Universidad CENFOTEC

Maestría en Ciberseguridad

Documento Final de Proyecto de Investigación Aplicada 2

Evaluación de Vulnerabilidades de la Infraestructura Tecnológica de la SUPEN

Pugh Vose Kareem Augusto

Septiembre, 2017

Declaratoria de derechos de autor

Dedicatoria

Doy gracias a Dios, a mis padres y a mi esposa, los cuales son pilares fundamentales de motivación, valores y ejemplo para seguir adelante con mis proyectos.

También para la Superintendencia de Pensiones y al Banco Central por todo el apoyo y oportunidad brindada durante todo este tiempo. A los compañeros de trabajo y la Universidad, así como a los profesores, donde sus ideas y recomendaciones, ayudaron para la realización de este proyecto.

Tabla de contenido

Índice de figuras

Índice de tablas

Abstract

Se evaluarán en este documento, las vulnerabilidades de la infraestructura de la SUPEN, el alcance de esta evaluación será únicamente para servidores físicos y virtuales, ambos en la red interna. Debido a las diferentes necesidades, la SUPERINTENDENCIA DE PENSIONES de COSTA RICA (SUPEN), el cual regula y supervisa el régimen de pensiones del país, tiene una arquitectura en tierra y también en la nube, el cual es Azure proveído por Microsoft Cloud Computing.

En referencia a los términos de telecomunicaciones, entre la arquitectura en tierra y en Azure, se tiene una conexión VPN que une ambas redes usando un servicio de Azure VPN Gateway y un dispositivo CISCO ASA en el perímetro de la tierra.

El resultado de este documento creará un plan de remediación para mitigar las vulnerabilidades encontradas. Para obtener los resultados anteriores, se tienen fases que deben ser ejecutadas usando la metodología seleccionada, la cual es (Technology, National Institute of Standards and Technology, 2008) para poder llegar a concluir la evaluación.

Capítulo 1: Introducción

Actualmente, Internet es una infraestructura que almacena o publica información para todo tipo de organizaciones. Esta se enfrenta día a día a las diferentes amenazas de seguridad y privacidad que surgen cuando se detectan o publican las vulnerabilidades de los productos utilizados para brindar servicios. La intención de esta investigación es analizar y evaluar los equipos físicos y virtuales que soportan y ejecutan procesos de los sistemas de información de la SUPEN para brindar varios servicios hacia los clientes externos e internos. En este proceso, se utilizarán herramientas aprendidas en los diferentes cursos de la carrera y otras no utilizadas previamente.

La investigación se concentrará en la infraestructura de tierra (OnPremise) y en la nube (Azure Cloud) los cuales son lugares donde SUPEN posee sus computadores.

Para realizar esta evaluación, se utilizará la revisión de literatura (Kitchenham, 2007) dónde se utilizó la guía descrita para la identificación de material para desarrollar el contenido del trabajo. Se utilizarán revistas e informes de conferencias de tecnología consultadas en la base de datos de la IEEE, ACM y de la EBSCO, aparte de las prácticas recomendadas por organizaciones como la SANS, NIST, junto con otras. Toda la documentación recolectada se utilizará para mejorar los procesos de análisis y evaluación de la infraestructura tecnológica.

Antecedentes

La Superintendencia de Pensiones nace en agosto del año 1996, producto de la aprobación de la Ley del Régimen Privado de Pensiones Complementarias y sus reformas, No. 7523. Esta ley autorizó la creación de los sistemas o planes privados de pensiones complementarias y de ahorro individual, destinados a brindar a los beneficiarios protección complementaria ante los riesgos de invalidez, vejez y muerte.

Durante los primeros cuatro años de existencia, el objetivo principal de la entidad fue la regulación y fiscalización del régimen de capitalización individual, constituido por operadoras de pensiones complementarias (OPC).

En febrero de 2000, con la aprobación de la Ley de Protección al Trabajador, No. 7983, su ámbito de acción varió considerablemente. Quedaron bajo la supervisión de la SUPEN, los regímenes básicos de pensiones, tanto el Régimen de Invalidez, Vejez y

Muerte de la Caja Costarricense de Seguro Social (CCSS) como los regímenes especiales sustitutos de este, los fondos complementarios de pensiones creados por leyes especiales o convenciones colectivas, el Régimen No Contributivo de la CCSS, así como el Régimen de Riesgos de Trabajo.

Por otra parte, a la SUPEN le fue encargada la regulación y supervisión de los nuevos regímenes que creó la Ley de Protección al Trabajador, a saber: el Régimen Obligatorio de Pensiones Complementarias, los Fondos de Capitalización Laboral, el Ahorro Voluntario y el Régimen Voluntario de Pensiones Complementarias, ambos basados en sistemas de capitalización individual. Además, la nueva ley le asignó la obligación de velar por el otorgamiento de los beneficios a los afiliados al sistema de pensiones por parte de las entidades autorizadas, regímenes básicos y fondos creados por leyes especiales, aspecto que no estaba contemplado en la legislación anterior.

A finales del año 2002, la Ley de Contingencia Fiscal, Ley No. 8343 del 18 de diciembre de 2002, modificó la Ley 7523 en su artículo 36, para encargar a la SUPEN la supervisión de la labor realizada por la Dirección Nacional de Pensiones del Ministerio de Trabajo y Seguridad Social, en el otorgamiento de las pensiones con cargo al presupuesto nacional, en relación con la legalidad y oportunidad de las resoluciones y en lo relativo a las modificaciones y revalorizaciones de las pensiones que son competencia de la mencionada Dirección.

Con la aprobación de la Ley Reguladora del Mercado de Seguros, Ley 8653, se recargó en la Superintendencia de Pensiones, por un periodo de dieciocho meses o antes, si las circunstancias así lo permitieran, las facultades, deberes, obligaciones, funciones y responsabilidades establecidas a la Superintendencia General de Seguros (SUGESE). Adicionalmente, la SUGESE asumió la supervisión del Régimen de Riesgos de Trabajo. A partir del 1 de enero de 2010 se nombra superintendente para la SUGESE, con lo que finaliza el recargo en la SUPEN.

La SUPEN se ha transformado en el tiempo y ha sido constante en la búsqueda del mejoramiento continuo, prueba de ello es la certificación en la norma INTE-ISO 9001-2000, la cual fue otorgada en el año 2008 y ha sido producto del esfuerzo de esta gran familia de colaboradores.

Recientemente, en el año 2015, el Área de Tecnologías de Información de los Órganos de Desconcentración Máxima del Banco Central de Costa Rica, sufrieron un cambio significativo en su estructura organizacional, estas pasaron a ser parte del Departamento de Servicios Tecnológicos (DST) del Banco Central de Costa Rica. A nivel funcional, se manejan de la misma manera, con la diferencia de que ahora los colaboradores están en equipos de trabajo según especialidad.

Descripción del problema

Como se define en los procesos del (SUPERINTENDENCIA DE PENSIONES, COSTA RICA, 2014), el área de Tecnologías de Información debe proveer los recursos necesarios y a tiempo para que las demás áreas puedan realizar sus actividades diarias, con el fin de que la institución pueda cumplir con los objetivos establecidos en el (SUPERINTENDENCIA DE PENSIONES, COSTA RICA, 2015). Este proceso debe garantizar que la infraestructura actual pueda estar en capacidad de proveer la integridad, confidencialidad y disponibilidad en los sistemas de información.

Actualmente no se realizan escaneos de vulnerabilidad a lo interno de la infraestructura, pero se ejecutan procesos de parchado de servidores y revisiones periódicas. Lo anterior se considera como un proceso que mitiga vulnerabilidades básicas, ya que si los sistemas de información se ven expuestos ante alguna amenaza diferente a los que se vigilan, el impacto podría ser alto. La última revisión de vulnerabilidades, fue realizada hace más de tres años por parte de la empresa DELOITTE.

Para los sitios públicos, tales como SUPERINTENDENCIA DE PENSIONES, COSTA RICA (s.f.), SUPERINTENDENCIA DE PENSIONES, COSTA RICA (s.f.) y SUPERINTENDENCIA DE PENSIONES, COSTA RICA (s.f.), se realizan pruebas de penetración en coordinación con el área de Seguridad de la División de Servicios Tecnológicos del Banco Central de Costa Rica, por lo que estos servicios se consideran cubiertos.

Definición del problema

Debido a lo descrito en la sección de Descripción del Problema, la ejecución de una prueba de ejecución de vulnerabilidades ayudaría a la Institución a garantizar la

integridad, confidenciales y disponibilidad de los sistemas de información, reforzando la seguridad de ellas.

Justificación

La intención del proyecto es evaluar la infraestructura tecnológica de la SUPEN. De igual manera, se pretende verificar que esta misma infraestructura adapte las recomendaciones derivadas de las diferentes evaluaciones y mejores prácticas que publican los entes expertos, con el fin de mantener la seguridad de los sistemas de información, tanto para el cliente externo como las operadoras de pensiones, así como para los clientes internos, es decir, los funcionarios de la organización.

Viabilidad

Punto de vista técnico

Se cuenta con experiencia en la utilización de herramientas que puedan lograr cumplir el objetivo de esta investigación para la realización de las pruebas de evaluación de vulnerabilidades de la infraestructura tecnológica. En caso de requerir mayor apoyo, se consideraría utilizar documentación de los diferentes fabricantes de las herramientas, las cuales están disponibles en Internet.

Punto de vista operativo

Se pretende impactar, lo menos posible, la disponibilidad de los recursos de la Institución.

Punto de vista económico

Este proyecto, al ser desarrollado internamente, no se estima un costo monetario, sino temporal. La ejecución de ciertas tareas deberá ser en horario donde no se obstruyan las labores diarias de la Institución. Por otra parte, para las herramientas, se utilizarán varias de uso gratuito. En caso de que alguna herramienta requiera ser pagada, esta será evaluada y en caso de ver la necesidad de adquirirlo, será financiada por parte del desarrollador de este proyecto.

Objetivos

Se utiliza la taxonomía de Benjamin Bloom de 1956 para la definición de los objetivos, la cual, a través de los años ha demostrado ser una de las más robustas.

Objetivo general

Evaluar las vulnerabilidades de la infraestructura tecnológica de la SUPEN.

Objetivos específicos

- Identificar los activos que conforman parte de la infraestructura tecnológica.
- Explicar los tipos de análisis y evaluaciones que se realizarán a la infraestructura.
- Aplicar técnicas para evaluar la seguridad de la infraestructura.
- Analizar los resultados obtenidos de la evaluación de vulnerabilidades contra las recomendaciones o mejores prácticas de la industria.
- Proponer un plan de implementación para la mitigación de las vulnerabilidades encontradas en el proceso de evaluación con el fin de incrementar la seguridad de los sistemas de información que soporta la infraestructura tecnológica.

Alcances y limitaciones

Alcances

Este proyecto se concentrará únicamente en los equipos físicos y virtuales que se encuentran en la tierra (OnPremise) y en la nube (Azure). La metodología a utilizar será la que provee la NIST, que tiene procesos mínimos que son los necesarios para generar los resultados.

A continuación, se definen los entregables, los cuales se basan en la metodología y en los objetivos planteados:

Fase *Planeación*

- Informe de revisión de políticas para identificar brechas de seguridad.
- Matriz de responsabilidades para cada servicio.

Fase *Descubrimiento*

- Informe de los activos. Inventario de los activos que serán evaluados.
- Resultado del escaneo de puertos y servicios.

Fase *Evaluación*

- Informe de los resultados de las pruebas de vulnerabilidad.

Fase *Análisis*

- Resultados obtenidos de las pruebas ejecutadas.
- Matriz de comparación de resultados contra mejores prácticas de la industria.

Fase *Reporte*

- Plan de mitigación de las vulnerabilidades encontradas.
- Mapa de riesgos usando las diferentes bases de datos (CVE, s.f.) para los resultados encontrados.

Limitaciones

Las ejecuciones de las diferentes evaluaciones irán únicamente en función de lo definido en el objetivo general de esta investigación.

Marco de referencia organizacional y socioeconómico

Tipo de negocio

La institución objeto de estudio es de carácter público y su función es supervisar y regular el Sistema Nacional de Pensiones.

Mercado meta

El mercado meta es el Sistema Nacional de Pensiones.

Misión

Promover pensiones dignas. (SUPERINTENDENCIA DE PENSIONES, COSTA RICA, 2015).

Visión

Ser un referente técnico en el fortalecimiento del Sistema Nacional de Pensiones. (SUPERINTENDENCIA DE PENSIONES, COSTA RICA, 2015)

Valores

Integridad: actuamos con rectitud para cumplir con nuestros compromisos. (SUPERINTENDENCIA DE PENSIONES, COSTA RICA, 2015)

Transparencia: informamos con claridad, veracidad y oportunidad sobre nuestras actuaciones. (SUPERINTENDENCIA DE PENSIONES, COSTA RICA, 2015)

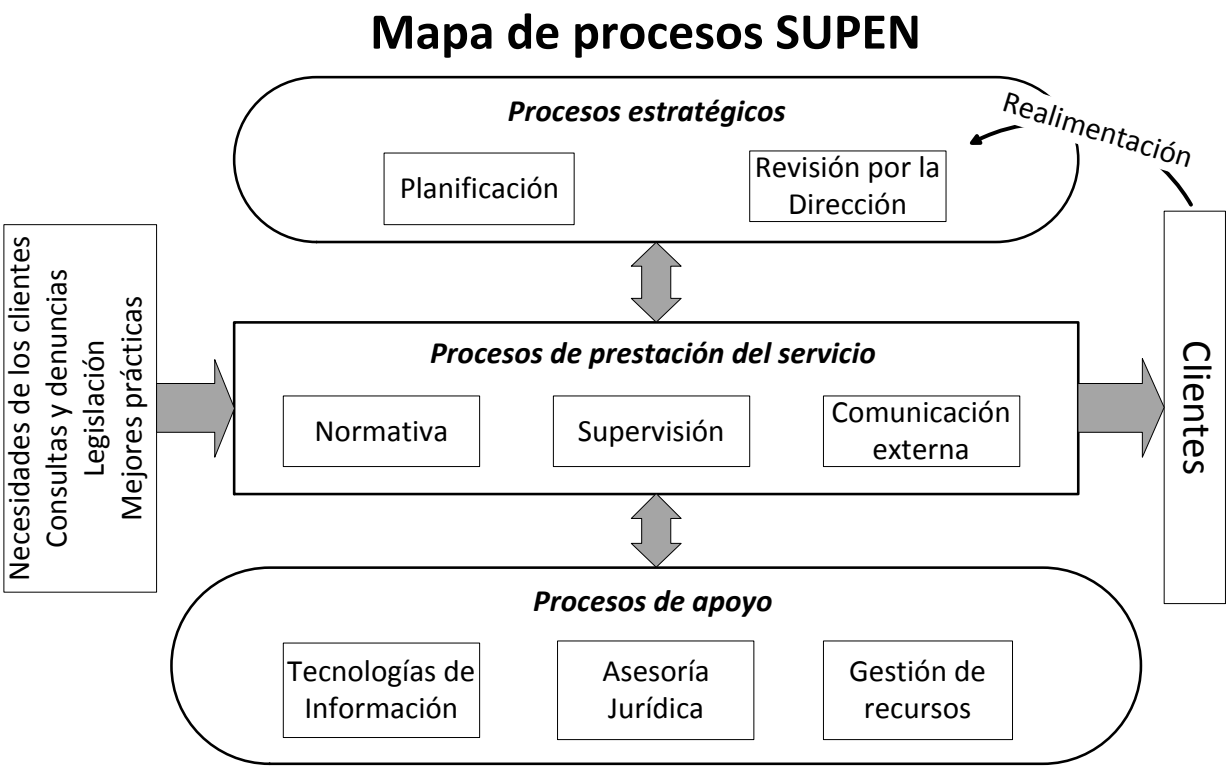
Mejora continua: promovemos el uso de mejores prácticas para brindar servicios de alta calidad a nuestros clientes. (SUPERINTENDENCIA DE PENSIONES, COSTA RICA, 2015)

Trabajo en equipo: laboramos de manera coordinada, en un ambiente de respeto y cordialidad, para alcanzar los objetivos de la organización. (SUPERINTENDENCIA DE PENSIONES, COSTA RICA, 2015)

Políticas institucionales

La SUPEN cuenta con políticas establecidas para cada proceso, las cuales se alinean con los planes estratégicos de la organización. En la Figura 1 se describen conceptualmente las interrelaciones de los procesos de la organización.

Figura 1. Mapa de procesos de SUPEN



Fuente: Manual de Calidad de SUPEN

Capítulo 2: Marco Conceptual

El desarrollo de este capítulo se realizará utilizando la metodología establecida en la Technology, National Institute of Standards and Technology (2008). Esta metodología indica “This guideline has been prepared for use by federal agencies. It may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright, though attribution is desired” Technology, National Institute of Standards and Technology (2008), por lo que se ajusta con el proyecto por ejecutar.

La metodología tiene la ventaja de minimizar el riesgo en las pruebas y además, es un proceso que fácilmente puede ser repetible y documentable, que también permite el desarrollo de políticas de seguridad personalizadas.

A continuación, se definirán algunos tipos de amenazas existentes actualmente.

Tipos de amenazas

Hacking

El hacking lo llevan a cabo personas con alto conocimientos en tecnologías de información, las cuales utilizan ese conocimiento para vulnerar sistemas de información con o sin buenas intenciones.

Tipos de hacker

Black hat: Tipo de hacker que vulneran los sistemas de información para extraer información que luego publican o comercializan.

Grey hat: Tipo de hacker que vulnera la seguridad de una organización para luego ofrecer sus servicios de protección.

White hat: Tipo de hacker con lo que se llaman con buenas intenciones, estos vulneran los sistemas de información para ayudar a corregir fallos.

Script kiddies

Hacker sin experiencia ni conocimiento que utiliza herramientas de hacker experimentados.

Phreakers

Personas que realizan ataques a compañías telefónicas, con el fin de obtener llamadas gratis.

Pharming

Consiste en redirección de sitios Web por medio de cambio en los registros de DNS, que al llegar al sitio para luego robar las credenciales o datos.

Phishing

Técnica para robar datos sensibles de los usuarios, por medio de clonación o falsificación de sitios. Estos sitios llegan a los usuarios por medio de correos

Ransomware

Código malicioso que encripta los datos del cliente a cambio de una recompensa.

Spyware

Código malicioso que recopila información de un usuario sin consentimiento.

Malware

Software dañino o malicioso.

Worm

Software malicioso que se auto reproduce e infecta a los equipos y son capaces de ser distribuido en toda la red de la organización.

Spoofing

Consiste en la aplicación de técnicas para suplantar la identidad.

Keylogger

Consiste en registrar todas las acciones ejecutadas de un teclado.

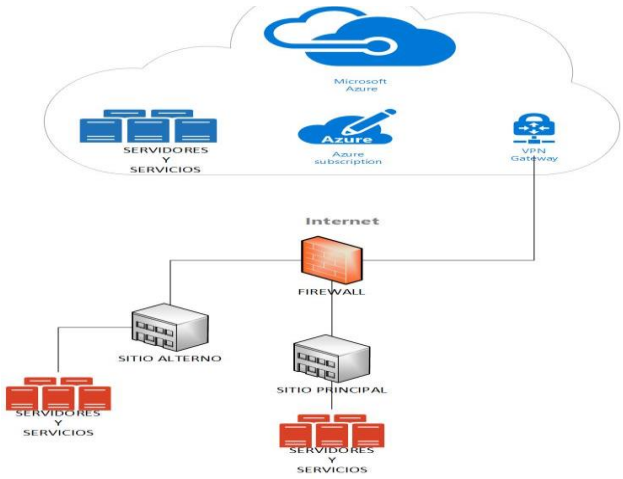
Ingeniería social

Consiste en técnicas de manipulación a usuarios para obtener información sensible o privilegiada.

Infraestructura actual

Se puede observar en la Figura 2, el diseño real de la infraestructura que posee la SUPEN, donde se tiene en realidad tres sitios, un sitio principal que está situado propiamente en la SUPEN, un segundo sitio remoto ubicado en algún lugar del país y por último el Azure, este se ubica en la infraestructura de Microsoft. Este último sitio, tiene la ventaja que está distribuido geográficamente, por lo que posee alta disponibilidad de los recursos.

Figura 2. Diseño de arquitectura de la SUPEN



Azure

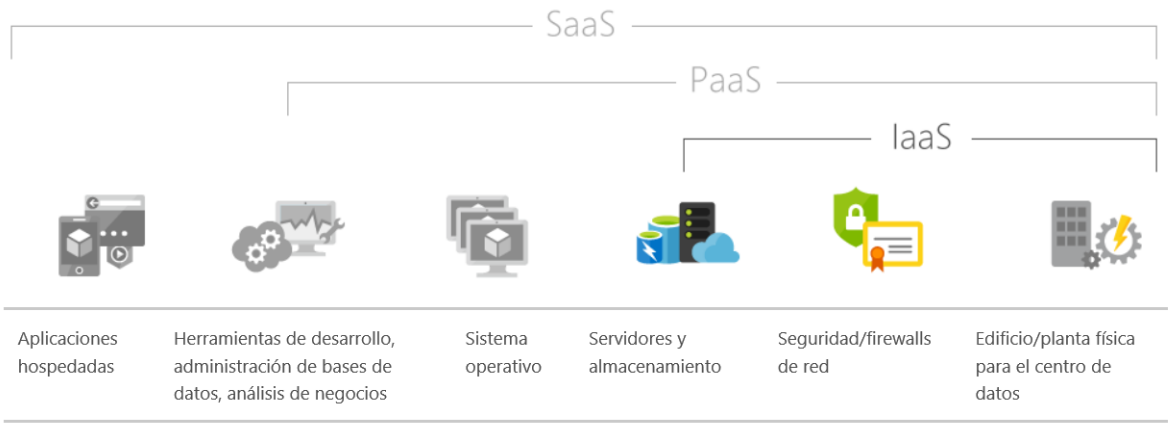
Los fabricantes han ido desarrollando su negocio bajo estas mismas normas con las nuevas tendencias tecnológicas, esto con el fin de ser utilizado bajo uso propio o venta de servicios. La computación en la nube ha sido un tema que se maneja en el lenguaje de las tecnologías de información, donde las diferentes organizaciones evalúan cuáles servicios de la nube son los que requieren.

La SUPEN incorporó esta tendencia del fabricante Microsoft, quienes desarrollaron Azure, el cual se enfoca en brindar diferentes servicios según lo requerido por los clientes. En Azure se manejan varios conceptos que nacen a raíz de los diferentes tipos de servicios que se ofrecen, según se observa en la Figura 3. A continuación, una breve definición de estos conceptos:

- IaaS (Infraestrucura como servicio): “es una infraestructura informática inmediata que se aprovisiona y administra a través de Internet. Permite reducir o escalar verticalmente los recursos con rapidez para ajustarlos a la demanda y se paga por uso.” (Microsoft, s.f.)
- PaaS (Plataforma como servicios): “es un entorno de desarrollo e implementación completo en la nube, con recursos que permiten entregar todo, desde aplicaciones sencillas basadas en la nube hasta aplicaciones empresariales sofisticadas habilitadas para la nube.” (Microsoft, s.f.)
- SaaS (Software como servicio):” permite a los usuarios conectarse a aplicaciones basadas en la nube a través de Internet y usarlas. Algunos ejemplos comunes son el correo electrónico, los calendarios y las herramientas ofimáticas (como Microsoft Office 365).” (Microsoft, s.f.)

Servicios según definición:

Figura 3. Servicios según definición de términos de computación en la nube.



Fuente: Microsoft (s.f.c.).

Proceso de planeación

Según se indica en la sección 6 de Technology, National Institute of Standards and Technology (2008), esta fase es de suma importancia, debido a que provee una guía de cómo crear, ejecutar priorizar las tareas para la evaluación de las vulnerabilidades.

Las actividades principales para esta etapa tal como las plantea la metodología son:

Desarrollar una política de evaluación de la seguridad:

- Esta política debe identificar las necesidades de la evaluación de la seguridad.
- Informar a todo el personal externo e interno.
- Debe ser revisada periódicamente.
- Matriz de roles y responsabilidades

Priorizar y calendarizar evaluaciones:

- Seleccionar los sistemas a ser evaluados.
- Categorizar los sistemas.
- Analizar el impacto a los sistemas.
- Medir la complejidad de los sistemas a evaluar.
- Determinar los componentes que serán evaluados.

- Indicar la periodicidad de las evaluaciones.

Seleccionando y personalizando pruebas técnicas y técnicas de examinación

- Basada en riesgos a los sistemas.
- Técnicas:
    - Revisión de documentación.
    - Revisión de la configuración de seguridad y reglas.
    - Descubrimiento de red y escaneo de vulnerabilidades.
    - Identificación de puertos y servicios.
    - Prueba de penetración interna/externa.
    - Revisión de bitácoras.

Logística de la evaluación:

- Considerar las habilidades del evaluador.
- Responsabilidades del evaluador:
    - Mantener informado al personal.
    - Desarrollar el plan de evaluación en conjunto con los administradores de los sistemas y jefaturas.
    - Analizar información recolectada y desarrollar recomendaciones de mitigación.
- Indicar las ubicaciones de las pruebas, herramientas y recursos:
    - Ambiente de pruebas.
    - Ambiente de producción.
    - Red.
    - Equipo.

Desarrollando el plan de evaluación:

- Determinar el tipo de evaluación del control de seguridad.
- Determinar los controles de seguridad y mejoras.
- Indicar la estrategia de evaluación.

Proceso de ejecución de la evaluación de la seguridad

Esta fase se ejecuta después de haber seleccionado las técnicas y métodos de evaluación. Esta sección indicará cuáles aspectos serán los que se deben considerar para este proceso de análisis.

Coordinación

- Mantener informado al personal.

Evaluando

Durante este proceso pueden registrarse incidentes, los cuales deben ser reportados y resueltos en los tiempos establecidos en los SLA de la organización. También hay otras barreras a la que se expone cada evaluador, como la resistencia a las evaluaciones por temas de disponibilidad, recursos y herramientas.

Análisis

Se categorizan en esta etapa, las vulnerabilidades y se determinan la causa del origen y la ejecución se lleva cabo con herramientas manuales y automáticas.

Manejo de los datos:

Esta sección indica los aspectos para mantener la integridad y confidencialidad de la información de los diferentes sistemas. A continuación, se especifica la consideración para este manejo:

Recolección de los datos:

Durante el proceso de evaluación, se recolectará información, así como las direcciones IP, nombres de equipos, sistemas operativos y las configuraciones y vulnerabilidades que poseen los mismos, por lo que se debe manejar con cuidado porque es información sensible de la organización. El manejo de la información recolectada para los resultados entregables, será lo más genérica posible, esto para reducir el riesgo de exposición de los activos.

Almacenamiento de los datos:

El resguardo de toda la información capturada del proceso de evaluación, será responsabilidad del evaluador protegerla y darle el uso adecuado. De igual manera, se presentarán los resultados ante los responsables de cada área para que estos sean aprobados por ellos, para tener el consentimiento de los resultados que irán en esta evaluación.

Transmisión de los datos:

La información será capturada usando las redes de la organización, por lo que no se expondrán al mundo exterior. En base en la Figura 2 de este documento, la información es protegida por la arquitectura actual.

Destrucción de los datos:

Al finalizar la evaluación, todos los documentos serán presentados a los responsables y ellos decidirán el tratamiento que se le dará a la información. En caso de que se decida destruir se aplicarían técnicas indicadas en Technology, National Institute of Standards and Technology (2008) para la destrucción de los datos.

Proceso post ejecución de actividades

Esta fase consistirá en presentar las vulnerabilidades encontradas y crear un plan de mitigación de estos, seguidamente se preparará un reporte y finalmente, la ejecución las recomendaciones para mitigar las vulnerabilidades y fortalecer la seguridad.

Recomendaciones de mitigación

Se intentará establecer, según se indica en la norma (Technology, National Institute of Standards and Technology, 2008), una estrategia para las pruebas de seguridad, esto para que se pueda seguir realizando periódicamente. Las recomendaciones generadas acá, podrán ser tanto técnicas como no técnicas (políticas, procesos, junto con otras). Se considerarán las recomendaciones de seguridad indicadas en National Institute of Standards and Technology (2013) para los diferentes controles.

Reporte

Los reportes generados van a contener la información completa del activo y tendrá asociado cada acción de mitigación de las vulnerabilidades. Este reporte servirá para llevar de mejor manera la trazabilidad de las acciones aplicados a cada servidor y servirá de plantilla para las futuras evaluaciones de vulnerabilidades a los equipos.

Remediación y mitigación

Todas las recomendaciones de remediación para esta sección, deben pasar previamente por el proceso de prueba antes de ser aplicadas en ambientes de producción, esto para minimizar el riesgo de que cuando se adopte alguna remediación, los equipos no se vean afectados, tanto por el rendimiento como por la usabilidad que se tiene definida. Esta práctica debe ser comunicada con las partes interesadas, tanto

para cambios técnicos como no técnicos y ser documentada. Cada proceso de remediación y mitigación tendrá que ser monitoreada con el fin de garantizar que las vulnerabilidades hayan sido subsanadas o bien, conocer el porcentaje de avance en la tarea.

Herramientas

Las herramientas para generar los resultados de esta evaluación, serán algunas de las mencionadas en el apéndice A de Technology, National Institute of Standards and Technology (2008), de igual manera, se investigarán otras según el análisis que se esté ejecutando a ese momento. Para determinar la efectividad de las herramientas, se usarán comparaciones que han hecho algunas instituciones de alta fidelidad como las publicadas en el reporte de Gartner (2015).

NMAP

Herramienta utilizada para escanear las redes y auditoría de seguridad. (Nmap, s.f.)

OPENVAS

Consiste en varios servicios y herramientas adicionales para escanear y gestionar las vulnerabilidades. (OpenVAS, s.f.)

ARMITAGE

Consiste en una serie de herramientas que visualiza los objetos y recomienda ataques a las posibles exposiciones de vulnerabilidad. (Kali Linux Tools, s.f.) Lo anterior para explotar vulnerabilidades. Esta herramienta al ser invasiva, se determinará si se utilizará en este proyecto, debido a que podría afectar algún servicio.

NEXPOSE

Solución de gestión de vulnerabilidades, que ayuda a reducir las exposiciones de las amenazas, de manera que prioriza los riesgos de las vulnerabilidades, configuraciones y controles. (Rapid7, s.f.)

NESSUS

En la

Tabla 1 se hace una comparación de algunas características que ofrece el software conocido para el desarrollo de este proyecto.

Tabla 1. Comparación de herramientas para el análisis de vulnerabilidades.

Herramienta	Licencia	Limitación de IPs	Exposición de datos	Escaneos
OpenVas	Gratis	No	No (Local)	Ilimitados
Nexpose	30 días	No	Sí (Nube)	Ilimitados
Nessus	7 días	Sí	No (Local)	Ilimitados
Qualys	Gratis	No	Sí (Nube)	Limitado

Fuente: Elaboración Propia

A continuación, en la Figura 4 se presenta el cuadrante mágico de Gartner, donde hace una comparación por pilar de los fabricantes de herramientas para el análisis de seguridad de aplicaciones.

Figura 4. Cuadrante mágico de Gartner de pruebas de seguridad en aplicaciones. Febrero 2017

Fuente: Jones (2017)

Capítulo 3: Marco metodológico

La gestión y evaluación de vulnerabilidades en una organización, deben ser continuas, debido a que es propiamente la autodefensa de la organización. En algunos reportes hechos por Gartner (Chuvakin & Barros, A Guidance Framework for Developing and Implementing Vulnerability Management, 2017), el cual es muy reciente, trata sobre la guía y la importancia sobre cómo llevar una buena gestión y evaluación de vulnerabilidades.

Gartner define la gestión de vulnerabilidad como “ciclo de procesos para descubrimiento, evaluación, remediación y mitigación de debilidades de seguridad en los sistemas de información” (Chuvakin & Barros, A Guidance Framework for Developing and Implementing Vulnerability Management, 2017).

Las vulnerabilidades que se encontraron en las organizaciones, se deben muchas veces a las herramientas y necesidades de negocio que demandan para ofrecer siempre un mejor servicio, según sea su giro comercial. Adicional a esto, la cultura organizacional puede ser cómplice de forma negativa o positiva a la seguridad de la misma. Todo lo anterior se debe tomar en consideración y cada servicio ser revisado según las recomendaciones o vulnerabilidades que poseen fuentes como OWASP (s.f.) o CVE (s.f.), que indican qué tipo de brecha de seguridad podría existir por tipo de producto disponible en la organización.

Tipo de investigación

Esta investigación es de tipo evaluativo, la cual conlleva la utilización de técnicas, herramientas y metodologías para determinar los tipos de riesgos o vulnerabilidades a las que está expuesta la infraestructura.

Alcance investigativo

El tipo de estudio utilizado en la recolección de los datos de la investigación es el evaluativo, debido a que se enfoca en la comparación de estado actual contra alguna omisión de alguna buena práctica recomendada.

Enfoque

El tipo de estudio utilizado será el evaluativo, porque el estudio busca identificar, analizar y corregir lo obtenido contra las recomendaciones de seguridad de los eventos

estudiados, que en el caso de la presente investigación, dichos eventos serían las vulnerabilidades o riesgos que podría tener la infraestructura tecnológica.

Diseño

El estudio parte de un ambiente donde se evalúa la infraestructura tecnológica ante posibles vulnerabilidades a las está sometida, sobre los sistemas de información de la SUPEN.

Población y muestreo

La investigación utilizará a la siguiente población para la recolección de datos:

- Director de TI: Se le realizarán consultas y se le mantendrá informado sobre cuáles servicios están siendo evaluados.
- Desarrolladores: Se les realizará consultas sobre las interrelaciones de los activos que utilizan y cómo los afectan.
- Administrador de bases de datos: Se le realizarán consultas sobre las interrelaciones de los activos que utiliza y cómo lo afectan.
- Usuarios finales expertos: Se les estará consultando para determinar si las pruebas están interfiriendo o reduciendo sus tareas diarias.

Instrumentos de recolección de datos

Se utilizará lo siguiente, con el fin de recolectar información precisa para la investigación:

- Entrevistas: Este instrumento permite el intercambio de información con los responsables de los servicios, las mismas deben ser estructuradas.
- Observaciones: Se pretende vigilar el comportamiento completo del servicio para verificar cuáles otros activos se utilizan.
- Evaluaciones de herramientas: Se debe comprender como funcionan las herramientas para poder hacer buen uso de ellas, permitiendo una mayor eficacia en su utilización.

Técnicas de análisis de la información

El enfoque de esta investigación, es cuantitativo, emplea mecanismos para evaluar las vulnerabilidades de la infraestructura de la Institución.

Estrategia de desarrollo de la propuesta

Fase de planeación

Se revisarán para esta fase, los documentos correspondientes a las políticas, procedimientos y guías institucionales del área de Tecnologías de Información, relacionados con la gestión de las vulnerabilidades, para luego hacer una tabla con estas y analizarlos posteriormente. Los ítems por revisar corresponden a las versiones o actualizaciones de los documentos y si están lo suficientemente completas, comparadas con las de las ODM y BCCR.

Los criterios de evaluación son los siguientes:

- Contiene lineamientos básicos de seguridad física y lógica.
- Contienen lineamientos de funciones y deberes.
- Protege activos.
- Controles de acceso.
- Incluye pasos técnicos.
- Delimita el ámbito de acción.
- Indica la herramienta a utilizar.
- Monitoreo de ejecución de tareas.
- Periodicidad de tareas.

Figura 5. Clasificación de criterios de evaluación: políticas, procedimientos y guías

Nivel	Criterios de Cumplimiento
ALTA	=> 5 criterios
MEDIA	< 5 y >= 3 criterios
BAJA	<= 2 criterios

Fuente: Elaboración propia.

En la *Figura 5* se muestra la forma en que se clasificarán las políticas, procedimientos y guías según el criterio elegido previamente. La clasificación es esencial para posteriormente, realizar las recomendaciones en el capítulo de propuestas de este proyecto.

Categorización del riesgo:

Se clasifican, para la evaluación de las vulnerabilidades, de acuerdo con su nivel de riesgo, lo depende del nivel de ocurrencia o probabilidad y el impacto que este genere a la organización.

Impacto

- ✓ Alto: Afecta el cumplimiento de los objetivos de la organización, reputación, interrupción total o parcial de servicios críticos, su valor será de 3.
- ✓ Medio: Considera interrupción parcial de servicios no críticos de la organización, pero necesarios para la operativa, su valor será de 2.
- ✓ Bajo: Considera aspectos menores, pero en igual ocasión, una interrupción o retrasos de las tareas, procesos o servicios no críticos, su valor será de 1.

Probabilidad

- ✓ Baja: Se genera al menos una vez al año, su valor será de 3.
- ✓ Media: Se genera al menos una vez al semestre, su valor será de 2.
- ✓ Alta: Se genera al menos una vez al mes, su valor será de 1.

Figura 6. Clasificación de la probabilidad de ocurrencia

Valor	Probabilidad de Ocurrencia	Nivel
1	Incidencia de una vez al año	Bajo
2	Incidencia de una vez al semestre	Medio
3	Incidencia de una vez al mes	Alto

Fuente: Elaboración propia

Niveles de aceptación del riesgo

Figura 7. Nivel de aceptación de riesgo

Tabla Niveles de Riesgo		
MEDIO	ALTO	ALTO
BAJO	MEDIO	ALTO
BAJO	BAJO	BAJO

Fuente: Elaboración propia

Se ha designado la siguiente clasificación para el tratamiento de los riesgos, basados en la aceptación por parte de la organización. En la Figura 8 se muestra el nivel de tratamiento o aceptación de los riesgos por encontrar:

Figura 8. Nivel de tratamiento del riesgo

Nivel de Aceptación del Riesgo			
	TOLERABLE - MITIGAR	INACEPTABLE - MITIGAR	INACEPTABLE - MITIGAR
	ACEPTABLE	TOLERABLE - MITIGAR	INACEPTABLE - MITIGAR
	ACEPTABLE	ACEPTABLE	TOLERABLE - MITIGAR

Fuente: Elaboración propia

Identificación del riesgo

El proceso de identificación del riesgo que realiza la herramienta es usando la base de datos de conocimiento actualizada con las últimas definiciones. Este procedimiento se ejecutará según se determine su periodicidad y utilizarán la cantidad de activos de la organización que consideren necesarios.

Análisis del riesgo

Proporciona un elemento de entrada para la valoración del riesgo y para tomar decisiones acerca de si es necesario tratar los riesgos, así como las estrategias y los métodos de tratamiento del riesgo más apropiados.

El análisis del riesgo consiste en determinar las consecuencias y sus probabilidades para eventos de riesgo identificados, teniendo en cuenta la presencia (o no) y la eficacia de todos los controles existentes. Las consecuencias y sus probabilidades se combinan para determinar un nivel de riesgo y las escalas se definirán dentro de esta metodología.

Evaluación del riesgo

Se aplicará el conocimiento del riesgo obtenido de la herramienta en la evaluación del riesgo, para tomar decisiones sobre acciones futuras. Las consideraciones consideradas en el contexto serán insumos para la toma de decisiones.

Fase de evaluación

Etapa de descubrimiento

Se escanearán las cuatro (4) subredes en esta etapa, correspondientes a la infraestructura de servidores de la organización. Para esta primera fase, se debe hacer un listado de puertos abiertos. Este escaneo incluye información tanto de los servidores como de los equipos de telecomunicación, por lo que se debe discernir cuáles

direcciones IP corresponden a la infraestructura de servidores. Lo anterior será un insumo necesario para la fase de penetración.

Etapa de análisis de vulnerabilidades

La fase de análisis consiste en tomar los datos de la fase de descubrimiento y realizar la búsqueda de vulnerabilidades únicamente para la infraestructura de servidores. La evaluación contemplará a los servidores y a sus subcomponentes, como lo son iLO, Onboard Administrator y enclosure. La herramienta utilizada es el OpenVas, debido a que se cuenta con alta experiencia en su uso. Para la selección de la herramienta, se validaron algunas recomendaciones hechas por Gartner como Barros & Chuvakin (s.f.) (Chuvakin, Vulnerability and Security Configuration Assessment Solutions Comparison, 2014).

Fase pos-ejecución

Etapa de recomendación de remediación

Luego de haber completado la fase de planeación y la fase de evaluación, se procederá a revisar las vulnerabilidades con ponderación altas y medias para presentar una acción de remediación. Estas recomendaciones se harán de acuerdo con el grupo de puertos asociados a las vulnerabilidades encontradas. Esta etapa es la que se verá en el capítulo de propuestas.

Capítulo 4: Análisis de resultados

Se toman en este capítulo, las referencias de la metodología seleccionada, con el fin de lograr los objetivos declarados en este proyecto. Debido a que la metodología explica varios procesos, en varias de las fases por desarrollar y se ejecutarán los puntos que consideren necesarios utilizar. La razón por la que se explicó detalladamente la metodología, es para que sirva de base para futuras evaluaciones.

Fase de planeación

Se debe conocer, con base en su clasificación de riesgo para comenzar la evaluación de la infraestructura de SUPEN, un inventario de servicios que esta ofrece para sus clientes, internos y externos. El inventario de la Tabla 2 también contempla la cantidad de servidores que conlleva cada servicio:

Tabla 2.Clasificación de sistemas de información de SUPEN según riesgo

Sistema	Servidores requeridos	ALTO	MEDIO	BAJO
VES (Ventanilla Electrónica de Servicios)	6	X		
Sistema de trámites	4	X		
Help desk	2			X
Sistema de inventario	2			X
Sistema de gestión de personal	2			X
Página Web	2	X		
IDEA	1			X
Sistema de inversiones	3	X		
Sistema de afiliados	3	X		
TeamMate	2		X	
Active directory	3	X		
ADFS	2	X		
DFS	3	X		
SQL	5	X		
ORACLE	5	X		
Antivirus	1	X		
Firma digital	1	X		
DNS	4	X		

Fuente: Elaboración propia.

Como se deduce de la Tabla 2, alrededor de 65% de los sistemas de información que se hospedan y gestionan manualmente, tiene un alto riesgo y esto precisamente es debido a que las entidades externas y los clientes internos, demandan tener la información con una alta disponibilidad, integridad y confidencialidad para ser usados en gestiones de origen legal o bien informativo.

Siguiendo la metodología definida en este proyecto, en la Tabla 3 se muestra un listado de procedimientos, políticas y guías vigentes que posee la SUPERINTENDENCIA DE PENSIONES, COSTA RICA (s.f.).

Tabla 3. Políticas del sistema de gestión de calidad de SUPEN

Políticas		
Nombre	**Versión**	**Cumplimiento**
PG SUPEN 08 POLÍTICA DE SEGURIDAD INFORMÁTICA	2015	ALTA
PO 01 SUPEN Adm del Recurso Informático	2010	ALTA

Fuente: SUPEN

Tabla 4. Procedimientos del sistema de gestión de calidad de SUPEN

Procedimientos		
Nombre	**Versión**	**Completitud**

P TEI 03 Administración de red informática	2014	ALTA
P TEI 04 Administración de incidentes	2014	ALTA
P TEI 11 Continuidad de servicio y disponibilidad	2014	ALTA
P TEI 13 Seguridad de la información	2014	ALTA
P TEI 06 Administración de servidores	2013	ALTA
P TEI 14 Administración de la capacidad	2014	ALTA

Fuente: SUPEN

Tabla 5.Guías del sistema de gestión de calidad de la SUPEN

Guías		
GT TEI 13.1 Guía para elaboración de plan de seguridad	2014	MEDIA
GT TEI 13.2 Guía para atención de incidentes de seguridad	2014	MEDIA
GT TEI 13.3 Guía para gestión de riesgo de la seguridad informática	2014	ALTA
GT TEI 13.4 Guía detección de vulnerabilidades de seguridad y pruebas de penetración	2014	BAJA
GT TEI 03.4 Instalación de equipo informático	2014	BAJA
GT TEI 03.7 Detección de vulnerabilidades de seguridad.	2014	BAJA
GT TEI 03.8 Monitoreo y revisión de servidores y unidades de almacenamiento	2014	BAJA
GT TEI 03.9 Mantenimiento preventivo de equipos	2014	BAJA
GT TEI 03.20 Cambio de contraseñas de acceso	2014	BAJA

Fuente: Elaboración propia.

Las políticas de la Tabla 3, al ser evaluadas, constatan que estas deben ser actualizadas de acuerdo con los servicios brindados a hoy. También se ve que se deben separar algunos puntos e incorporarlos tanto a guías como a procedimientos, ya que su contenido o descripción es completamente técnico o de interés para el responsable del servicio.

A nivel de los procedimientos descritos en la Tabla 4, el cambio que requieren es menor, debido a que algunos pasos ya están considerados dentro de otros procedimientos y a la vez intersecan, por lo que solo habría que descartarlos en cualquiera de las guías que se consideren necesarios.

Las guías de la Tabla 5 explican que hacer ante cualquier incidente o solicitud, estas se compararon con las que aplican según servicio y se demuestra que se encuentran muy por detrás de las BCCR. Para un ejemplo rápido en el uso de herramientas, estas no especifican cuál emplear.

Tabla 6. Matriz RACI según área de trabajo.

Puesto	Cantidad	Seguridad	Sistemas	Red
Director	1	A	A	A
Base de datos	1	IC	RC	I
Servidores	1	R	C	C

Telecomunicaciones	1	R	C	R
Desarrolladores	4	I	R	I
Soporte usuario	1	R	I	I
Total	9			

Fuente Elaboración propia. R=responsable A=A cargo, C=consultado, I=informado

Como se muestra en la *Tabla 6* , la función de la seguridad es compartida entre varios funcionarios y es debido a que no se cuenta con un puesto de seguridad, a diferencia de las ODM y el BCCR. En estas dependencias tienen un área completa de seguridad, la cual vela a tiempo completo por este tema.

Fase de evaluación

Se ven varios procesos en esta fase, esto primero para identificar los activos que componen la infraestructura tecnológica y el otro, para evaluar qué vulnerabilidades presentaba cada activo.

En la etapa de descubrimiento, se procedió a detectar cuáles puertos de los equipos dentro del ámbito por evaluar, se encontraban expuestos.

Tabla 7. Puertos abiertos de los componentes de la infraestructura tecnológica (Servidores, SAN, iLO, OA)

Puerto	Total	Puerto	Total	Puerto	Total
21	**2**	**1040**	**1**	**8000**	**1**
22	**21**	**1045**	**1**	**8001**	**1**
23	**5**	**1048**	**0**	**8080**	**3**
25	**2**	**1050**	**1**	**8081**	**5**
53	**3**	**1352**	**1**	**8082**	**1**
80	**43**	**1433**	**7**	**8083**	**2**
81	**8**	**1500**	**1**	**8084**	**0**
82	**6**	**1501**	**1**	**8086**	**0**
83	**3**	**1521**	**7**	**8087**	**1**
84	**1**	**1801**	**2**	**8400**	**2**
88	**3**	**1947**	**1**	**8402**	**2**
111	**2**	**2030**	**2**	**8443**	**0**
113	**0**	**2049**	**0**	**9010**	**1**
135	**49**	**2103**	**2**	**9100**	**0**
139	**46**	**2105**	**2**	**14000**	**1**
161	**2**	**2107**	**2**	**17988**	**16**
389	**3**	**2179**	**13**	**49152**	**15**
427	**1**	**2301**	**1**	**49153**	**33**
443	**32**	**2381**	**1**	**49154**	**30**

Puerto	Total	Puerto	Total	Puerto	Total
445	50	2383	2	49155	20
464	3	2701	0	49156	12
515	0	2869	0	49157	12
593	4	3268	3	49158	3
631	0	3269	3	49159	2
636	3	3389	52	49160	3
843	1	3800	0	49161	4
1025	1	5500	1	49163	1
1026	3	5560	1	49165	1
1027	1	5988	1	49167	1
1028	2	5989	1		
		7627	0		

Fuente: Elaboración propia.

En la Tabla 7 se nota una considerable cantidad de puertos abiertos, los cuales corresponden a servicios desplegados y también la configuración por defectos de varios equipos. Los puertos de los servicios como DC, DFS, DNS, SQL, Analysis Services y RDP, por ejemplo, se aceptan sus condiciones de abiertos por su funcionalidad e interconexión.

La siguiente Tabla 8 contiene las cantidades y clasificación de acuerdo al riesgo de vulnerabilidades encontradas en cada red.

Tabla 8. Resumen de vulnerabilidades encontradas.

Red	Alto	Medio	Bajo
A	48	231	65
B	1	20	3
C	0	85	9
D	0	5	1
Total	49	341	78

Fuente: Elaboración propia

De las vulnerabilidades encontradas, se atenderán las que tienen riesgos, alto y medio, ya que según la Figura 8, deben ser mitigados. Sin embargo, se mencionarán todas las encontradas, para que se tenga conocimiento de los riesgos de la organización.

Tabla 9. Vulnerabilidades altas encontradas.

Vulnerabilidades
HP Onboard Administrator Multiple Security Vulnerabilities
IPMI Cipher Zero Authentication Bypass Vulnerability
OS End of Life Detection
Microsoft Windows SMB Server Multiple Vulnerabilities-Remote
Cisco Smart Install Protocol Misuse
Microsoft Internet Information Services Buffer Overflow Vulnerability
Microsoft IIS Web Server End of Life Detection
Microsoft IIS WebDAV Remote Authentication Bypass Vulnerability
Report default community names of the SNMP Agent
HTTP Brute Force Logins with Default Credentials Reporting
SSH Brute Force Logins with Default Credentials Reporting
HP Integrated Lights-Out Multiple Vulnerabilities

Fuente: Elaboración propia.

Tabla 10. Vulnerabilidades medias encontradas.

Vulnerabilidades
SSH Weak Encryption Algorithms Supported
DCE/RPC and MSRPC Services Enumeration Reporting
SSL/TLS: Report Weak Cipher Suites
SSL/TLS: Certificate Signed Using A Weak Signature Algorithm
SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability
SSL/TLS: Report Vulnerable Cipher Suites for HTTPS
SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
SSL/TLS: Di-e-Hellman Key Exchange Insufficient DH Group Strength Vulnerability
SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection
SNMP GETBULK Rejected DRDoS
Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability
HP Integrated Lights-Out XSS Vulnerability
SSL/TLS: OpenSSL TLS 'heartbeat' Extension Information Disclosure Vulnerability
Microsoft IIS Default Welcome Page Information Disclosure Vulnerability
Use LDAP search request to retrieve information from NT Directory Services
SSL/TLS: Missing `secure` Cookie Attribute
Missing `httpOnly` Cookie Attribute

Fuente: Elaboración propia.

Tabla 11.Vulnerabilidades bajas encontradas.

Vulnerabilidades
TCP timestamps
SSH Weak MAC Algorithms Supported
SSL/TLS: TLS/SPDY Protocol Information Disclosure Vulnerability (CRIME)

Fuente: Elaboración propia.

Las vulnerabilidades según su clasificación de las Tabla 9, Tabla *10* y Tabla 11, deben ser atendidas en un proceso coordinado con la administración para que se reduzca el riesgo ante la materialización de estos, especialmente las de riesgo alto y medio.

GPO

En la siguiente Tabla 12, se tiene la cantidad de políticas de usuario y equipo desplegado en la organización. El nivel de protección de ellas, es bastante alto y están sujetas a mejoras.

Tabla 12. Resumen de políticas de dominio.

Política	Cantidad
Usuarios	22
Computadoras	36
Total	58

Fuente: Elaboración propia.

VLAN

La cantidad de VLAN encontradas para, tanto los servidores en tierra como en nube, son planas, con esto se indica que solo existe una sola VLAN para la comunicación de todos los equipos entre sí. Se identifica que los respaldos, parchado, descargas de Internet, enlaces entre ODM y BCCR, conexión para sistemas con la nube e incluso computadoras especiales, lo anterior se menciona para ver la cantidad de equipos que usan solo esa VLAN para sus operaciones.

Firmware

Se revisaron los equipos físicos y se detectó que varios de estos no cuentan con la última versión. La actualización de este componente es esencial para varias cosas, la primera es para mejorar la seguridad y la segunda es para optimizar la capacidad o rendimiento de los mismos.

Es importante mencionar que los equipos son del mismo fabricante, con eso se puede tener mayor control sobre la versión y definición de guías para su uso. En la Tabla 13 se encuentran las versiones de firmware para los servidores, SAN, iLO e OA.

Tabla 13. Versiones de firmware encontradas.

Versión	Revisión	Año
A13	n/a	2008
A17	n/a	2009
I24	a	2009
I24	c	2009
1.20	n/a	2011
I24	c	2011
2.09	n/a	2012
TS2509003	n/a	2013
1.82	n/a	2015
I38	v1.40	2015
I38	v2.20	2015
I38	v2.30	2016

Fuente: Elaboración propia.

Capítulo 5: Propuesta

Políticas

La recomendación para las políticas definidas en la Tabla 3, luego de revisar estas, no se considera necesario algún cambio en los documentos. La categorización realizada para este documento tuvo un resultado de ALTA.

Procedimientos

Los procedimientos al igual que las políticas demuestran en la Tabla 4 los que tienen un resultado de ALTA, utilizando los criterios definidos en la metodología.

Guías

Todas las guías a nivel general, deber ser ajustadas y detalladas. Esta labor es extensa, por lo que se recomienda que cada área responsable elabore la suya. Los desarrollos de estas guías conllevan que durante el proceso se tengan que revisar las guías de otras dependencias, la decisión resultante sería unificarlas o bien, adoptar la que esté mejor definida.

Vulnerabilidades altas

Se atenderán en esta sección, las descripciones de las vulnerabilidades altas encontradas, así como la manera en que se establece mitigarlos.

HP Onboard Administrator Multiple Security Vulnerabilities

Descripción: Esta vulnerabilidad encontrada puede causar que un atacante obtenga información sensible y redirija al usuario a un sitio potencialmente malicioso utilizando el mecanismo de phishing.

Mitigación: Actualizar al último software disponible por parte del fabricante.

IPMI Cipher Zero Authentication Bypass Vulnerability

Descripción: La vulnerabilidad encontrada permite la desviación de la forma de autenticación, por lo que un atacante podría acceder el dispositivo y obtener información sensible.

Mitigación: Actualizar al último software disponible por parte del fabricante.

OS End of Life Detection

Descripción: Esta vulnerabilidad se refiere a los equipos con sistemas operativos obsoletos, tal es el caso de la familia Windows 7 y Windows Server 2003.

Mitigación: Coordinar y migrar el servicio a una versión de sistema operativo moderno.

Microsoft Windows SMB Server Multiple Vulnerabilities-Remote (4013389)

Descripción: Esta vulnerabilidad consiste en dar acceso a un atacante remoto para obtener la habilidad de ejecutar código en los equipos y es a falta de actualizaciones del sistema operativo y también permitir la divulgación de información.

Mitigación: Actualizar al último software disponible por parte del fabricante.

Cisco Smart Install Protocol Misuse

Descripción: Esta vulnerabilidad afecta a equipos de telecomunicación, permitiendo cambiar la configuración inicial del equipo, cargar una imagen o ejecutar comandos con privilegios altos.

Mitigación: Ejecutar el comando “no vstack” e incorporarlo a la configuración inicial de todos los equipos que tengan este protocolo.

Microsoft Internet Information Services Buffer Overflow Vulnerability

Descripción: El servicio de IIS es propenso a desbordamiento de buffer y podría ocasionar la ejecución arbitraria de código causando una denegación de servicio (DoS).

Mitigación: Coordinar y migrar el servicio a una versión de sistema operativo moderno.

Microsoft IIS Web Server End of Life Detection

Descripción: Esta vulnerabilidad se basa en que el servicio de IIS no se está actualizado, debido a la finalización de soporte del sistema operativo.

Mitigación: Coordinar y migrar el servicio a una versión de sistema operativo moderno.

Microsoft IIS WebDAV Remote Authentication Bypass Vulnerability

Descripción: La vulnerabilidad consiste en que el servicio IIS está configurado con el módulo WebDAV, el cual es propenso a desvíos en la autenticación, causando que un atacante pueda enviar caracteres UNICODE maliciosos y enviarlo al módulo.

Mitigación: Actualizar al último software disponible por parte del fabricante.

Report default community names of the SNMP Agent

Descripción: La vulnerabilidad asociada al protocolo Simple Network Management Protocol (SNMP) es la que la comunidad pública y privada configurada podría ser adivinada por un atacante y este podría leer y cambiar los datos del dispositivo.

Mitigación: Deshabilitar el servicio si el equipo no soporta SNMP v3.

HTTP Brute Force Logins with Default Credentials Reporting

Descripción: Esta vulnerabilidad consiste en que se logró autenticar al servicio remoto de aplicación Web, utilizando la técnica de fuerza bruta por defecto, con usuarios y contraseñas por defecto.

Mitigación: Renombrar la cuenta y cambiar la contraseña.

SSH Brute Force Logins with Default Credentials Reporting

Descripción: Esta vulnerabilidad encontrada, consiste en utilizar la técnica de fuerza bruta para ingresar al servicio remoto Secure Shell (SSH), mediante el uso de usuarios y contraseñas por defecto.

Mitigación: Renombrar la cuenta y cambiar la contraseña.

HP Integrated Lights-Out Multiple Vulnerabilities

Descripción: La vulnerabilidad consiste en la facilidad que se tiene configurado para propiciar múltiples vulnerabilidades y ataques remotos.

Mitigación: Actualizar al último software disponible por parte del fabricante.

Vulnerabilidades medias

Se atenderán en esta sección, las descripciones de las vulnerabilidades medias encontradas, así como la manera en que se establece mitigarlas.

SSH Weak Encryption Algorithms Supported

Descripción: La vulnerabilidad asociada consiste en que el protocolo SSH permite algoritmos de autenticación débiles, como por ejemplo 3des-cbc, aes128-cbc, aes256-cbc, las cuales se asocian al cifrado RC4 que poseen llaves débiles. Lo anterior podría permitir que un atacante obtenga datos en texto claro de bloques cifrados.

Mitigación: Deshabilitar el algoritmo de encriptación y habilitar modernos.

DCE/RPC and MSRPC Services Enumeration Reporting

Descripción: La vulnerabilidad es debido a que el servicio MSRPC se encuentra en ejecución y por medio de la conexión al puerto, esta puede ser utilizada por un atacante para conocer detalles del equipo.

Mitigación: Filtrar el tráfico entrante.

SSL/TLS: Report Weak Cipher Suites

Descripción: La vulnerabilidad consiste en enlistar toda la suite de cifrado SSL/TLS aceptado por el servicio. Se identificó que acepta las siguientes suites de cifrado:

Protocolo TLSv1.0: TLS_ECDHE_RSA_WITH_RC4_128_SHA,
TLS_RSA_WITH_RC4_128_MD5, TLS_RSA_WITH_RC4_128_SHA
Protocolo TLSv1.1: TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5, TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
Protocolo TLSv1.2: TLS_ECDHE_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_RC4_128_MD5, TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA
Protocolo SSLv3: TLS_RSA_WITH_RC4_128_MD5
TLS_RSA_WITH_RC4_128_MD5, TLS_RSA_WITH_RC4_128_SHA
TLS_RSA_WITH_SEED_CBC_SHA

Mitigación: Eliminar las suites de cifrados listados anteriormente.

SSL/TLS: Certicate Signed Using A Weak Signature Algorithm

Descripción: La vulnerabilidad consiste en que el servicio remoto una cadena de certificados SSL/TLS, usando un algoritmo de hash criptográficamente débil (SHA-1).

Mitigación: Regenerar los certificados para el servicio con SHA-2.

SSL/TLS: OpenSSL CCS Man in the Middle Security Bypass Vulnerability

Descripción: La vulnerabilidad consiste en que por medio de esta configuración los atacantes pueden obtener información sensible por medio de un ataque de hombre en el medio, propias o proporcionadas por el mismo protocolo OpenSSL.

Mitigación: Actualizar al último software disponible por parte del fabricante.

SSL/TLS: Report Vulnerable Cipher Suites for HTTPS

Descripción: La vulnerabilidad consiste en enlistar toda la suite de cifrado SSL/TLS aceptado por el servicio. Se identificó que acepta las siguientes suites de cifrado del protocolo SSLv3:

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

TLS_RSA_WITH_DES_CBC_SHA (SWEET32)

Cifrado protocol TLSv1.0:

TLS_RSA_WITH_3DES_EDE_CBC_SHA (SWEET32)

TLS_RSA_WITH_DES_CBC_SHA (SWEET32)

Mitigación: Eliminar las suites de cifrados listados anteriormente.

SSL/TLS: SSLv3 Protocol CBC Cipher Suites Information Disclosure Vulnerability (POODLE)

Descripción: La vulnerabilidad encontrada propicia la divulgación de información, por lo que un ataque de hombre en el medio podría obtener datos en texto plano.

Mitigación: Deshabilitar el protocolo SSL v3, suite de cifrado CBC y habilitar el TLS_FALLBACK_SCSV.

SSL/TLS: Deprecated SSLv2 and SSLv3 Protocol Detection

Descripción: La vulnerabilidad encontrada determinó que se usa el protocolo SSLv2 o SSLv3, el cual podría permitir que un atacante aproveche los fallos criptográficos e interceptar la conexión segura entre el cliente y el servicio y así, obtener información sensible.

Mitigación: Deshabilitar el protocolo SSLv2 y SSLv3.

SSL/TLS: Diffie-Hellman Key Exchange Insufficient DH Group Strength Vulnerability

Descripción: La vulnerabilidad encontrada indica que el servicio utiliza llave débil de encriptación menor a 2048 bits, la cual podría ser desencriptada fácilmente por un atacante.

Mitigación: Aumentar a más de 2048 bits la llave de encriptación o bien, utilizar un algoritmo de curvas elípticas para encriptación.

SNMP GETBULK Rejected DRDoS

Descripción: La vulnerabilidad consiste en que un atacante podría enviar paquetes de 41 bytes para causar una denegación de servicio al servicio de SNMP.

Mitigación: Deshabilitar el servicio SNMP o restringir el acceso a este.

Apache HTTP Server 'httpOnly' Cookie Information Disclosure Vulnerability

Descripción: La vulnerabilidad consiste en que el servicio de Apache propicia que la información sensible por medio de las cookies y estas sean divulgadas.

Mitigación: Actualizar la versión del servicio a la más reciente.

HP Integrated Lights-Out XSS Vulnerability

Descripción: La vulnerabilidad presentada consiste en que es susceptible a ataques de cross-site scripting, se hace por medio de scripts en donde el atacante los inyecta en el sitio del componente y este le responde con información.

Mitigación: Actualizar al último software disponible por parte del fabricante.

SSL/TLS: OpenSSL TLS 'heartbeat' Extension Information Disclosure Vulnerability

Descripción: La vulnerabilidad permite la divulgación de información sensible.

Mitigación: Actualizar al último software disponible por parte del fabricante.

Microsoft IIS Default Welcome Page Information Disclosure Vulnerability

Descripción: La vulnerabilidad permite la divulgación de información sensible por medio de la facilidad que le ofrece el servicio IIS.

Mitigación: Deshabilitar el sitio por defecto del servicio.

Use LDAP search request to retrieve information from NT Directory Services

Descripción: La vulnerabilidad consiste en que el active directory o directorio activo enliste o divulgue la composición de su estructura.

Mitigación: Eliminar la compatibilidad de pre-Windows 2000.

SSL/TLS: Missing `secure` Cookie Attribute

Descripción: La vulnerabilidad consiste en que las cookies no están utilizando el atributo seguro, lo cual pasa del cliente al servidor por medio de un canal no seguro, permitiendo al atacante secuestrar la sesión. Esto es asociado al servicio de conexión SSL/TLS ejecutándose en el equipo.

Mitigación: Habilitar el atributo seguro para cualquier cookie enviada por una conexión SSL/TLS.

Missing 'httpOnly' Cookie Attribute

Descripción: La vulnerabilidad encontrada consiste en la falta del atributo "httpOnly" en las cookies.

Mitigación: Habilitar el atributo "httpOnly" para todas las cookies enviadas usando la conexión SSL/TLS.

Vulnerabilidades bajas

Se atenderán en esta sección las descripciones de las vulnerabilidades bajas encontradas, así como la manera en que se establece mitigarlos.

TCP timestamps

Descripción: La vulnerabilidad encontrada permite que se conozca la disponibilidad del equipo.

Mitigación: Deshabilitar el servicio de sellado de tiempo TCP.

SSH Weak MAC Algorithms Supported

Descripción: La vulnerabilidad consiste que el equipo permite algoritmos débiles para SSH. Los algoritmos son:

Cliente a servidor: hmac-md5, hmac-md5-96, hmac-sha1-96

Servidor a cliente: hmac-md5, hmac-md5-96, hmac-sha1-96

Mitigación: Eliminar los algoritmos listados anteriormente.

SSL/TLS: TLS/SPDY Protocol Information Disclosure Vulnerability (CRIME)

Descripción: La vulnerabilidad encontrada propicia la divulgación de información si un atacante utiliza la técnica de hombre en el medio. Los protocolos de compresión

detectados vulnerables al ataque “CRIME” son: TLSv1.1: DEFLATE, TLSv1.2: DEFLATE, TLSv1.0: DEFLATE, SSLv3: DEFLATE.

Mitigación: Deshabilitar la compresión TLS o bien, cambiar el protocolo SPDY/4 o HTTP/2 por los sucesores de estos.

Recomendaciones adicionales para asegurar la infraestructura

Las mitigaciones descritas anteriormente tratan lo encontrado por medio de las herramientas de escaneo y gestión de vulnerabilidades utilizados. Pero debido a que se conocen otras consideraciones de seguridad importantes y de riesgo sumamente alto, que no se está implementado, se describirán a continuación, más recomendaciones obligatorias que tiene que ser ejecutadas en conjunto.

Acceso a Internet

Los accesos a Internet son necesarios en varios equipos y servicios, pero también se debe restringir para evitar cualquier riesgo ante posibles infecciones por virus, ransomware, junto con otras. Se definirán los equipos y servicios en Tabla 14 que estarán expuestos a Internet, por lo que todos los demás estarán sin acceso a Internet. Para cualquier equipo o servicio nuevo por implementar por defecto, no tendrá Internet. Para solicitar este permiso, se deberá solicitar por los procedimientos existentes de mesa de ayuda o help desk.

Tabla 14. Tabla de accesos a Internet.

Servicio	Cantidad	Filtrado
WSUS	1	Sí
ADFS	2	Sí
VES	6	Sí
Sistema de trámites	1	Sí
Página Web	1	No
Sistema de inventario	1	Sí
Sistema de gestión de personal	1	Sí
Antivirus	1	No
DNS externo	2	Sí
Filtrado Web	2	Sí

Fuente: Elaboración propia.

GPO

Las políticas definidas tanto para equipos y usuario que se tienen configuradas, tienen una disposición que imposibilita o restringe la ejecución o apertura de componentes de software, creando un ambiente seguro de trabajo para los usuarios con los sistemas de información.

Luego de revisar las políticas enumeradas en la Tabla 12, se determinó que se deben adicionar las siguientes:

Tabla 15.Configuración de políticas de grupo necesarias.

Política	Descripción
Finalizar sesiones desconectadas	Configurar a un máximo de dos horas, las sesiones que se encuentren en estado desconectado.
Límite de sesión activa	Configurar a un máximo de dos horas, la inactividad de sesiones.
Cambio de contraseña de administradores	Configurar a 90 días, el cambio de la contraseña de los administradores.
Cambio de contraseña de cuentas de servicio.	Configurar a 360 días, el cambio de la contraseña de los administradores.

Fuente: Elaboración propia.

En la Tabla 15 están las opciones que se considera, deben adicionarse a la configuración de políticas. Las primeras configuraciones encontradas se encuentran parcialmente implementadas. El término parcialmente implementada, es debido a que está configurada para los usuarios, no así para las cuentas de gestión. Esta nueva adición tendría como ámbito las cuentas de los administradores y por último, la renovación de credenciales para las cuentas de servicio con la especificación dada. Esta última conlleva a procedimientos definidos de resguardo de contraseña de forma segura.

DNSSEC

El DNSSEC es una extensión de seguridad para propiamente el DNS. La recomendación se fundamentada en la razón de que, debido a las vulnerabilidades asociadas a este servicio, spoofing es una de ellas y se considera que firmar digitalmente los registros de nombre de dominio, reduce enormemente este riesgo.

VLAN

Actualmente se tiene una estructura plana de la red de infraestructura, debido a que solamente se tiene definida una (1) vlan desplegada para la comunicación de los diferentes equipos, por esto se considera necesario implementar lo siguiente:

Tabla 16. VLAN para la infraestructura de SUPEN.

VLAN
Servidores
Almacenamiento
iLO, OA y SAN
WSUS
Respaldo
DMZ

Fuente: Elaboración propia.

La Tabla 16 contiene las vlan que deben crearse para tener un ambiente seguro para la infraestructura de servidores. Se define o mantiene la vlan de servidores como red de negocio, donde se encuentran todos los sistemas de información. Para la gestión del almacenamiento también se recomienda la creación de la vlan para hacer un buen uso del ancho de banda.

La vlan del iLO, OA y SAN se define para que se gestione el hardware, para la vlan de WSUS y no interfiera con cualquier servicio.

Firmware

Deben ser actualizadas anualmente, no sin antes ser evaluadas para que no afecten los sistemas de información desplegados.

Capítulo 6: Conclusiones

La metodología utilizada Technology, National Institute of Standards and Technology (2008), fue la mejor opción para este tipo de investigación, de igual manera, se revisaron publicaciones relacionadas que permitirían tener una mejor visión de lo que se realizó y por este motivo se busca en las bibliotecas de las instituciones que clasifican todo tipo de servicio y producto. Se cuenta con acceso a Gartner, donde se encontraron publicaciones relacionadas (Chuvakin & Barros, A Guidance Framework for Developing and Implementing Vulnerability Management, 2017), las cuales también se emplearon como apoyo para la metodología que se seleccionó.

Este proyecto, requirió de varios esfuerzos y autorizaciones con el fin de tener la información exacta y necesaria para poder cumplir los objetivos del trabajo. También se tuvo que remover información que se consideró sensible para no exponer a la organización, tal es el caso de las direcciones IP y nombre de servidores.

En cumplimiento con el primer objetivo, se enlistaron los activos de la organización que forman parte de la infraestructura tecnológica, así como documentación relacionada con la gestión de vulnerabilidades. Como se puede apreciar en las Tablas 3, 4, 5, 6 y 7, se parte de ver el estado actual, para posteriormente hacer recomendaciones conforme los encuentros que se tengan de las evaluaciones. De los resultados obtenidos en esta primera etapa, se destaca el de la Tabla 7, el cual será insumo para el encargado de red quien será el responsable de actualizar toda información pertinente a su documentación. A partir de este punto, cualquier solicitud de apertura de puertos, deberá estar registrado y contabilizado para que, en evaluaciones siguientes, se tenga un punto de comparación.

Para las guías actuales, están deben ser atendidas en un plazo corto, ya que deben contener información precisa sobre cómo ejecutar ciertas tareas. Si bien, los expertos conocen qué hacer, estar definidas paso a paso es necesario y crítico para que esta no sea subjetiva.

Los análisis y evaluaciones de vulnerabilidades realizadas permitieron conocer toda la infraestructura tecnológica, por medio de las herramientas utilizadas durante toda la carrera. Al tener un amplio conocimiento en el uso de las herramientas, facilitó enormemente la obtención de resultados o insumos necesarios para completar este proyecto. Para evaluaciones posteriores, se recomienda el uso de Nmap (s.f.) y OpenVAS (s.f.) y en un ambiente controlado donde se pueda utilizar el Armitage de Kali Linux Tools (s.f.). Estas herramientas son potentes y además, gratuitas. En caso de que la organización desee utilizar otras de pago, como Rapid7 (s.f.) y Tenable (s.f.), se recomienda hacer una comparación de uso contra el costo y además considerar la contratación de una empresa que realice estas evaluaciones de seguridad.

Continuando con las evaluaciones encontradas, se tuvo vulnerabilidades altas, medias y bajas, tal y como se ve en la Tabla 8, por lo que es necesario atender las indicaciones de mitigación encontradas. Para la atención de las mitigaciones, según el tipo de vulnerabilidad, se definirán plazos de acción para ejecutar la remediación.

Muchas de estas vulnerabilidades se mitigarán con los procesos que se hacen periódicamente de parchado de servidores, pero hay acciones que requieren de intervención manual. El personal del área encargada de la infraestructura de servidores,

cuenta con experiencia para atender las recomendaciones de mitigación en caso de que el plan de mitigación sea aceptado.

Tabla 17. Plan de mitigación de vulnerabilidades.

Vulnerabilidad	Plazo de mitigación (Máximo)
ALTAS	6 meses
MEDIAS	9 meses
BAJAS	12 meses

Fuente: Elaboración propia.

En la Tabla 17 se recomiendan estos plazos, debido a que, conforme pasa el tiempo, las vulnerabilidades MEDIAS y BAJAS pueden convertirse en ALTAS, debido a que día a día se encuentran diferentes técnicas para explotarlas. Además, este proceso de evaluación, según procedimientos definidos en el área de Tecnologías de Información, debe ser realizado anualmente, con esto se cumple con este proceso y además debe seguir la misma metodología utilizada para desarrollar este proyecto. Esto garantiza que no se traslapen los períodos de mitigación.

Para la efectiva mitigación de vulnerabilidades en la infraestructura tecnológica, se definen varios aspectos parar disminuir los riesgos que podrían generar estos. El primer aspecto, considera el acceso a internet. Se encontró que todos los servicios y equipos tienen acceso a Internet, desde este punto de vista, esto debe ser corregido inmediatamente, por lo que se definen en la Tabla 14 cuáles servicios y equipos deben contar con este acceso.

El segundo aspecto, se considera varios cambios en las políticas para objetos de equipo y usuario, estas deben implementarse de forma inmediata, por dos motivos la primera es la de mayor seguridad y la otra de fácil implementación.

El tercer aspecto, considera la implementación del servicio de DNSSEC, esto para evitar cualquier tipo de ataque tipo spoofing, pharming o phishing, los cuales se aprovechan contaminando los registros de DNS y redirigir hacia sitios falsos. La implementación garantiza la autenticidad de los sitios, por medio del proceso de firmado digital, impidiendo este tipo de riesgos. Esto debe aplicarse parar todos los DNS en la organización.

El cuarto aspecto, considera la creación de VLAN adicionales para toda la infraestructura tecnológica, esta recomendación está basada para optimizar el ancho de

banda de la red y adicionalmente, un mayor control del tráfico de red. Esta recomendación se debe canalizar al experto responsable de la red para que sean atendidas en el tiempo que determinen necesario.

El último aspecto considera, la aplicación de firmware más reciente en todos los equipos. Se recomienda incorporar esta tarea antes de la ejecución de una nueva evaluación de vulnerabilidades.

Tabla 18. Resumen de atención de aspectos adicionales de seguridad.

Ítem	Plazo de mitigación (máxima)	responsable
GPO	Inmediata	Servidores
DNSSEC	Inmediata	Servidores
VLAN	Seis meses	Telecomunicaciones
FIRMWARE	Inmediata	Servidores

Fuente: Elaboración propia.

En la Tabla 18 se aprecian los tiempos y los responsables de implementar los aspectos adicionales de seguridad para la infraestructura tecnológica de la SUPEN.

Finalmente, se considera que los resultados obtenidos son, gracias a las diferentes experiencias acumuladas a través de la carrera, teniendo claro que estas técnicas deben ser compartidas en el entorno de trabajo. Todas las recomendaciones brindadas deben ser atendidas en los plazos indicados. Con lo anterior, se garantiza que la infraestructura estará con niveles de riesgo bajos. De esta manera, queda claro que el objetivo general y los específicos se cumplieron a satisfacción.

Reflexiones finales

Se considera para la ejecución de este proyecto, que el contenido de la Maestría en Ciberseguridad, es fundamental y crítico para poder llevar a cabo los diferentes análisis e implementación de recomendaciones en el área de tecnologías de información.

Permite al profesional desarrollar un mejor criterio experto, destrezas, capacidad y conocimiento en técnicas y herramientas al tiempo de trabajar, considerar y proponer diferentes aspectos que permiten que la infraestructura tecnológica, tener un mayor nivel de seguridad, garantizando siempre la confidencialidad, integridad y disponibilidad de los diferentes elementos que la componen.

En la ejecución de este trabajo se utilizaron materias como metodologías de investigación aplicada, para estructurar de una mejor manera un trabajo de investigación,

también materias como seguridad en sistemas operativos; seguridad y protocolos de comunicación; análisis de detección de vulnerabilidades; análisis y evaluación de riesgos de seguridad permiten desempeñarse y ejecutar este tipo de trabajo de una manera eficiente y eficaz por todo el conocimiento en técnicas y herramientas aprendidas.

Glosario

BCCR: Banco Central de Costa Rica.

ODM: Órgano de Desconcentración Máxima.

CONASSIF: Consejo Nacional de Supervisión del Sistema Financiero.

Seguridad: Sistema o conjunto de instrucciones para mantener los activos protegidos.

Seguridad de la Información: Protección de la información, garantizando la confidencialidad, integridad y disponibilidad de ella.

Ciberseguridad: Protección de activos digitales.

Vulnerabilidad: Defecto o características que puede ser atacada.

Riesgo: Posibilidad de pérdida.

Amenaza: posibilidad de que un evento explote una vulnerabilidad.

Impacto: afectación causada por la explotación de una vulnerabilidad.

Probabilidad: capacidad de que ocurra un evento en un tiempo determinado.

Penetración / Explotación

Confidencialidad: Asegurar la información de tal manera que solo sea accesible a todas aquellas personas autorizadas.

Integridad: Exactitud y completitud de la información.

Disponibilidad: Acceso a la información cuando este sea requerido.

Información:

Activo: Objeto con valor tangible e intangible.

Política: Definen elementos, alcances y funciones.

Procedimiento: Instrucciones paso a paso para la implementación de tareas.

Guía: Listado de pasos específicos para ejecutar una tarea.

Directriz: Controles discrecionales

Norma / Estándar: Establecen los requisitos para uso de protocolos comunes.

Control: Conjunto de políticas, acciones, normas y procedimientos para reducir el riesgo de un activo.

Mejores Prácticas: Configuraciones de seguridad aprobadas.

COBIT: Objetivo de Control para Información y Tecnologías Relacionadas.

ITIL: Biblioteca de Infraestructura de TI.

ISO: Organización Internacional de Normalización.

BSI: Instituto Británico de Estándares.

ITSEC: Criterios de Evaluación de Seguridad de Tecnologías de la Información.

NIST: Instituto Nacional de Estándares y Tecnología.

Enclosure / Gabinete: conjunto de interconexiones que integran fuentes de poder, ventilación y administración para servidores modulares.

Servidor: Instancia de un programa que recibe y responde a las solicitudes de clientes.

iLO: integrated Lights Out.

Onboard Administator: Consola de administración de un gabinete

NVT: Prueba de vulnerabilidad de red. (OpenVas, s.f.)

CVSS: Sistema de ponderación de vulnerabilidades comunes. (Forum of Incident Response and Security Teams, s.f.)

AD: Servicio de Directorio activo o Active Directory.

DNS: Servicio de Nombre de Dominio.

DHCP: Protocolo de Configuración Dinámica de host.

DFS: Sistema Distribuido de Archivos.

SQL: Motor de Base de Datos. Lenguaje de consultas estructuradas.

IIS: Servicio de Información de Internet.

ADFS: Servicio Federado de Directorio Activo.

SMTP: Protocolo de Transferencia Simple de Correo.

ORACLE: Motor de Base de Datos

TLS: Seguridad en la Capa de transporte

SSL: Capa de puertos Seguros.

SSH: Intérprete de órdenes Seguro

RPC: Procedimiento de Llamado Remoto

HTTP: HyperText Transport Protocol.

TCP: Protocolo de Control de Transferencia.

IP: Protocolo IP

Filtrado Web: Servicio basado en políticas para controlar la navegación hacia y desde internet.

GPO: Objeto de Políticas de Grupo.

WSUS: Servicio de Actualización de Windows.

Red: Interconexión de equipos por medio de una conexión inalámbrica o física.

Parches: Actualización de un componente de un Sistema operativo.

Sistema Operativo: Software de bajo nivel que soporta funciones básicas de computadoras, así como programando tareas y controlando equipos periféricos.

Port Mirroring: Redirección de puertos hacia una conexión con monitoreo.

Firmware: Conjunto de instrucciones de software para controlar los dispositivos.

Internet: Red global de computadoras que provee una variedad de información y comunicación, utilizando protocolos de comunicación estandarizada.

Línea Base: Estandarización de los paquetes de software para ser instalados en un dispositivo.

Referencias

Barros, A., & Chuvakin , A. (s.f.). *A Comparison of Vulnerability and Security Configuration Assessment Solutions*. Obtenido de A Comparison of Vulnerability and Security Configuration Assessment Solutions: www.gartner.com

Chuvakin, A. (2014). *Vulnerability and Security Configuration Assessment Solutions Comparison*. Obtenido de Vulnerability and Security Configuration Assessment Solutions Comparison: www.gartner.com

Chuvakin, A., & Barros, A. (2017). *A Guidance Framework for Developing and Implementing Vulnerability Management.* Gartner.

Common Vulnerability Scoring System SIG. (s.f.). Obtenido de Common Vulnerability Scoring System SIG: https://www.first.org/cvss/

CVE. (s.f.). *Common Vulnerabilities and Exposures*. Obtenido de CVE: https://cve.mitre.org/about/

Forum of Incident Response and Security Teams. (s.f.). *Common Vulnerability Scoring System SIG*. Obtenido de https://www.first.org/cvss/

Gartner. (17 de noviembre de 2015). *A Comparison of Vulnerability and Security Configuration Assessment Solutions* . Obtenido de www.gartner.com

Jones, N. (2017). *IBM Retains Leadership Position in 2017 Gartner Magic Quadrant for Application Security Testing*. Recuperado de https://securityintelligence.com/ibm-retains-leadership-position-in-2017-gartner-magic-quadrant-for-application-security-testing/

Kali Linux Tools. (s.f.). *Armitage*. Obtenido de https://tools.kali.org/exploitation-tools/armitage

Kitchenham, B. (2007). *Guidelines for performing Systematic Literature Reviews in Software Engineering.* UK: Keele University.

Microsoft. (s.f.). *Microsoft Azure*. Obtenido de https://azure.microsoft.com/en-us/

Microsoft. (s.f.). *Microsoft Azure ¿Qué es IaaS?* Obtenido de https://azure.microsoft.com/es-es/overview/what-is-iaas/

Microsoft. (s.f.). *Microsoft Azure ¿Qué es PaaS?* Obtenido de https://azure.microsoft.com/es-es/overview/what-is-paas/

Microsoft. (s.f.c). *Microsoft Azure ¿Qué es SaaS?* Obtenido de https://azure.microsoft.com/es-es/overview/what-is-saas/

NIST. (s.f.). *NVD CVSS Support*. Obtenido de NVD CVSS Support: https://nvd.nist.gov/vuln-metrics/cvss

Nmap. (s.f.). *Nmap*. Obtenido de Nmap: https://nmap.org/

OpenVas. (s.f.). *NVT Development*. Obtenido de NVT Development: http://www.openvas.org/nvt-dev.html

OpenVAS. (s.f.). *OpenVAS*. Obtenido de OpenVAS: http://www.openvas.org/

OWASP. (s.f.). *OWASP Top Ten Project*. Obtenido de https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project#tab=OWASP_Top_10_for_2017_Release_Candidate

Oxford Dictionaries. (s.f.). *Internet*. Obtenido de https://en.oxforddictionaries.com/definition/Internet

Oxford Dictionaries. (s.f.). *Operating System*. Obtenido de https://en.oxforddictionaries.com/definition/operating_system

Oxford Dictionaries. (s.f.). *SQL*. Obtenido de https://en.oxforddictionaries.com/definition/sql

Rapid7. (s.f.). *Nexpose*. Obtenido de https://www.rapid7.com/globalassets/_pdfs/product-and-service-briefs/rapid7-nexpose-product-brief.pdf

Rapid7. (s.f.). *Rapid7 Nexpose*. Obtenido de https://www.rapid7.com/products/nexpose/

SUPERINTENDENCIA DE PENSIONES, COSTA RICA. (2002). *Ficha de Proceso de TI.* SAN JOSÉ: SUPERINTENDENCIA DE PENSIONES.

SUPERINTENDENCIA DE PENSIONES, COSTA RICA. (2012). *POLÍTICA DE ADMINISTRACIÓN DEL RECURSO INFORMÁTICO.* SAN JOSÉ: SUPERINTENDENCIA DE PENSIONES.

SUPERINTENDENCIA DE PENSIONES, COSTA RICA. (2014). *Manual del Sistema de Calidad Gestión de Calidad.* SAN JOSÉ: SUPERINTENDENCIA DE PENSIONES.

SUPERINTENDENCIA DE PENSIONES, COSTA RICA. (2014). *Proceso de la Seguridad de la Información.* SAN JOSÉ: SUPERINTENDENCIA DE PENSIONES.

SUPERINTENDENCIA DE PENSIONES, COSTA RICA. (2015). *PLAN ESTRATÉGICO 2016 - 2020.* SAN JOSÉ: SUPERINTENDENCIA DE PENSIONES.

SUPERINTENDENCIA DE PENSIONES, COSTA RICA. (2015). *POLÍTICA DE SEGURIDAD INFORMÁTICA.* SAN JOSÉ: SUPERINTENDENCIA DE PENSIONES.

SUPERINTENDENCIA DE PENSIONES, COSTA RICA. (s.f.). *Sistema de Trámites*. Obtenido de https://si.supen.fi.cr

SUPERINTENDENCIA DE PENSIONES, COSTA RICA. (s.f.). *SUPEN*. Obtenido de www.supen.fi.cr

SUPERINTENDENCIA DE PENSIONES, COSTA RICA. (s.f.). *VES*. Obtenido de https://ves.supen.fi.cr

Technology, National Institute of Standards and Technology. (2008). *Technical Guide to Information Security Testing and Assessment Recommendations of the National Institute of Standards and Technology.* Estados Unidos: National Institute of Standards and Technology.

Tenable. (s.f.). *Nessus*. Obtenido de https://www.tenable.com/products/nessus-vulnerability-scanner.