en políticas, ofreciendo un conjunto de procesos administrativos en seguridad donde el negocio selecciona como implementar un ISMS coherente para poder alcanzar todos los objetivos de seguridad del negocio. La idea principal es definir la confidencialidad, disponibilidad, integridad y conceptos relacionados con seguridad de la información, realizando un diseño de cinco niveles de madurez; permitiendo a las organizaciones elegir una línea base para la implementación del sistema de gestión de la seguridad de la información (ISM) y utilizar el resto de los niveles como hitos para niveles O-ISM3 más altos a medida que la organización evoluciona. Con los niveles de madurez, la organización puede priorizar la inversión y medir el progreso.
El proyecto O-ISM3 ha sido probado con diferentes estándares como CMMI, ISO 9001, COBIT, ITIL, ISO 27001, entre otros; hallando mejoras considerables en los campos de aplicación vinculando las necesidades del negocio, utilizando un enfoque basado en procesos proporcionando detalles adicionales en la implementación y sugerencias de métricas preservando la compatibilidad de los estándares actuales de administración en seguridad y TI. El estándar es llamativo para la solución del trabajo de grado, ya que Grupo Nethexa S.A.S no tiene un sistema de gestión de seguridad de la información que pueda ser compatible con procesos de ISO 27001, ITIL y COBIT, que sea ágil de implementar, económico ya que se facilita en adaptarse en empresas de tienen recursos limitados y es

compatible con los estándares más utilizados en las organizaciones, a las que le presta el servicio de TIC.
En el proyecto de maestría pretende implementar el sistema de gestión integral de seguridad informática en servicios WEB de e-learning y Telefonía IP en Grupo Nethexa S.A.S, con el fin de poder utilizar una metodología que permita establecer procesos y políticas que permitan realizar una evaluación en seguridad WEB constante en la organización, con el objetivo de no afectar la disponibilidad del servicio WEB de los clientes. A través de, identificación de vulnerabilidades existentes informáticas a aplicaciones HTTP que pueden ser explotadas en los servicios WEB de e-learning y Telefonía IP en Grupo Nethexa S.A.S. Con el fin de administrar y controlar el riesgo de las vulnerabilidades críticas adaptando controles de seguridad que ayuden a mitigar y a minimizar el riesgo informático de los servicios WEB de la organización, contribuyendo en la mejora de la continuidad del negocio reduciendo los problemas de seguridad informática.

8 Fundamentación del proyecto

8.1 Objetivo General

Implementar un sistema de gestión integral de seguridad informática en los servicios WEB de e-learning y Telefonía IP de Grupo Nethexa S.A.S. que permita identificar y mitigar los riesgos de seguridad críticos que afectan la disponibilidad de los servicios, implementando controles que proporcionen confiabilidad, integridad y autenticidad de los datos.

8.2 Objetivos Específicos, actividades y cronograma

Tabla 1. Objetivos específicos

Objetivo Específico No. 1							
Seleccionar un modelo de gestión que oriente el proceso de auditoría de seguridad en los servicios WEB de e-learning y Telefonía IP en la organización.							
Productos							
Documento de auditoria en la evaluación constante en seguridad informática, en los servicios WEB de e-learning y Telefonía IP en Grupo Nethexa S.A.S.							
Actividades							
No	**Descripción**	**Cronograma**					
		M1	**M2**	**M3**	**M4**	**M5**	**M6**
1	Búsqueda del modelo de gestión de seguridad de la información.	X					
2	Establecimiento de los procesos y políticas que ayuden a la auditoria de seguridad informática en los servicios WEB de la organización.	X	X				
3	Documentación de los procesos y políticas en la auditoria de seguridad informática y levantar plantillas que ayude a analizar los resultados de la identificación de vulnerabilidades en los servicios WEB de la organización.		X				

Tabla 2 Objetivos específicos

Objetivo Específico No. 2
Determinar las vulnerabilidades críticas que poseen los servicios WEB de e-learning y Telefonía IP en la organización.
Productos
- Reporte de vulnerabilidades y riesgos identificadas en los servicios WEB de e-learning y Telefonía IP en la organización. - Informe de análisis de los riesgos en los servicios WEB de e-learning y Telefonía IP en la organización.
Actividades

No	Descripción	Cronograma					
		M1	M2	M3	M4	M5	M6
1	Selección de técnicas eficientes para identificar las vulnerabilidades de los servicios WEB de la Organización.			X			
2	Búsqueda de las vulnerabilidades que poseen los servicios WEB de e-learning y Telefonía IP en la organización.			X			
3	Evaluación de la criticidad de las vulnerabilidades encontradas con un análisis de riesgos.				X		

Tabla 3 Objetivos específicos

Objetivo Específico No. 3							
Adaptar controles de seguridad que permitan disminuir el impacto de los ataques informáticos en los servicios WEB de e-learning y Telefonía IP en la organización.							
Productos							
- Documento con metodología de controles y configuración de buenas prácticas de seguridad en los servicios WEB de e-learning y Telefonía IP en la organización.							
Actividades							
No	**Descripción**	**Cronograma**					
		M1	**M2**	**M3**	**M4**	**M5**	**M6**
1	Determinación de los controles que mitiguen el impacto de la materialización de las vulnerabilidades y riesgos identificados, en los servicios WEB de e-learning y Telefonía IP en la organización.					X	
2	Determinación de buenas prácticas en la configuración de seguridad en los servicios WEB de e-learning y -Telefonía IP de la organización.					X	X
3	Documentación del análisis de los controles y la configuración de buenas prácticas de seguridad, que deben ser aplicados en los servicios WEB de e-learning y Telefonía IP en la organización.						X

8.3 Metodología y Alcance

8.3.1 Metodología

Para alcanzar los objetivos planteados, y brindarle a Grupo Nethexa S.A.S el conocimiento necesario para analizar las vulnerabilidades que afectan la seguridad en los servicios WEB de e-learning y Telefonía IP. Se propone desarrollar un sistema de gestión integral de seguridad informática que se encargará de identificar y mitigar los problemas de seguridad de los servicios WEB de la organización. Las fases propuestas son las siguientes:

Fase 1. Seleccionar un modelo de gestión que oriente el proceso de auditoría de seguridad en los servicios WEB de e-learning y Telefonía IP en la organización.
Determinar modelo de gestión de seguridad de la información ágil que permita establecer todos los procesos de auditoria necesarios para evaluar y mitigar las vulnerabilidades de los servicios WEB de la organización.

- Búsqueda del modelo de gestión de seguridad de la información.
- Establecimiento de los procesos y políticas que ayuden a la auditoria de seguridad informática en los servicios WEB de la organización.
- Documentación de los procesos y políticas en la auditoria de seguridad informática y levantar plantillas que ayude a analizar los resultados de la identificación de vulnerabilidades en los servicios WEB de la organización.

Fase 2. **Determinar las vulnerabilidades críticas que poseen los servicios WEB de e-learning y Telefonía IP en la organización.**
Generar reporte de vulnerabilidades identificadas en los servicios WEB de e-learning y Telefonía IP en la organización, con el fin de realizar un análisis de riesgos identificando las vulnerabilidades críticas.

- Selección de técnicas eficientes para identificar las vulnerabilidades de los servicios WEB de la Organización.
- Búsqueda de las vulnerabilidades que poseen los servicios WEB de e-learning y Telefonía IP en la organización.
- Evaluación de la criticidad de las vulnerabilidades encontradas con un análisis de riesgos.

Fase 3. Adaptar controles de seguridad que permitan disminuir el impacto de los ataques informáticos en los servicios WEB de e-learning y Telefonía IP en la organización.
Con la obtención de los resultados de las vulnerabilidades críticas identificadas en el análisis de riesgos, es necesario adaptar los controles de seguridad en los servicios WEB de la organización, con el fin de crear un documento que proporcione

las pautas de seguridad necesarias que permitan la implementación de los controles y buenas prácticas de seguridad informática.

- Determinación de los controles que mitiguen el impacto de la materialización de las vulnerabilidades y riesgos identificados, en los servicios WEB de e-learning y Telefonía IP en la organización.
- Determinación de buenas prácticas en la configuración de seguridad en los servicios WEB de e-learning y -Telefonía IP de la organización.
- Documentación del análisis de los controles y la configuración de buenas prácticas de seguridad, que deben ser aplicados en los servicios WEB de e-learning y Telefonía IP en la organización.

8.3.2 Alcance

El alcance del proyecto de grado es poder implementar un sistema de gestión integral de seguridad informática en los servicios WEB de e-learning y Telefonía IP en Grupo Nethexa S.A.S. Que permita la identificación y corrección de los problemas de seguridad críticos que afectan la disponibilidad del servicio, proporcionando controles que aporten confiabilidad, integridad y autenticidad en las aplicaciones y servicios HTTP. El proyecto se enfoca en entregar a la empresa un modelo de gestión de seguridad de la información, con el objetivo de identificar vulnerabilidades, evaluar el riesgo informático y proporcionar controles de seguridad, en las plataformas de la organización donde se genera la documentación necesaria de seguridad con el fin de, implementar controles que mitiguen los problemas de seguridad críticos de las plataformas WEB de e-learning y Telefonía IP en la organización.

El trabajo por realizar no se compromete a implementar los controles de seguridad en las plataformas WEB que se encuentran en producción, se realizará un SGSI con toda la información necesaria que apunta a los objetivos estratégicos de la organización y de gobierno, que tendrán la responsabilidad de hacer cumplir los lineamientos de seguridad establecidos en las plataformas de producción.

Los entregables del proyecto son los siguientes:

- Documento de auditoria en la evaluación constante en seguridad informática, en los servicios WEB de e-learning y Telefonía IP en Grupo Nethexa S.A.S.
- Reporte de vulnerabilidades y riesgos identificados en los servicios WEB de e-learning y Telefonía IP en la organización.
- Informe de análisis de los riesgos en los servicios WEB de e-learning y Telefonía IP en la organización.
- Documento con metodología de controles y configuración de buenas prácticas de seguridad en los servicios WEB de e-learning y Telefonía IP en la organización.

Presupuesto General del Proyecto

Tabla 1. Descripción de personal (en horas).

INVESTIGADOR / ASESOR/ AUXILIAR	FORMACIÓN ACADÉMICA	FUNCIÓN DENTRO DEL PROYECTO	DEDICACIÓN (h/sem)	Total de horas	
				UPB	Otras fuentes
Sebastian Restrepo	Ingeniero	Investigador	10	96	144
Juan Camilo Estrada	Ingeniero	Asesor Temático	2	0	48
Julian Gutierrez	Ingeniero	Asesor Técnico	2	0	48
Director	Magister	Director	4	96	0
TOTAL				192	240

Tabla 2. Descripción de los equipos(que se planea adquirir o están en uso)(en miles de $).

EQUIPO	JUSTIFICACIÓN	RECURSOS*		TOTAL
		UPB	Otras Fuentes	
Portátil	Degradación de equipo propio	$0	$1.000.000	$1.000.000
Servidor	Alquiler	$0	$2.000.000	$2.000.000
TOTAL		$0	$3.000.000	$3.000.000

** indique si el valor es por a) compra b) depreciación de equipo propio o c) alquiler*

Tabla 3: Descripción de software (en miles de $).

SOFTWARE	JUSTIFICACIÓN	RECURSOS		TOTAL
		UPB	Otras Fuentes	
HexaDialer	Alquiler	$0	$500.000	$500.000

HexaHUD	Alquiler	$0	$500.000	$500.000
Plataforma e-learning	Alquiler	$0	$1.000.000	$1.000.000
TOTAL		$0	$2.000.000	$2.000.000

Tabla 4: Descripción de material bibliografico (en miles de $).

Material bibliográfico	**JUSTIFICACIÓN**	**RECURSOS**		**TOTAL**
		UPB	**Otras Fuentes**	
Artículos Científicos	Compra	$200.000	$0	$200.000
Material Técnico	Compra	$0	$500.000	$500.000
TOTAL		$200.000	$500.000	$700.000

Tabla 5: Descripción de viajes(en miles de $).

Viajes	**JUSTIFICACIÓN**	**RECURSOS**		**TOTAL**
		UPB	**Otras Fuentes**	
TOTAL		$0	$0	$0

9 Propiedad Intelectual y Confidencialidad

La titularidad de los derechos de propiedad intelectual se determinará de conformidad con el Estatuto de Propiedad Intelectual de la Universidad Pontificia Bolivariana y las leyes vigentes sobre la materia. En todo caso, los derechos morales corresponderán siempre a los creadores del Proyecto de Grado y éstos serán debidamente reconocidos para cualquier uso que se haga de la creación intelectual de que se trate.

Se recomienda guardar reserva de la información confidencial relativa al Proyecto de Grado, pues tal reserva puede ser fundamental para efectos de la protección de las creaciones intelectuales derivadas del mismo, por la vía de la propiedad intelectual.

Declaración de Privacidad del Archivo de Formulación
¿Es Privado el Archivo de Formulación? (Marque con una X)

X	SI, este documento sólo puede ser visto por los participantes en el proyecto y coordinadores
	NO, cualquiera puede ver el archivo en la web

10 Concepto ético

Aunque no se realizará experimentación directa con humanos o animales, el proceso de experimentación y validación podrá requerir consentimiento informado, para lo cual el proyecto se acogerá a las normas que rigen esta actividad y se informará a cada participante del proceso. En particular, durante la ejecución del proyecto se trabajará con niveles éticos que sirvan como soporte para la obtención de productos y que reflejen la necesidad de incluirlos en los procesos de estructuración y desarrollo del mismo. Se tendrán en cuenta los siguientes conceptos:

- Respetar las fuentes en el proceso de interpretación, presentación y divulgación, acatando, si se solicita, condiciones de confidencialidad y anonimato.
- Respeto por los derechos de autor, referenciando en todo momento a los autores de los documentos que de alguna manera contribuyan al trabajo investigativo y a los experimentos.
- Tratar adecuadamente las fuentes de información, ya sean escritas o digitales, en lo que tiene que ver con manipulación, análisis y copyright, teniendo en cuenta que algunas pueden corresponder a documentos importantes para la historia y el desarrollo de las empresas facilitadoras.
- Realizar la experimentación de acuerdo con las normatividades medioambientales que sean pertinentes en el desarrollo de la investigación.

- Mantener un alto grado de confidencialidad entre el grupo de trabajo para evitar las filtraciones de información que puedan mal interpretarse en círculos ajenos al proceso investigativo.
- Respeto por el usuario como receptor de los productos, en lo relacionado con la calidad y fiabilidad de los mismos.

11 Bibliografía

Decisión 351 (1993). Decisión 351 de 1993 de la Comunidad Andina de Naciones. Recuperado: http://www.ins.gov.co/normatividad/Decisiones/DECISION%20351%20DE%201993%20DE%20LA%20COMUNIDAD%20ANDINA%20DE%20NACIONES.pdf?Mobile=1&Source=%2Fnormatividad%2F_layouts%2Fmobile%2Fview%2Easpx%3FList%3D2ce58563%252D79fd%252D4769%252D8c5e%252D3a742c40a659%26View%3Deff26a98%252Dfa3e%252D4727%252D957d%252D66b0ab29e9ed%26CurrentPage%3D1. 20 de octubre de 2017.

Ley 222 (1995). Ley 222 de Colombia de 1995. Recuperado: http://www.secretariasenado.gov.co/senado/basedoc/ley_0222_1995.html#top. 20 de octubre de 2017.

Berners-Lee, T., Fielding, R. y Frystyk, H. (1996). Hypertext Transfer Protocol -- HTTP/1.0, RFC1945. Recuperado: https://tools.ietf.org/html/rfc1945. 2 de marzo de 2017.

Fielding, R., Gettys, J., Mogul, J., Frystyk, H., Masinter, L., Leach, P. y Berners-Lee, T. (1999). Hypertext Transfer Protocol -- HTTP/1.1, RFC2616. Recuperado: https://tools.ietf.org/html/rfc2616. 2 de marzo de 2017.

Nielsen, H., Leach, P. y Lawrence, S. (2000). An HTTP Extension Framework, RFC2774. Recuperado: https://tools.ietf.org/html/rfc2774. 2 de marzo de 2017.

Ley 599 (2000). Ley 599 del 2000 de Colombia. Recuperado: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388. 20 de octubre de 2017.

Jackson, C. y Barth, A. (2008). ForceHTTPS: Protecting High-Security Web Sites from Network Attacks, ACM. p.1-9. Recuperado: https://crypto.stanford.edu/forcehttps/. 20 de marzo de 2017.

CRAMM (2002). Análisis y Gestión de Riesgos CRAMM. Recuperado: https://www.sans.org/reading-room/whitepapers/auditing/qualitative-risk-analysis-management-tool-cramm-83. 20 de noviembre de 2017.

EBIOS (2003). Metodología de Gestión de los Riesgos EBIOS. Recuperado: https://www.ssi.gouv.fr/archive/es/confianza/documents/methods/ebiosv2-methode-plaquette-2003-09-01_es.pdf. 20 de noviembre de 2017.

Baz, I., Bonilla, J., Gorrotxategi, G., Ibarra, S., Santamaría, D. y Ruiz, I. (2009). Introducín a la VoIP y Asterisk Irontec. Recuperado: http://paginaspersonales.deusto.es/igor.ira/teaching/courses/voip_irontec_november_2009/igor.ira_Introduccion_a_la_VoIP_y_Asterisk.pdf. 20 de nobiembre de 2017.

Ley 1273 (2009). Protección de la información y de los datos TIC. Recuperado: http://www.mintic.gov.co/portal/604/articles-3705_documento.pdf. 21 de octubre de 2017.

Brooks, R. y Deng, J. (2010). Lies and the Lying Liars that Tell Them: A Fair and Balanced Look at TLS - Holcombe Department of Electrical and Computer Engineering, ACM. p. 1-3.

Benton, k., Jo, J. y Kim, Y. (2011). SignatureCheck: A Protocol to Detect Man-In-The-Middle Attack in SSL, ACM. p. 1-4.

MEHARI (2010). Metodología de Análisis y gestión de Riesgos MEHARI. Recuperado: http://meharipedia.x10host.com/wp/wp-content/uploads/2016/12/MEHARI-2010-IntroduccionESP.pdf. 20 de noviembre de 2017.

Gutiérrez, R. (2010). Seguridad en VoIP:Ataques, Amenazas y Riesgos. Universidad de Valencia. Recuperado: http://www.it-docs.net/ddata/896.pdf. 21 de marzo de 2018.

Ley 1450 (2011). Plan Nacional de Desarrollo y Plan de Inversiones 2011-2014. Recuperado: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=43101. 20 de octubre de 2017.

Mavrogiannopoulos, N., Vercauteren, F., Velichkov, V. y Preneel, B. (2012). A Cross-Protocol Attack on the TLS Protocol, ACM. p. 1-11.

Dacosta, I., Ahamad, M. y Traynor, P. (2012). Trust No One Else: Detecting MITM Attacks Against SSL/TLS Without Third-Parties. Recuperado: https://w ww.cise.ufl.edu/~traynor/papers/dacosta-esorics12.pdf. 2 de septiembre de 2016.

Hodges, J., Jackson, C. y Barth, A. (2012). HTTP Strict Transport Security (HSTS) RFC6797. Recuperado: https://tools.ietf.org/html/rfc6797. 15 de febrero de 2017.

Ley 1581 (2012). Disposiciones generales para la protección de datos personales. Recuperado: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=49981. 21 de octubre de 2017.

Rodríguez. A. J. (2013). Man in the Middle Attacks on SSL/TLS (Tesis de Maestría). Universidad autónoma de Barcelona. Recuperado de

http://openaccess.uoc.edu/webapps/o2/bitstream/10609/18443/6/acaroalTFM0113memoria.pdf. 4 September de 2016.

Sugavanesh, B., Prasath, H. y Selvakumar, S. (2013). SHS-HTTPS Enforcer: Enforcing HTTPS and preventing MITM Attacks, ACM. p. 1-4.

OWASP (2013). OWASP Top 10 for 2013. Recuperado: https://www.owasp.org/images/5/5f/OWASP_Top_10_-_2013_Final_-_Espa%C3%B1ol.pdf. 15 de marzo de 2017.

Barhoum, K. y Muhsen, Z. (2013). Risks and Remedies in ISRA University E-Learning System, iJET. p.39-42.

Ley 1712 (2014). Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional. Recuperado: http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=56882. 22 de octubre de 2017.

Wang, J., Yang, Y., Chen, L., Yang, G., Chen, Z. y Wen, L. (2015). A Combintion of Timing Attack and Statistical Method to Reduce Computational Complexities of SSL/TLS Side-Channel Attacks. 11th International Conference on Computational Intelligence and Security, IEEE. p. 1-5.

Eldewahi, A., Sharfi, T., Mansor, A. y Mohamed, N. (2015). SSL/TLS Attacks: Analysis and Evaluation. International Conference on Computing, Control, Networking, Electronics and Embedded System Engineering, IEEE. p. 1-6.

LeonardoNev (2015). SSLStrip version to defeat HSTS. Recuperado: https://github.com/LeonardoNve/sslstrip2. 17 de febrero de 2017.

Romero, D. (2015). Awesome-web-hacking. Recuperado: https://github.com/infoslack/awesome-web-hacking#tools. 15 de marzo de 2017.

Belshe, M., Peon, R. y Thomson, M. (2015). Hypertext Transfer Protocol Version 2 (HTTP/2), RFC7540. Recuperado: https://tools.ietf.org/html/rfc7540. 2 de marzo de 2017.

Han, S., Kwon, H., Hahn, C., Koo, D. y Hur, J. (2016). A Survey on MITM and its Countermeasures in the TLS Handshake Protocol. Department of Computer Science and Engineering, IEEE.p. 1-6.

Santiso, H., Koller, J. y Bisaro, M. (2016). Seguridad en Entornos de Educación Virtual. Recuperado: http://www.um.edu.uy/docs/Seguridad_en_entornos_de_educacion_virtual.pdf. 21 de marzo de 2018.

Guitierrez, J. (2017). Grupo Nethexa S.A.S. Recuperado: https://nethexa.com/. 21 de octubre de 2017.

Torres y Rojas (2017). Modelo de Gestión de Riesgos Aplicando Metodología Octave Allegro en entidades del Sector Fiduciario. Recuperado:

https://auditoriauc20102mivi.wikispaces.com/file/view/Metodolog%C3%ACas+deGesti%C3%B2n+de+Riesgos.pdf. 21 de noviembre de 2017.

SGSI (2017). Sistemas de Gestión de la Seguridad de la Información. Recuperado: http://www.mintic.gov.co/gestionti/615/w3-article-5482.html. 22 de octubre de 2017.

MSPI (2017). Modelo de seguridad y privacidad de la información Colombiano. Recuperado: http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html. 21 de noviembre de 2017.

O-ISM3 (2017). Information security management maturity standard. Recuperado: http://www.ism3.com/node/42. 20 de noviembre de 2017.

12 Posibles evaluadores

1. Nombre	
Título de posgrado	Christian Obando
Entidad	UPB
E-mail	christian.obando@upb.edu.co
Teléfono fijo	
Celular	3146730886
Grupo de investigación/ Empresa donde labora	UPB
2. Nombre	
Título de posgrado	Javier Contreras
Entidad	COMFAMA
E-mail	javier.contreras@upb.edu.co
Teléfono fijo	
Celular	3158949643
Grupo de investigación/ Empresa donde labora	COMFAMA
3. Nombre	
Título de posgrado	Carlos Cerón
Entidad	COMFAMA
E-mail	carloscu@comfama.com.co
Teléfono fijo	
Celular	3117691973
Grupo de investigación/ Empresa donde labora	COMFAMA