Universidad Cenfotec

Maestría en Ciberseguridad

Tema:

Analizar la metodología de gestión de vulnerabilidades para mejorar la seguridad en los sistemas informáticos en una institución financiera nacional

Elaborado por:

Kailor Paolo Murillo Prado

Diciembre, 2022

Declaratoria de derechos de autor

TRIBUNAL EXAMINADOR

Este proyecto fue aprobado por el Tribunal Examinador de la carrera: **Maestría Profesional en Ciberseguridad,** requisito para optar por el título de grado de **Maestría,** para el estudiante: **Murillo Prado Kailor.**

DENNIS ALONSO DURAN CESPEDES (FIRMA)
Firmado digitalmente por DENNIS ALONSO DURAN CESPEDES (FIRMA)
Fecha: 2023.03.17 21:50:03 -06'00'

M.Sc. Dennis Alonso Durán Céspedes
Tutor

ARTURO RAMIREZ HEGG (FIRMA)
Firmado digitalmente por ARTURO RAMIREZ HEGG (FIRMA)
Fecha: 2023.03.19 16:29:15 -06'00'

M.Sc. Arturo Ramírez Hegg
Lector 1

IGNACIO TREJOS ZELAYA (FIRMA)
Firmado digitalmente por IGNACIO TREJOS ZELAYA (FIRMA)
Fecha: 2023.03.20 20:37:15 -06'00'

M.Sc. Ignacio Trejos Zelaya
Lector 2

San José, Costa Rica, 17 de marzo de 2023

Firmada digitalmente, de conformidad con la Ley de Certificados, Firmas Digitales y Documentos Electrónicos N° 8454, destacando el artículo 9°-

Carta de aprobación del filólogo

Cartago, 09 de enero de 2023

Los suscritos, Elena Redondo Camacho, mayor, casada, filóloga, incorporada a la Asociación Costarricense de Filólogos con el número de carné 0247, portadora de la cédula de identidad número 3-0447-0799 y, Daniel González Monge, mayor, casado, filólogo, incorporado a la Asociación Costarricense de Filólogos con el número de carné 0245, portador de la cédula de identidad número 1-1345-0416, ambos vecinos de Quebradilla de Cartago, revisamos el trabajo final de graduación que se titula: *Analizar la metodología de gestión de vulnerabilidades para mejorar la seguridad en los sistemas informáticos en una institución financiera nacional*, sustentado por Kailor Paolo Murillo Prado.

Hacemos constar que se corrigieron aspectos de redacción, estilo y otros vicios del lenguaje que se pudieron trasladar al texto. A pesar de esto, la originalidad y la validez del contenido son responsabilidad directa de la persona autora.

Esperamos que nuestra participación satisfaga los requerimientos de la Universidad Cenfotec.

Elena Redondo Camacho
Filóloga - Carné ACFIL n.º 0247

X

Daniel González Monge
Filólogo - Carné ACFIL n.º 0245

X

Tabla de contenido

Resumen

El presente estudio tiene como fin indagar un poco en la metodología de gestión de vulnerabilidades que se utiliza actualmente en una institución financiera de Costa Rica para implementar o aplicar medidas de seguridad de la información a sus sistemas informáticos. Se basa específicamente en un análisis de vulnerabilidades realizado a una muestra de equipos de una subred específica y así observar la viabilidad de su ejecución en este ámbito. A partir de esto se busca analizar algunos de los cuidados que deben tener empresas financieras para tener segura la información que debe guardar de forma íntegra.

Palabras clave: ciberseguridad, vulnerabilidades, viabilidad, ventajas, desventajas, metodologías, empresas, costarricense.

Capítulo 1. Introducción

1.1 Generalidades

Se debe entender la importancia que tiene para una empresa mantener sus datos y los de sus clientes de forma segura, en especial cuando se trata de una organización bancaria. Lo anterior ya que contar con alguna vulnerabilidad se puede prestar para la pérdida de grandes cantidades de dinero, reputación de la entidad, entre otras cosas.

1.2 Antecedentes del problema

Las entidades financieras siempre son un objetivo atractivo para los ciberdelincuentes, por lo que estas organizaciones reciben constantemente ataques cibernéticos que tienen como fin encontrar vulnerabilidades que los exponga, por lo tanto, deben establecer medidas para proteger sus sistemas informáticos y prevenir el robo de información. Por ejemplo, algunas organizaciones establecen una figura de centro de operaciones de seguridad, la cual siempre monitorea estos ataques, además de contar con un equipo especializado de ciberseguridad, el cual busca y analiza información y soluciones para lograr el aseguramiento de los activos de la organización.

Es importante mencionar que las empresas que actualmente no cuenten con medidas para la seguridad de sus sistemas informáticos, o bien hayan implementado algunas, tal vez no de la mejor manera, corren un alto riesgo de

que se comprometa su información, cause un daño a la imagen organizacional e incluso ocasionar el cierre de sus operaciones en el mercado.

1.3 Definición y descripción del problema

Este trabajo tiene como objetivo analizar la metodología de gestión de vulnerabilidades para mejorar la seguridad en los sistemas informáticos en una institución financiera nacional.

Se debe tener en cuenta que, con el avance de nuevas tecnologías y su implementación en la industria, diariamente surgen nuevas vulnerabilidades capaces de ser explotadas por los ciberdelincuentes para hacer daño a organizaciones que no tengan definida una buena gestión de vulnerabilidades.

Muchas empresas en la actualidad operan utilizando infraestructuras obsoletas, con malos diseños en la arquitectura de seguridad, sin hacer reconocimientos del estado de sus equipos, entre muchos otros factores que generan un riesgo potencial para la organización.

1.4 Justificación

De acuerdo con Navarro (2020): “La ciberseguridad es un elemento crucial para el correcto funcionamiento de cualquier tipo de organización hoy en día. Sin ella, muchas podrían desaparecer con un único ciberataque. Por ello invertir en ciberseguridad nunca será un gasto” (s. p).

Se debe ver la ciberseguridad como una inversión necesaria para cualquier compañía. Esto se debe a que, si no se toman las medidas necesarias para protegerse, la información que se genere y almacene puede verse comprometida.

Es posible tomar como ejemplo un banco que no cuente con oficiales de seguridad, puertas de acceso restringido, cámaras, entre otras cosas. El no tener estas medidas de seguridad física expone a un banco a algún tipo de robo, por lo tanto, se debe invertir en esa seguridad. Actualmente, la ciberseguridad es igual de importante que la seguridad física, sin esta se estaría igual de expuesto o incluso es todavía mayor el riesgo.

El hecho de implementar esto en una organización representa una suma de dinero que se debe invertir. Sin embargo, se debe tener en cuenta qué es lo que necesita la entidad y cómo implementarlo, ya que no es posible esperar que

una pyme pueda invertir del mismo modo que una gran empresa.

Cualquiera sea el caso, el implementar seguridad permite a las organizaciones estar protegidas de algún daño que alguien quiera hacer en su contra, asegurar su información y ser vista por la sociedad como una entidad confiable.

1.5 Viabilidad

Este proyecto es viable gracias a la colaboración del Departamento de Tecnologías de Información y el Área de Ciberseguridad de una institución financiera de Costa Rica. Estas entidades brindaron los recursos necesarios para

analizar vulnerabilidades a una muestra de equipos y observar el flujo de la gestión de vulnerabilidades en la empresa para realizar el debido análisis. Además, se debe mencionar que existe mucha información en la web sobre este tema, lo que permite realizar comparaciones y conocer sobre mejores prácticas.

1.5.1 Punto de vista técnico

Como profesional en sistemas de información y futuro máster en ciberseguridad, el autor de este documento cuenta con el conocimiento y experiencia en manejo de *software* para realizar diferentes tipos de análisis de vulnerabilidades, así como conocimiento en diversas metodologías para la gestión de vulnerabilidades en una organización. De igual manera, se espera que en este proceso de investigación pueda adquirir todavía más experiencia y conocimiento que pueda aplicarse y facilite la resolución del problema expuesto.

1.5.2 Punto de vista operativo

Para lograr que sea posible realizar la investigación sin alterar el funcionamiento normal de la empresa, se coordinan sesiones con el personal de ciberseguridad en horas que no exista gran carga laboral. El acceso a recursos lo brindan los compañeros del centro de operaciones de seguridad y los escaneos se programan para hacerse en horarios que no alteren o generen estrés en los equipos.

1.5.3 Punto de vista económico

El costo teórico que implica el desarrollo de este proyecto, tomando en cuenta las horas de investigación, licencias de *software*, *hardware* y otros gastos asociados, corre por cuenta del autor del proyecto. No obstante, la organización cuenta con el *hardware* y *software* necesario y lo pone a disposición

para elaborar el proyecto.

Al tomar en cuenta la página oficial de Tenable, la licencia del *software* Nessus empresarial tiene un costo de $2,275.00 USD anual. Se considera un promedio del salario anual de una analista de ciberseguridad en Costa Rica en $45,000.00 USD, por lo que se estima el costo teórico del trabajo en $32,275.00 USD.

1.6 Objetivos

Se utiliza la taxonomía original de Bloom de 1956 para plantear los objetivos de esta investigación, debido a su metodología jerárquica, la cual escala hasta emitir un criterio de evaluación.

1.6.1 Objetivo general.

- Analizar la metodología de gestión de vulnerabilidades para el mejoramiento de la seguridad en los sistemas informáticos en una institución financiera nacional.

1.6.2 Objetivos específicos.

- Conocer la necesidad de una entidad bancaria para que se ejecute un análisis de vulnerabilidades.
- Comprender las ventajas y desventajas que pueda tener la ejecución de un análisis de vulnerabilidades en entidades bancarias.
- Demostrar cuáles metodologías se pueden utilizar para que se lleve a cabo un análisis de vulnerabilidades.
- Realizar un análisis de vulnerabilidades a una muestra de equipos de una institución financiera de Costa Rica para que se brinde la solución a las vulnerabilidades encontradas.

1.7 Alcances y limitaciones

1.7.1 Alcances

Ofrecer a los lectores el conocimiento del impacto que tiene la ciberseguridad en la industria y la importancia de una buena gestión de vulnerabilidades en las organizaciones.

El análisis de vulnerabilidades se aplica a un grupo específico de equipos en producción de una subred de una entidad financiera de Costa Rica. Se realizan tres entregables con avances de este documento y, adicionalmente,

una presentación final.

1.7.2 Limitaciones

Aunque se busca analizar vulnerabilidades a un segmento de red entero, por la enorme cantidad de equipos que contemplan las subredes de la organización, el alcance se ve limitado a una muestra de equipos específicos para realizar los escaneos.

Además, por temas regulatorios de la organización, no es posible gestionar un permiso de acceso para realizar las pruebas, a la vez, estas se solicitan y realizan en un acompañamiento con el personal que sí cuenta con el debido permiso para realizarlas.

No se desarrollan casos en los que se ponga en riesgo la disponibilidad de un servicio de la organización.

1.8 Estado de la cuestión

Según Mora Mora (2010): “Tanto dependen los países desarrollados de sus redes de computación y la interconectividad, que se estima que el próximo ataque terrorista será un ciber ataque, capaz de paralizar la economía norteamericana” (s. p).

Desde hace algunos años atrás hasta la actualidad se ha sido testigo de los avances tecnológicos que se han presentado en el mundo, hasta el punto de que con mucha frecuencia es asombrante lo que ha sido capaz de crear el ser humano con la tecnología. Dichosamente, muchos de estos avances son para la búsqueda de mejoras o invenciones, sin embargo, a medida que los avances surgen, a la vez, salen a la luz eventos en los que la tecnología ha logrado vulnerarse. Existen personas u organizaciones cuyo propósito es realizar acciones no éticas hacia algún objetivo específico, aprovechándose de factores tecnológicos y así obtener su propio beneficio.

Se tiene un avance progresivo con la tecnología, pero a medida que esta avanza, también aumenta la posibilidad de ser vulnerado y sufrir un ciberataque y es justamente de esto que se tiene que estar al margen.

La cita de Mora Mora (2010) sirve para aportar que actualmente no solo los países desarrollados sufren esa dependencia a la tecnología, sino el mundo en

general. Debido a esto es que se debe proteger para prevenir afectaciones por algún daño que alguien pueda causar.

Costa Rica es un país que cuenta con una parte de su industria automatizada tecnológicamente y se debe analizar la posibilidad de mantener todo esto de una manera segura.

1.8.1 Planificación de la revisión.

En esta etapa se plantea una pregunta clara del tema de investigación. Se realiza una búsqueda exhaustiva de la documentación existente en el tema, con el fin de conocer el desarrollo académico que existe en este, considerar las investigaciones existentes para proteger el derecho a la propiedad intelectual y también para ampliar el desarrollo del tema.

1.8.1.1 Formulación de la pregunta

La formulación de la pregunta ayuda a definir el cuestionamiento central que la investigación plantea responder, delimitando la búsqueda de información e investigación. El objetivo es abordar el problema y, a través de los hallazgos y análisis de la información, brindar una respuesta en la conclusión del trabajo.

1.8.1.1.1 Foco de la pregunta

Para la presente investigación es necesario priorizar la búsqueda de documentos técnicos que especifiquen las mejores prácticas para la gestión de vulnerabilidades en entornos empresariales y metodologías que se utilizan.

1.8.1.1.2 Amplitud y calidad de la pregunta

En este apartado se define la pregunta de investigación que se quiere responder de manera clara y concisa, tomando como base un problema por resolver. Además, se enlistan algunos términos clave para la búsqueda de la información.

1. <u>Problema</u>

La existencia de vulnerabilidades en la infraestructura tecnológica de una organización es una debilidad que puede causar grandes daños monetarios, reputacionales y muchos otros. Por lo tanto, si una entidad cuenta con una metodología deficiente para la gestión de vulnerabilidades, se expone a que en

cualquier momento se manifieste algún riesgo que pueda ser de grandes dimensiones y cause un gran impacto al negocio.

2. Pregunta

Con la anterior definición del problema, se formula la siguiente pregunta de investigación:

¿Existe la posibilidad de mejorar la metodología de gestión de vulnerabilidades en esta institución financiera de Costa Rica?

3. Palabras clave y sinónimos

A continuación, se elabora una lista de palabras clave que se utilizan para la búsqueda de documentos y trabajos que se relacionan con la investigación:

Vulnerabilidades
Tecnología
Metodología
Servidores
Infraestructura
Gestión
Nessus
Sistemas
Información

Tabla 1: Listado de palabras.

4. Intervención

Analizar los resultados de un análisis de vulnerabilidades aplicado a una muestra, indagar la manera en que se gestionan las vulnerabilidades en la entidad y examinar documentos de relevancia para la investigación para comparar y analizar los resultados.

5. Control

Se inicia con una búsqueda de documentos relevantes para la investigación desde cero, ya que al inicio no se tiene ninguna base de información.

6. Efectos

Se espera que con la búsqueda exhaustiva se pueda obtener suficiente información de los esfuerzos que ya se han hecho, tanto en Costa Rica como fuera del país. Lo anterior para optimizar el proceso de gestión de vulnerabilidades en distintas organizaciones, así como tener una noción de cuáles procesos se pueden mejorar para lograr una gestión de vulnerabilidades más efectiva.

7. Medida de salida

Para los documentos que se encontraron se lleva a cabo una revisión de la calidad en sitios web especializados para este fin.

8. Aplicación

Este tipo de investigación puede ser útil para personas dedicadas al área de la ciberseguridad, estudiantes que tengan interés en la gestión de vulnerabilidades en el ámbito organizacional y para empresas que deseen conocer de qué manera mejorar en su gestión de vulnerabilidades.

1.8.1.2 Selección de fuentes

En este apartado se indican las fuentes para identificar los estudios primarios para la investigación.

1.8.1.2.1 Definición del criterio de selección de fuentes

Para la selección de fuentes se tomaron en cuenta aspectos como la popularidad entre investigadores, popularidad de los sitios y el respaldo técnico y teórico con que cuenta la fuente. Además, se consideran las fuentes que contengan una gran variedad de artículos y con documentos desarrollados en fechas recientes.

1.8.1.2.2 Lenguaje de estudio

En lo que respecta a la búsqueda de información, se utiliza tanto el idioma español como el inglés.

1.8.1.2.3 Identificación de fuentes

En este apartado se describe la selección de fuentes para la

documentación primaria, además, se describe cómo se ejecutan las búsquedas y se brinda una lista de fuentes.

1. Método de selección de fuentes:

Se basa principalmente en el respaldo con el que cuenta la fuente en el área tecnológica con respecto a la publicación de estudios y documentos investigativos. Además, se considera la facilidad de acceso al sitio y para hacer las búsquedas.

2. Cadena de búsqueda:

Las cadenas de búsqueda que se utilizan tienen combinación como gestión y vulnerabilidades, *vulnerability* y *management*, ciberseguridad y empresarial, manejo y vulnerabilidades, ciberseguridad y empresarial.

3. Lista de fuentes:

Se considera el uso de las siguientes fuentes:

- Google Scholar
- ACM digital library
- IEEE digital library
- Motor de búsqueda de Google

1.8.1.2.4 Selección de fuentes después de la evaluación

Los elementos para refinar la lista de fuentes dependen de la facilidad de aplicación de las cadenas de búsqueda y la calidad de los documentos. Un aspecto para tomar en cuenta es la facilidad que se tiene para acceder al material.

1.8.1.2.5 Comprobación de las fuentes

No se cuenta con criterio experto en este momento para la selección de las fuentes. Sin embargo, se escogieron las que más se utilizan para obtener documentación relacionada con tecnología y otras ramas. Se espera obtener un criterio experto para refinar la lista o agregar más, según sea necesario.

Capítulo 2. Marco teórico o conceptual

Para el desarrollo del marco conceptual de este trabajo se generó la siguiente nube de palabras, para observar de manera gráfica los conceptos más relevantes mencionados a lo largo de la investigación.

Figura 1: Nube de conceptos importantes.
Fuente: Elaboración propia generada utilizando el sitio web https://www.nubedepalabras.es

A continuación, se definen los conceptos observados en la nube de palabras, los cuales corresponden a los que tienen mayor relevancia para la investigación. Cabe mencionar que los conceptos no se desarrollan en un orden específico ni llevan algún tipo de orden por nivel de importancia. Se busca conocer su definición para brindar un margen más claro de entendimiento al estudio realizado.

2.1 Definición de ciberseguridad

De acuerdo con Microsoft (s. f.): “La ciberseguridad, también conocida

como seguridad digital, es la práctica de proteger su información digital, dispositivos y activos. Esto incluye información personal, cuentas, archivos, fotos e incluso el dinero" (s. p.). La ciberseguridad tiene como fin prioritario proteger tres aspectos fundamentales de la información, los cuales son:

- Confidencialidad: Hace referencia a garantizar que la información sea accedida únicamente por los usuarios que estén autorizados para hacerlo.
- Integridad: Busca garantizar que la información sea la que tiene que ser. Es decir, que no se modifique o elimine sin permiso, de manera malintencionada.
- Disponibilidad: El fin es lograr que se pueda tener acceso a la información y sistemas cuando se requiera sin ningún inconveniente.

2.2 Definición de ciberataque

Según Crowdstrike (2022): "Un ataque cibernético o ciberataque es un intento por parte de delincuentes cibernéticos, piratas informáticos u otros adversarios digitales de acceder a una red o sistema informático, generalmente con el propósito de alterar, robar, destruir o exponer la información" (s. p).

2.3 Definición de computación

Es posible comprender como computación a la ciencia encargada de estudiar los sistemas y computadoras que automáticamente gestionan información. Entre su campo de estudio existen distintas áreas como la estructura

de datos y algoritmos, sistemas operativos, arquitectura de computadoras y lenguajes de programación.

2.4 Definición de economía

Sevilla Arias (2015) brinda una definición técnica sobre el término economía, la cual menciona lo siguiente:

La economía es una ciencia social que estudia la forma de administrar los recursos disponibles para satisfacer las necesidades humanas. Analiza el comportamiento, las decisiones y las acciones de los humanos, es decir, estudia como las personas, empresas y gobiernos toman decisiones relacionadas con la producción, distribución y consumo (s. p.).

2.5 Definición de automatización

Según Logicbus (s. f.): “La automatización es el conjunto de elementos o procesos informáticos, mecánicos y electromecánicos que operan con mínima o nula intervención del ser humano” (s. p.).

En la actualidad, este proceso se utiliza para optimizar y mejorar otros procesos o tareas específicas en la industria o incluso en la vida cotidiana de las personas. Es importante mencionar que este es un proceso fundamental para la transformación digital y los avances tecnológicos actuales.

2.6 Definición de interconectividad

Este término surge del concepto conectividad, el cual se refiere a la capacidad de establecer conexiones o conectarse y, de esta forma, lograr comunicación entre dos elementos. A partir de esto, se puede ubicar el término interconectividad, que se utiliza a menudo en el campo de la informática como la capacidad de comunicación entre dos o más redes. De esta manera, es posible compartir recursos, acceder a bases de datos, entre otros aspectos.

2.7 Definición de tecnología

La Real Academia Española (RAE) (s. f.) define tecnología como el: “Conjunto de teorías y de técnicas que permiten el aprovechamiento práctico del conocimiento científico” (s. p.).

En la tecnología se aplican todos los conocimientos conseguidos por el ser humano a través del tiempo, para resolver algún problema determinado o satisfacer alguna necesidad en un ámbito concreto. En la actualidad, la tecnología está presente en todos los ámbitos de la vida cotidiana, de alguna forma.

2.8 Definición de redes

En el ámbito de la informática el concepto de red hace referencia a un conjunto de técnicas e interconexiones físicas que se utilizan para conectar entre sí a dos o más equipos informáticos. De esta manera, se logra intercambiar información y periféricos a gran velocidad. Un ejemplo de esto es el Internet, el cual se conoce como *la red de redes,* o bien la red más grande.

2.9 Definición de vulnerabilidad

De acuerdo con Adrián (2022): “La vulnerabilidad es la particularidad que

tiene un sujeto de poder ser lastimado. Un individuo vulnerable es susceptible a ser herido" (s. p). En lo que respecta al ámbito de la informática, de igual manera, este concepto hace referencia a una debilidad presente en una organización, capaz de ser explotada por un sujeto o entidad que puede causar daños catastróficos.

2.10 Definición de ética

La Enciclopedia Humanidades (s. f.) la define como:

La ética o filosofía moral es una de las ramas más antiguas de la filosofía, dedicada al estudio de la conducta humana, relacionada a temas como lo correcto y lo incorrecto, lo bueno y lo malo, la virtud, la felicidad y el deber (s. p).

Capítulo 3. Marco metodológico

3.1 Tipo de investigación

El propósito del presente proyecto consiste en analizar la metodología de gestión de vulnerabilidades en los sistemas informáticos de una institución financiera nacional para comparar y emitir un criterio de los hallazgos para mejorar en temas de seguridad. Por esto, se considera esta investigación evaluativa.

3.2 Alcance investigativo

Al valorar el propósito que tiene la investigación, el alcance investigativo se considera exploratorio y descriptivo, esto al tomar en cuenta que los estudios exploratorios se utilizan cuando el objetivo es examinar un tema poco estudiado. Además, los estudios de alcance descriptivo muestran situaciones, contextos, fenómenos y eventos, con el fin de medir o recolectar información sobre ellas para mostrar posteriormente con precisión sus dimensiones.

3.3 Enfoque

De acuerdo con Naranjo Zeledón (2020):

El enfoque alternativo se ubica en el paradigma pragmático. Este apego al pragmatismo permite al investigador una enorme flexibilidad en el uso de diseños mixtos, ampliamente documentados en las fuentes bibliográficas. La ganancia de ello es que no se ve obligado a encuadrarse dentro de un enfoque con diseños o métodos predefinidos, más bien utiliza lo necesario para alcanzar sus objetivos (s. p).

Al tomar en cuenta lo citado y la naturaleza del proyecto se propone

un abordaje alternativo.

3.4 Diseño

El diseño de la investigación se define con la siguiente serie de pasos: • Para identificar los procedimientos que se utilizan para el análisis de vulnerabilidades se realiza una entrevista al técnico experto encargado.

- Se aplica un escaneo de vulnerabilidades a la muestra que se seleccionó para la investigación.
- Se interpretan los resultados.
- Se identifican las oportunidades de mejora y puntos fuertes de la metodología empleada.
- Se realiza un análisis final con sus conclusiones.
- Se brindan las recomendaciones correspondientes a los interesados.

3.5 Población y muestreo

Para efectos del estudio se define como universo o población objetivo a los equipos alojados en la subred 10.1.X.X de la institución financiera, al utilizar como muestreo no probabilístico por conveniencia a 15 servidores ubicados en esta red. Esto se debe a la magnitud de equipos que se encuentran en esta subred, lo cual

hace que para efectos de la investigación sea imposible analizarlos todos tomando en cuenta recursos como costo y tiempo.

3.6 Instrumentos de recolección de datos

Yépez (2021) indica lo siguiente:

El instrumento de recolección de datos lo constituye cualquier recurso del que se vale el investigador para aproximarse a los fenómenos en estudio, y obtener de ellos la información requerida. Según Arias (2006) define las técnicas de recolección de datos como “distintas formas de obtener la información en diferentes modalidades como son oral y escrita (s. p.).

3.6.1 Entrevista

Según Mejía Jervis (2017):

La entrevista de investigación es aquella conversación cara a cara que se

da entre el investigador (entrevistador) y el sujeto de estudio (entrevistado). Con el fin de obtener información relevante sobre el tema de estudio, a través de respuestas verbales dadas por el sujeto de estudio (p. 1).

Este abordaje proporciona a la investigación una mayor flexibilidad para obtener más y mejor información que la que se logra obtener con otros instrumentos de recolección de datos. Específicamente, para este trabajo se utiliza una entrevista de investigación no estructurada.

3.6.2 Nessus

Nessus es una herramienta que se utiliza como escáner de vulnerabilidades, la cual se desarrolló Tenable, Inc. Esta herramienta permite analizar objetivos específicos o grupos de servidores, con el fin de encontrar vulnerabilidades de todo tipo de criticidad, configuraciones incorrectas en los

equipos, contraseñas predeterminadas establecidas que sean comunes o ausentes en algunas cuentas del sistema, entre otros. Además de emitir reportes con el análisis correspondiente y algunas recomendaciones.

Para efectos de la investigación se utiliza esta herramienta para realizar un escaneo y análisis a la subred definida en la población y muestra para obtener hallazgos que retroalimenten el estudio.

Capítulo 4. Análisis del diagnóstico

4.1 Metodología de gestión de vulnerabilidades

Los tipos de metodologías de gestión de vulnerabilidades pueden variar según el contexto o entorno organizacional, lo que incluye las amenazas a las que se enfrentan. Sin embargo, una metodología robusta comprende un modelo cíclico donde se abordan los siguientes puntos:

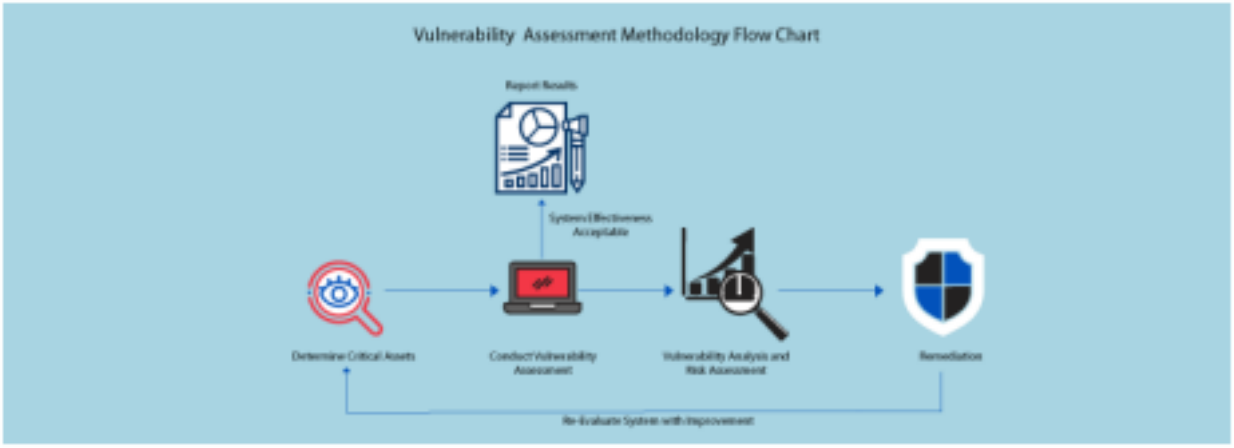


Figura 2: Diagrama de flujo de la metodología de evaluación de vulnerabilidades Fuente: Chinnasamy (2021).

4.1.1 Determinar los activos críticos de la organización

El primer paso por realizar durante la gestión de vulnerabilidades es identificar y comprender el entorno. Es necesario determinar cuáles de los activos son más críticos para mantener la operación del negocio. Además, se deben buscar las posibles amenazas de los activos que se identifican.

4.1.2 Realizar una evaluación de vulnerabilidades

Generalmente, se utilizan dos tipos de evaluación de vulnerabilidades:

Evaluación de vulnerabilidades externa: este tipo de evaluación se lleva a cabo desde la perspectiva de un intruso o atacante. Su fin es evaluar los activos y sistemas digitales de la entidad que son accesibles desde Internet. Esto permite brindar detalles sobre las vulnerabilidades que pueden detectar los piratas informáticos y que pueden explotar si no se logran solucionar a tiempo. De esta manera, se logra tener un panorama del nivel de seguridad que tiene la organización contra amenazas externas.

Evaluación de vulnerabilidades interna: Contraria a la evaluación externa, esta se realiza desde la perspectiva de un usuario interno o privilegiado de la organización. Tiene como fin evaluar los activos y sistemas de la entidad a los que se puede acceder desde dentro de la red. La evaluación de vulnerabilidades interna permite identificar debilidades que pueden explotar personas internas maliciosas, además da la posibilidad de tener un margen de la seguridad que tiene la organización contra amenazas internas.

Adicional al tipo de evaluación de vulnerabilidades que se utilice, existen algunos métodos comunes para realizar la evaluación. Entre ellos se destacan los siguientes.

4.1.2.1 Pruebas de penetración

Consiste en un tipo de prueba que busca simular un ataque real hacia los activos y sistemas de la organización. Algunas grandes organizaciones cuentan con personal especializado para realizar este tipo de pruebas, sin embargo, es común que empresas de menor escala prefieran contratar este servicio mediante una empresa externa dedicada a este fin. Las pruebas de penetración se pueden llevar a cabo de manera manual o automática, utilizando un conjunto de herramientas ofensivas o activas que intentan explotar vulnerabilidades en los sistemas.

La ventaja principal de las pruebas de penetración es identificar vulnerabilidades en la infraestructura de una organización, pero además se tiene el beneficio de descubrir debilidades emergentes acumulativas y contar con un informe de resultados de la prueba. En este informe se indica la información detallada del proceso y la lista de medidas de seguridad que se pueden implementar para prevenir una posible afectación.

En lo que respecta a las desventajas, el mayor riesgo es la interrupción del funcionamiento correcto de un sistema si el proceso no se realiza correctamente. Esto puede suceder si no se aplica un enfoque correcto para las pruebas, lo cual puede resultar en pérdidas monetarias por la interrupción de operaciones en las organizaciones o pérdida de información valiosa. Otro punto para tener en cuenta es que la organización tiene que confiar en la capacidad del probador para realizar la prueba, lo cual es riesgoso porque nunca se puede saber si alguien es lo suficientemente capaz de manejar las situaciones que surgen durante la simulación.

4.1.2.2 Escaneo de vulnerabilidades

El escaneo de vulnerabilidades es un tipo de prueba automatizada que tiene la finalidad de buscar debilidades de sistemas, utilizando una base de datos de vulnerabilidades conocidas. Cuando una herramienta de este tipo logra identificar una vulnerabilidad potencial, esta genera un informe que puede

contener información sobre cómo explotarla, una escala de gravedad de la vulnerabilidad y cómo remediarla. Un ejemplo de este tipo de herramienta es Nessus.

Entre las ventajas que se obtienen al realizar escaneos de vulnerabilidades en una organización está el aumento de la visibilidad de la postura de seguridad organizacional. Además de ser un proceso menos invasivo si se compara con las pruebas de penetración. Si este tipo de escaneos se realizan regularmente en la entidad se tiene la posibilidad de detectar posibles vulnerabilidades y así reaccionar de manera oportuna a ellas, lo que evita incidentes de seguridad.

Es importante contemplar que la organización cuente con los recursos adecuados para realizar este tipo de escaneos, por ejemplo, de procesamiento o de red, ya que si por algún motivo fueran insuficientes también pueden afectar la operación normal.

4.1.2.3 Análisis manual

El análisis manual lo realizan analistas de seguridad que revisan manualmente el código de un sistema, archivos de configuración y archivos de registro, esto con el fin de identificar posibles vulnerabilidades. Por lo general, este tipo de análisis se complementa con algunas otras pruebas automatizadas, por ejemplo, las pruebas de penetración y el análisis o escaneo de vulnerabilidades.

Realizar este tipo de análisis con personal experto puede suponer una gran ventaja, ya que, de esta manera, se puede indagar en profundidad sobre posibles vulnerabilidades que algunas herramientas automatizadas puedan pasar por alto. Sin embargo, es un análisis que se debe utilizar como complemento, debido a que por el factor humano es imposible llevar a cabo análisis de grandes volúmenes de información de forma manual en términos de eficiencia y veracidad de la información.

4.1.2.4 Gestión de riesgos

La gestión de riesgos es el proceso que se utiliza para identificar, controlar y disminuir el impacto de los eventos inciertos. El objetivo del programa de gestión de riesgos es reducir el riesgo de realizar alguna actividad o función a un nivel aceptable y obtener autorización de la dirección.

La gestión de riesgos es un enfoque proactivo de la seguridad que tiene como

objetivo ayudar a las organizaciones a identificar y reducir el impacto de posibles amenazas. Este proceso consiste en realizar los siguientes pasos:

• Identificar: identificar los riesgos potenciales de la organización. • Evaluar: evaluar la probabilidad y el impacto de cada riesgo. • Mitigar: Mitigar los riesgos con controles y procedimientos de seguridad. • Supervisar: Supervisar la eficacia de los controles.

La principal ventaja de la gestión de riesgos es que permite a las organizaciones administrar eficientemente su exposición al riesgo. De esta manera, se minimiza la pérdida ante hechos imprevistos, pero predecibles en cuanto a su probabilidad de ocurrencia.

4.1.3 Análisis de vulnerabilidades y evaluación de riesgos

Esta fase de la metodología de gestión de vulnerabilidades tiene como fin identificar la fuente y causa raíz de la debilidad de seguridad identificada en la fase dos, para tener una visibilidad coherente de la remediación. En esta etapa se busca asignar un puntaje de gravedad a cada susceptibilidad, con base en los siguientes factores:

- ¿Cuáles datos están en riesgo?
- ¿Cuál red o sistema está afectado?
- La gravedad de los posibles ataques.
- Facilidad de compromiso.
- Daño potencial si ocurre un ataque.

4.1.4 Remediación

Esta etapa tiene como objetivo principal el cierre de las brechas de seguridad encontradas. Se debe determinar el camino efectivo para la mitigación en cada vulnerabilidad que se encuentra. Algunas de las posibles acciones de remediación pueden ser las siguientes:

• Actualizar todos los cambios de configuración u operativos. • Desarrollar e implementar parches de vulnerabilidad.

• Implementar nuevas medidas, procedimientos o herramientas de seguridad.

4.1.5 Reevaluación

Después de la solución de las debilidades de seguridad encontradas, se debe volver a analizar el sistema con los cambios o actualizaciones propuestos. Esta fase tiene como fin identificar las nuevas estimaciones para la probabilidad de neutralización, probabilidad de interrupción y la probabilidad de eficacia del

sistema. Es importante repetir todo este proceso hasta que se traten de la mejor manera posible todas las vulnerabilidades de seguridad y aumente la eficacia general.

4.1.6 Informe de resultados

La última fase en la metodología de gestión de vulnerabilidades de seguridad es informar el resultado de manera comprensible. La información presentada en los informes debe ser precisa, que defina claramente la eficacia del sistema y brinde posibles soluciones en caso de que la medida de seguridad actual parezca ineficaz.

4.2 Aplicación de entrevistas a expertos

Como parte del proceso de análisis de la información se aplicaron los instrumentos de recolección de datos y se obtuvieron los siguientes resultados.

4.2.1 Aplicación de entrevista a representantes de la institución financiera de Costa Rica

A continuación, se detalla la entrevista aplicada a las personas funcionarias de la institución financiera.

4.2.1.1 Entrevista aplicada a un analista de seguridad informática Se realizó una entrevista a un analista de seguridad informática de la institución financiera y quien forma parte del centro de operaciones de seguridad de la entidad con una larga trayectoria. En la Tabla 2 se presentan las respuestas obtenidas:

Tabla 2: Respuestas obtenidas en la entrevista con el analista de seguridad informática de la institución financiera

Preguntas realizadas	Anotaciones a partir de respuestas del analista de seguridad informática

¿Cómo funciona el proceso de análisis de vulnerabilidades actualmente en la organización?	• El proceso inicia cuando alguna plataforma requiere que los equipos que albergan alguno de sus servicios a cargo en la

	CMDB se analicen en busca de vulnerabilidades. El representante o dueño del servicio debe completar un formulario con información necesaria para realizar el análisis, por ejemplo, el nombre del equipo, IP, horario por llevar a cabo el análisis, etc. Posteriormente, se ingresa una solicitud de servicio, a través de la mesa de servicio virtual, dirigida al grupo de SOC para que esta se asigne a alguno de los analistas y que se ejecute. Una vez asignada, el analista debe programar un escaneo mediante la herramienta Nessus, según el horario de ejecución que se haya definido. Una vez que el analista obtenga el reporte con los resultados, debe reenviarlo al solicitante del análisis para que este se encargue de tratar las vulnerabilidades existentes de acuerdo con su criticidad y realizar un informe con los resultados.

	• Se cuenta con el procedimiento AN03-PR77TI01 donde se detalla este proceso.
¿Qué impacto tiene este proceso para la entidad?	• Este proceso es crucial para evaluar la condición actual de la infraestructura en lo que respecta a seguridad. • Siempre se realizó de una u otra forma. En algún momento se utilizó una herramienta que causó afectación en algunas bases de datos. En la actualidad, se utiliza Nessus y hasta el momento no se ha tenido ningún inconveniente con los escaneos. • Además, se excluye el uso de fuerza bruta para no generar estrés a los equipos.
¿Cuál cree que sea una oportunidad de mejora para este proceso?	• En la actualidad, los escaneos solo se realizan por demanda, no se ha logrado implementar escaneos programados automáticamente debido a que en algunos equipos corren algunos procesos a ciertas horas del día que necesitan muchos recursos del equipo y esto les puede ocasionar estrés. Por esto, se busca que sea el

	encargado del equipo quien

	solicite el escaneo e indique el horario de ejecución. Aunque esto significa que, en algunas ocasiones, se haga únicamente 1 escaneo por semestre o 1 por año para algunos equipos. A excepción de cierta infraestructura que se rige por algunas normas como PCI y se debe analizar de manera seguida. • Además, se debe fomentar la actualización de la infraestructura obsoleta, ya que a partir de este punto surgen muchas vulnerabilidades que no se pueden corregir debido a falta de soporte. En algunos casos producción ha indicado que alguna infraestructura no se puede actualizar a una versión de sistema operativo más reciente debido a problemas con compatibilidad de algunos aplicativos, pero tampoco se ha llevado un acompañamiento con el área

	encargada de desarrollo para actualizar estos aplicativos y corregir las vulnerabilidades.

4.2.1.2 Entrevista aplicada al supervisor de seguridad operativa y ciberseguridad Se realizó una entrevista al supervisor de seguridad operativa y ciberseguridad de la institución. En la Tabla 3 se presentan las respuestas obtenidas:

Tabla 3: Respuestas obtenidas en la entrevista con el supervisor de seguridad operativa y ciberseguridad de la institución

Preguntas realizadas	Anotaciones a partir de las respuestas del supervisor de seguridad operativa y ciberseguridad
¿Cómo funciona el proceso de análisis de vulnerabilidades actualmente en la organización?	• Se cuenta con herramientas que se dedican a hacer análisis y otras que se encargan del monitoreo. Estas herramientas escanean y evidencian recomendaciones para solventar las vulnerabilidades. Está implementada una solución que realiza monitoreo 7x24 y utiliza inteligencia artificial. • Algunas herramientas que se utilizan son: Nessus, Microsoft Sentinel, Defender Security Center, Azure Identity Protection, entre otras.

	• En la actualidad, la organización utiliza marcos de referencia como NIST y Cobit para la mejora de sus procesos.

¿Cuáles son algunas ventajas y desventajas del análisis de vulnerabilidades en la organización?	• Se logran apreciar más las ventajas que las desventajas de realizarlo. El análisis de vulnerabilidades es fundamental y debe ser un proceso cíclico en el que constantemente se valore el estado de salud de los equipos. Esto permite reaccionar de forma oportuna a las vulnerabilidades y, de esta manera, aumentar el nivel de seguridad en la organización. • En algún momento no se tuvo una metodología o marco de referencia el cual seguir. Realizar este proceso sin tener un *norte* para seguir supone una desventaja en el rendimiento o realización adecuada de este proceso.

¿Cuáles cree que son algunas oportunidades de mejora para este proceso?	• Brindar autonomía al equipo de ciberseguridad para realizar acciones y depender de otras instancias. • Mejorar la estructura organizacional para unificar y fortalecer el área de ciberseguridad.

4.3 Análisis de entrevistas a expertos

4.3.1 Análisis de entrevista a los representantes de la institución financiera de Costa Rica

A continuación, se detalla el análisis de las entrevistas realizadas a los representantes de la institución.

4.3.1.1 Análisis de la entrevista con el analista de seguridad informática Se identifica la metodología que utiliza la institución en la actualidad para la gestión de vulnerabilidades. Además, se obtienen los pasos detallados con los que se realiza el proceso y documentación oficial del procedimiento.

Se logra apreciar la criticidad e importancia de este proceso para la organización. El entrevistado menciona la ventaja que supone para la entidad realizar este proceso, además de una desventaja al utilizar una herramienta que en el momento no fue la más indicada, ya que les causó afectación en su operativa. Adicionalmente, se logra obtener algunas oportunidades de mejora, desde su punto de vista, para optimizar la gestión de vulnerabilidades.

4.3.1.2 Análisis de la entrevista con el supervisor de seguridad operativa y ciberseguridad

Se logra identificar el uso de herramientas adicionales para el monitoreo de vulnerabilidades. El entrevistado menciona varias herramientas que se utilizan e indica la capacidad de monitorear el comportamiento de amenazas de seguridad 7x24.

Se logra conocer el uso de NIST como uno de los principales marcos de

referencia para la organización y la desventaja que supuso en el momento realizar este proceso sin una referencia concreta para servir de guía.

Se logra apreciar la necesidad de autonomía para el equipo de ciberseguridad, debido a las dependencias existentes actualmente.

4.4 Análisis a la metodología de gestión de vulnerabilidades Gracias a los diversos medios para recolectar información y los puntos desarrollados es posible conocer la situación actual de la entidad y se destaca lo siguiente:

La organización cuenta con una CMDB (Configuration Management Data Base), la cual almacena los datos de la composición de la infraestructura y registro de los diferentes componentes del entorno.

La evaluación de vulnerabilidades se realiza por diversas herramientas automatizadas, como escáneres, *software* de monitoreo, etc.

El análisis de las vulnerabilidades y evaluación de riesgos se basa en mayor medida en las diferentes herramientas que utilizan en la evaluación de vulnerabilidades, debido a que el proceso se realiza en parte de manera automática. Sin embargo, también se cuenta con la figura de SOC y un grupo de analistas que también interviene en esta etapa.

El punto de la remediación se realiza junto con las diferentes áreas que se encargan de los equipos o servicios.

El uso de las herramientas de monitoreo empleadas por la entidad facilita bastante la reevaluación de las vulnerabilidades gracias al monitoreo continuo. Sin embargo, no se tiene una claridad de este proceso en cuanto a los escaneos de vulnerabilidades.

Se asumen los informes finales, según lo que indica el analista de seguridad informática.

4.5 Aplicación de la herramienta Nessus

Como parte del proceso de análisis de información se realizó un escaneo a 15 equipos de la subred 10.1.X.X de la institución. En la Figura 3 se pueden apreciar las vulnerabilidades encontradas en los equipos, tomando como

referencia en el *eje y* la cantidad de equipos donde se presentó la vulnerabilidad y en el *eje x* la vulnerabilidad que se encuentra. Además, se establece un orden por

criticidad, donde las alertas críticas se muestran a la izquierda y continuando hacia la derecha disminuye su criticidad.

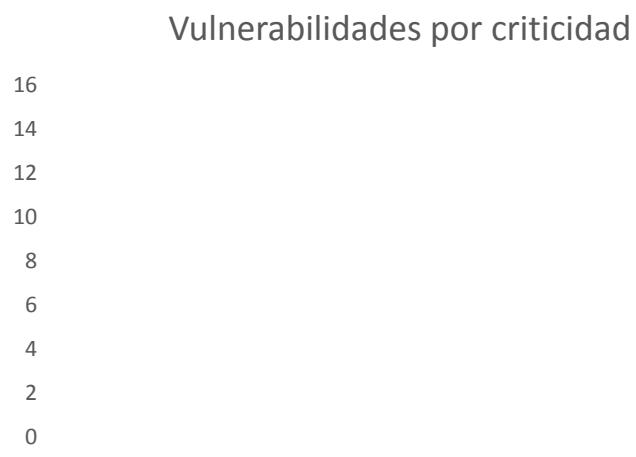


Figura 3: Gráfico de vulnerabilidades por criticidad

4.6 Análisis del escaneo con la herramienta Nessus

El reporte que creó la herramienta Nessus detalla las vulnerabilidades encontradas en cada uno de los equipos escaneados, estas se desarrollan a continuación.

4.6.1 Solución a las vulnerabilidades encontradas en los equipos analizados

A continuación, se detalla la solución para cada una de las vulnerabilidades encontradas en los equipos analizados. Estas son repetitivas en algunos equipos, por lo que se detallan los equipos que contienen estas vulnerabilidades.

4.6.1.1 Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)

El *host* remoto se ve afectado por una vulnerabilidad de ejecución remota de código en el protocolo de escritorio remoto (RDP). Un atacante remoto no autenticado puede explotar esto, a través de una serie de solicitudes diseñadas especialmente para ejecutar código arbitrario (Carvajal Ávila, 2018). Según el Common Vulnerability Scoring System (CVSS), esta vulnerabilidad tiene una puntuación crítica de 9.8.

Microsoft lanzó un conjunto de parches para corregir esta vulnerabilidad en los equipos que cuenten con Windows XP, 2003, 2008, 7 y 2008 R2. Actualizar los equipos para mantenerse al día con los parches de seguridad solventa este problema. El equipo uno cuenta con esta vulnerabilidad.

4.6.1.2 Unsupported Web Server Detection

Según su versión, el servidor web remoto está obsoleto y su vendedor o proveedor ya no lo mantiene. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto y, como resultado, puede contener vulnerabilidades de seguridad (Carvajal Ávila, 2018). De acuerdo con CVSS, esta vulnerabilidad tiene una puntuación crítica de 10.

Se debe eliminar el servidor web si ya no es necesario. De lo contrario, se debe actualizar a una versión compatible si es posible o cambiar a otro servidor. El equipo 1, equipo 9, equipo 10, equipo 12 y equipo 15 cuentan con esta vulnerabilidad.

4.6.1.3 Unsupported Windows OS (remote)

A la versión remota de Microsoft Windows le falta un paquete de servicio o ya no es compatible. Como resultado, es probable que contenga vulnerabilidades de seguridad. Según CVSS, esta vulnerabilidad tiene una puntuación crítica de 10.

Por este motivo, es necesario actualizar el sistema operativo del servidor a una versión que cuente con soporte del fabricante. El equipo 1, equipo 7, equipo 8, equipo 9, equipo 10, equipo 12, equipo 13, equipo 14 y equipo 15 cuentan con esta vulnerabilidad.

4.6.1.4 SSL Medium Strength Cipher Suites Supported

(SWEET32) De acuerdo con Carvajal Ávila (2018):

El host remoto admite el uso de cifrados SSL que ofrecen cifrado de nivel medio. Nessus considera de fuerza media cualquier encriptación que use longitudes de clave de al menos 64 bits y menos de 112 bits, o que use la suite de encriptación 3DES. Se debe tener en cuenta que es considerablemente más fácil eludir el cifrado de nivel medio si el atacante está en la misma red física (p. 75).

Según CVSS, esta vulnerabilidad tiene una puntuación alta de 7.5. Por lo tanto, se debe volver a configurar la aplicación afectada si es posible para evitar el uso de cifrados de intensidad media. El equipo 1, equipo 3, equipo 4, equipo 5, equipo 6, equipo 7, equipo 8, equipo 9, equipo 10, equipo 11, equipo 12, equipo 13, equipo 14 y equipo 15 cuentan con esta vulnerabilidad.

4.6.1.5 TLS Version 1.0 Protocol Detection

El servicio remoto acepta conexiones cifradas mediante TLS 1.0, el cual tiene varios defectos de diseño criptográfico. Las implementaciones modernas de TLS 1.0 mitigan estos problemas, pero las versiones más nuevas de TLS como 1.2 y 1.3 están diseñadas para estos defectos y deben usarse siempre que sea posible (Carvajal Ávila, 2018).

Los dispositivos que no están habilitados para TLS 1.2 y superior ya no funcionan correctamente con los principales navegadores web y los principales proveedores.

Según CVSS, esta vulnerabilidad tiene una puntuación media de 6.5.

Se debe habilitar la compatibilidad con TLS 1.2 y 1.3 y deshabilitar la compatibilidad con TLS 1.0. El equipo 1, equipo 2, equipo 3, equipo 4, equipo 5, equipo 6, equipo 7, equipo 8, equipo 9, equipo 10, equipo 11, equipo 12, equipo 13, equipo 14 y equipo 15 cuentan con esta vulnerabilidad.

4.6.1.6 SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

bits Según Carvajal Ávila (2018):

Al menos uno de los certificados X.509 enviados por el host remoto tienen una clave de menos de 2048 bits. De acuerdo con los estándares de la industria

establecidos por el foro de la autoridad de certificación/navegador (CA/B), los certificados emitidos después del 1 de enero de 2014 deben tener al menos 2048

bits. Algunas implementaciones SSL de navegador pueden rechazar claves de menos de 2048 bits después del 1 de enero de 2014. Además, algunos proveedores de certificados SSL pueden revocar certificados de menos de 2048 bits antes del 1 de enero de 2014 (s. p.).

CVSS no registra una puntuación para esta vulnerabilidad. Es necesario remplazar el certificado que contiene una clave RSA de menos de 2048 bits de longitud por uno con una clave más larga. Además, se debe emitir cualquier certificado firmado por el certificado anterior. El equipo 2, equipo 3, equipo 4, equipo 7, equipo 8, equipo 13 y equipo 15 cuentan con esta vulnerabilidad.

4.6.1.7 TLS Version 1.1 Protocol Deprecated

El servicio remoto acepta conexiones cifradas mediante TLS 1.1, el cual no es compatible con los conjuntos de cifrado actuales y recomendados. “A partir del 31 de marzo de 2020, los dispositivos que no estén habilitados para TLS 1.2 y versiones posteriores ya no funcionarán correctamente con los principales navegadores web y los principales proveedores” (Boisson Morales, 2020). Según CVSS, esta vulnerabilidad tiene una puntuación media de 6.5.

Se debe habilitar la compatibilidad con TLS 1.2 o 1.3 y deshabilitar la compatibilidad con TLS 1.1. El equipo 3, equipo 4, equipo 5, equipo 6, equipo 7, equipo 9, equipo 10, equipo 11, equipo 12, equipo 14 y equipo 15 cuentan con esta vulnerabilidad.

4.6.1.8 SSL Certificate Expiry

Este complemento comprueba las fechas de caducidad de los certificados asociados con los servicios habilitados para SSL en el destino e informa si alguno ya ha caducado, lo que significa que en este equipo residen uno o más certificados expirados.

Se requiere comprar o generar un nuevo certificado SSL para reemplazar el existente que se encuentra expirado. El equipo 3 y el equipo 4 cuentan con esta vulnerabilidad.

4.6.1.9 Microsoft SQL Server Unsupported Version Detection (remote check)

Según su número de versión autorreportado, ya no se soporta la instalación de

Microsoft SQL Server en el *host* remoto: “La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad” (Guevara Rivera y Téllez Castillo, 2020, p. 66). De acuerdo con CVSS, esta vulnerabilidad tiene una puntuación crítica de 10.

Es necesario actualizar la versión de Microsoft SQL Server que se encuentra instalada en el equipo, a una versión que cuente con soporte del fabricante. El equipo 5, equipo 7, equipo 8 y equipo 15 cuentan con esta vulnerabilidad.

4.6.1.10 HSTS Missing from HTTPS Server (RFC 6797)

De acuerdo con Guevara Rivera y Téllez Castillo (2020):

> El servidor web remoto no aplica HSTS, según lo define RFC 6797. HSTS es un encabezado de respuesta opcional que se puede configurar en el servidor para indicarle al navegador que solo se comunique a través de HTTPS. La falta de HSTS permite ataques de degradación, ataques de hombre en el medio que eliminan SSL y debilita las protecciones de secuestro de cookies (p. 66).

De acuerdo con CVSS, esta vulnerabilidad tiene una puntuación media de 6.5. Por lo tanto, se debe configurar el servidor web para utilizar HSTS. El equipo 6 cuenta con esta vulnerabilidad.

4.6.1.11 SSL Version 2 and 3 Protocol Detection

El servicio remoto acepta conexiones cifradas mediante SSL 2.0 o SSL 3.0. Estas versiones de SSL están afectadas por varias fallas criptográficas, que incluyen:

- Un esquema de relleno inseguro con cifrados CBC.

- Esquemas inseguros de renegociación y reanudación de sesiones.

Un atacante puede explotar estas fallas para realizar ataques de hombre en el medio o para descifrar las comunicaciones entre el servicio afectado y los clientes. Aunque SSL/TLS tiene un medio seguro para elegir la versión más compatible del protocolo, muchos navegadores web lo implementan de una manera insegura que permite que un atacante degrade una conexión (como en Poodle). Por lo tanto, se recomienda que estos protocolos se deshabiliten por

completo (Bolaños González *et al.*, 2018).

NIST determinó que SSL 3.0 ya no es aceptable para comunicaciones seguras. A partir de la fecha de aplicación que se encuentra en PCI DSS v3.1, cualquier versión de SSL no cumplirá con la definición de *criptografía fuerte* de PCI SSC (Bolaños González *et al.*, 2018). Según CVSS, esta vulnerabilidad tiene una puntuación crítica de 9.8. Por ende, se debe deshabilitar SSL 2.0 y 3.0 y utilizar TLS 1.2 o superior en su lugar. El equipo 7, equipo 8 y equipo 13 cuentan con esta vulnerabilidad.

4.6.1.12 Microsoft Windows Server 2003 Unsupported Installation

Detection Según Gamboa Castillo y Ruano Gamboa (2019):

El host remoto ejecuta Microsoft Windows Server 2003. El soporte para este sistema operativo por parte de Microsoft finalizó el 14 de julio de 2015. La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto y como resultado, es probable que contenga vulnerabilidades de seguridad. Además, es poco probable que Microsoft investigue o reconozca los informes de vulnerabilidades (p. 67).

Según CVSS, esta vulnerabilidad tiene una puntuación crítica de 10. Se debe actualizar la versión del sistema operativo del equipo a una versión que cuente con soporte del fabricante. El equipo 8 y el equipo 13 cuentan con esta vulnerabilidad.

4.6.1.13 Microsoft Windows SMBv1 Multiple Vulnerabilities El *host* remoto de Windows tiene habilitado el protocolo Server Message Block (SMBv1). Por lo tanto, se ve afectado por múltiples vulnerabilidades:

- Existen múltiples vulnerabilidades de divulgación de información en SMBv1 debido al manejo inadecuado de los paquetes. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de un paquete SMBv1 especialmente diseñado, para revelar información confidencial. (CVE-2017-0267, CVE-2017-0268, CVE-2017-0270, CVE-2017-0271, CVE-2017-0274, CVE-2017- 0275, CVE-2017-0276)

Además, un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de un paquete SMBv1 especialmente diseñado, para

ejecutar código arbitrario. (CVE-2017-0272, CVE-2017-0277, CVE-2017-0278, CVE-2017-0279)

- También existen múltiples vulnerabilidades de denegación de servicio en SMBv1 debido al manejo inadecuado de las solicitudes. Un atacante remoto no autenticado puede explotar estas vulnerabilidades, a través de una solicitud SMB especialmente diseñada, para hacer que el sistema deje de responder. (CVE 2017-0269, CVE-2017-0273, CVE-2017-0280) (Guevara Rivera y Téllez Castillo, 2020, p. 69)

Según CVSS, esta vulnerabilidad tiene una puntuación alta de 8.1. Para corregir la vulnerabilidad se deben aplicar los siguientes parches según la versión de sistema operativo:

- Windows Server 2008: KB4018466
- Windows 7: KB4019264
- Windows Server 2008 R2: KB4019264
- Windows Server 2012: KB4019216
- Windows 8.1/RT 8.1: KB4019215
- Windows Server 2012 R2: KB4019215
- Windows 10: KB4019474

- Windows 10 Version 1511: KB4019473
- Windows 10 Version 1607: KB4019472
- Windows 10 Version 1703: KB4016871
- Windows Server 2016: KB4019472

El equipo 8 y el equipo 13 cuentan con esta vulnerabilidad

4.6.1.14 SMB NULL Session Authentication

Es posible iniciar sesión por medio del protocolo SMB utilizando una sesión nula, es decir, sin usuario ni contraseña. Según la configuración es posible que un atacante remoto no autenticado aproveche este problema para obtener información sobre el *host* remoto. De acuerdo con CVSS, esta vulnerabilidad tiene una puntuación alta de 7.3.

Es posible que un atacante remoto pueda iniciar sesión en el *host* con una sesión nula, por lo que se requiere validar esta configuración y en caso de que sea necesario involucrar al proveedor del producto para conocer las soluciones que se

recomiendan. El equipo 8 y el equipo 13 cuentan con esta vulnerabilidad. **4.6.1.15 MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)**

Según Guevara Rivera y Téllez Castillo (2020):

El host remoto de Windows se ve afectado por una vulnerabilidad de elevación de privilegios en los protocolos del administrador de cuentas de seguridad (SAM) y la autoridad de seguridad local (política de dominio) (LSAD) debido a una negociación incorrecta del nivel de autenticación en los canales de llamada a procedimiento remoto (RPC) (p. 83).

Un ataque de hombre en el medio es capaz de interceptar las comunicaciones entre un cliente y un servidor que aloja una base de datos SAM y puede aprovechar esto para forzar la degradación del nivel de autenticación. Esto le permite al atacante hacerse pasar por un usuario autenticado y acceder a la base de datos SAM (Guevara Rivera y Téllez Castillo, 2020). Según CVSS, esta vulnerabilidad tiene una puntuación media de 6.8.

Microsoft lanzó un conjunto de parches para corregir esta vulnerabilidad en los equipos que cuenten con Windows Vista, 2008, 7, 2008 R2, 2012, 8.1, RT 8.1, 2012 R2 y 10. El actualizar los equipos para mantenerse al día con los parches de seguridad solventa este problema. El equipo 8 y el equipo 13 cuentan con esta vulnerabilidad.

4.6.1.16 Microsoft Windows EFSRPC NTLM Reflection Elevation of Privilege (PetitPotam) (Remote)

El *host* remoto se ve afectado por una vulnerabilidad de elevación de privilegios de reflejo NTLM conocida como *PetitPotam*. Un atacante remoto no autenticado puede explotar esto, enviando una solicitud EFSRPC diseñada especialmente para hacer que el *host* afectado se conecte a un servidor malicioso. Después, un atacante puede utilizar una retransmisión NTLM para hacerse pasar por el *host* de destino y autenticarse en servicios remotos. Según CVSS, esta vulnerabilidad tiene una puntuación media de 5.3.

Se deben aplicar las actualizaciones proporcionadas por el proveedor. Opcionalmente, se puede consultar el documento KB5005413 de Microsoft para orientarse sobre la mitigación. Además, se pueden implementar filtros RPC para

bloquear el acceso remoto a los UUID de la interfaz necesarios para este *exploit*. El equipo 8 cuenta con esta vulnerabilidad.

4.6.1.17 Remote Desktop Protocol Server Man-in-the-Middle Weakness La versión del protocolo de escritorio remoto en el servidor es vulnerable a un ataque de hombre en el medio. El cliente RDP no hace ningún esfuerzo por validar la identidad del servidor al configurar el cifrado. Un atacante con la capacidad de interceptar el tráfico del servidor RDP puede establecer el cifrado con el cliente y el servidor sin ser detectado. Un ataque de hombre en el medio de esta naturaleza permite al atacante obtener cualquier información confidencial transmitida, incluidas las credenciales de autenticación (Guevara Rivera y Téllez Castillo, 2020).

Esta falla existe porque el servidor RDP almacena una clave privada RSA codificada conocida públicamente. Cualquier atacante en una ubicación de red privilegiada puede usar la clave para este ataque.

Se debe forzar el uso de SSL como una capa de transporte para este servicio si es compatible. En los sistemas operativos Microsoft Windows, se puede seleccionar la configuración *Permitir conexiones solo desde computadoras que ejecutan escritorio remoto con autenticación de nivel de red* si está disponible. El equipo 8 cuenta con esta vulnerabilidad.

4.6.1.18 Oracle Database Unsupported Version Detection

Según su versión, ya no se admite la base de datos Oracle instalada en el *host* remoto. “La falta de soporte implica que el proveedor no lanzará nuevos parches de seguridad para el producto. Como resultado, es probable que contenga vulnerabilidades de seguridad” (Guevara Rivera y Téllez Castillo, 2020, p. 66). De acuerdo con CVSS, esta vulnerabilidad tiene una puntuación crítica de 10.

Por este motivo, es necesario actualizar la versión de base de datos Oracle a una que cuente con soporte del fabricante. El equipo 13 cuenta con esta vulnerabilidad.

4.6.1.19 Oracle Database Multiple Remote Vulnerabilities (Mar, 2005) La base de datos Oracle remota, según su número de versión, contiene una vulnerabilidad de ejecución de comandos remotos que puede permitir que un atacante que puede ejecutar declaraciones SQL con ciertos privilegios ejecute comandos

arbitrarios en el *host* remoto. De acuerdo con CVSS, esta vulnerabilidad tiene una puntuación alta de 7.5.

Oracle lanzó un conjunto de parches para corregir esta vulnerabilidad en las bases de datos. Aplicar los parches que brinda el proveedor solventa este problema. El equipo 13 cuenta con esta vulnerabilidad.

4.6.1.20 Anonymous FTP Enabled

Nessus encontró que el servidor FTP que se ejecuta en el *host* remoto permite inicios de sesión anónimos. Por lo tanto, cualquier usuario remoto puede

conectarse y autenticarse en el servidor sin proporcionar una contraseña o credenciales únicas. Esto le da la posibilidad al usuario de acceder a cualquier archivo que el servidor FTP haya puesto a su disposición. Según CVSS, esta vulnerabilidad tiene una puntuación media de 5.3.

Se debe deshabilitar el FTP anónimo si no es necesario, además de verificar rutinariamente el servidor FTP para asegurarse de que el contenido confidencial no esté disponible. El equipo 13 cuenta con esta vulnerabilidad. **4.6.1.21 Oracle 8i/9i Database Server UTL_FILE Traversal Arbitrary File Manipulation**

Según su número de versión, se informa que la instalación de Oracle en el *host* remoto está sujeta a múltiples vulnerabilidades de cruce de directorios que pueden permitir que un atacante remoto lea, escriba o cambie el nombre de archivos arbitrarios con los privilegios del servidor de Oracle Database. Un usuario autenticado puede crear consultas SQL, de modo que pueda recuperar cualquier archivo en el sistema y recuperar potencialmente o modificar archivos en la misma unidad que la aplicación afectada. De acuerdo con CVSS, esta vulnerabilidad tiene una puntuación media de 6.5.

Oracle lanzó un conjunto de parches para corregir esta vulnerabilidad en las bases de datos. Aplicar los parches que brinda el proveedor solventa este problema. El equipo 13 cuenta con esta vulnerabilidad.

4.6.1.22 Oracle Database Listener Program (tnslsnr) Service Blank Password

El programa Oracle Listener remoto (tnslsnr) no tiene asignada una contraseña. Un atacante puede usar este hecho para apagarlo arbitrariamente y evitar que los usuarios legítimos lo usen. Según CVSS, esta vulnerabilidad tiene

una puntuación media de 5.

Se debe utilizar el comando lsnrctrl CHANGE_PASSWORD para asignar una contraseña al *listener* de la base de datos. El equipo 13 cuenta con esta vulnerabilidad.

41

4.6.1.23 FTP Supports Cleartext Authentication

El servidor FTP remoto permite que el nombre y la contraseña del usuario se transmitan en texto no cifrado, lo que puede interceptar un rastreador de red o un ataque de intermediario. Según CVSS, esta vulnerabilidad tiene una puntuación baja de 2.6.

Es necesario cambiar a SFTP (parte de la *suite* SSH) o FTP (FTP sobre SSL/TLS). En el último caso configurar el servidor para que las conexiones de control estén encriptadas. El equipo 13 cuenta con esta vulnerabilidad. **4.6.1.24 Oracle Database 9i/10g Fine Grained Auditing (FGA) SELECT Statement Logging Weakness**

El *host* remoto ejecuta una versión de Oracle Database que sufre una falla en la que la auditoría detallada (FGA) se desactiva cuando el usuario SYS ejecuta una declaración SELECT. Según CVSS, esta vulnerabilidad tiene una puntuación baja de 2.6. En este caso, es necesario aplicar el conjunto de parches 10.1.0.4 para Oracle 10g. El equipo 13 cuenta con esta vulnerabilidad.

42

Capítulo 5. Propuesta de solución

5.2 Propuesta para mejorar la seguridad en los sistemas informáticos de la institución

La gestión de vulnerabilidades es un tema de vital importancia para toda organización y cabe destacar que no todas las organizaciones son conscientes de esto o no cuentan con alguna metodología que les permita realizar este proceso. La entidad en estudio tiene una base sólida en lo que respecta a este tema, tomando como referencia la metodología analizada en el punto 4.1. La empresa realiza este proceso cíclico por medio de varias herramientas, sin embargo, existe la posibilidad de mejorar esta gestión.

El primer aspecto que se puede optimizar es la periodicidad en la que se realizan los escaneos de vulnerabilidades en sus equipos. En la actualidad, los escaneos

se llevan a cabo únicamente por demanda mediante una solicitud al SOC de la organización, lo cual puede permitir que, por algún factor como el olvido, no se haga el escaneo a algún equipo o equipos en un lapso prudente. Se propone establecer una periodicidad de 2 a 3 meses para los escaneos de vulnerabilidades de la infraestructura crítica y una periodicidad máxima de 6 meses para los equipos de baja criticidad.

Adicionalmente, es importante implementar una comprobación, mediante un nuevo análisis de vulnerabilidades, para detectar que las vulnerabilidades registradas en el informe anterior se trataron de la manera adecuada. Efectivamente, como se detalla en el punto 4.1.5 la reevaluación es relevante para tratar las vulnerabilidades de la mejor forma posible.

En el análisis realizado a la muestra de equipos de la institución se encontró que existen equipos obsoletos o fuera de soporte, con procesos críticos para la organización, lo cual expone a la entidad a un grado de riesgo alto ante algún evento. Se recomienda abordar el caso mediante la actualización de los equipos, para contar al menos con infraestructura que tenga soporte por parte de los fabricantes. En caso de que esto no sea posible por alguna dependencia, se debe analizar la manera de mitigar el riesgo.

Asimismo, se propone realizar algunas pruebas más invasivas, como las pruebas de penetración, de manera controlada para valorar los resultados que se puedan obtener. De esta forma, enfrentarse a escenarios de la vida real y tener un panorama más amplio de la seguridad de la infraestructura.

El uso de herramientas de monitoreo táctico supone una gran ventaja para la organización gracias a que existe un Departamento de SOC que mantiene un monitoreo continuo 7x24. Se recomienda aprovechar su uso y optimizarlas de la mejor manera posible para depurar falsos positivos que se puedan encontrar.

Por último, se propone realizar periódicamente pruebas de *phishing* a las personas colaboradoras de la organización. Lo anterior con el fin de fomentar la educación en este tema y concientizar la importancia del factor humano en temas de seguridad organizacional.

Capítulo 6. Conclusiones

Es estrictamente necesario para una entidad bancaria ejecutar

periódicamente análisis de vulnerabilidades en su infraestructura, debido a la criticidad de sus funciones operativas. Además del riesgo reputacional y económico de la empresa en caso de la explotación de alguna vulnerabilidad en su infraestructura.

A partir del estudio realizado se logra comprender las ventajas y desventajas de la ejecución de los análisis de vulnerabilidades en entidades bancarias, con base en la posibilidad de atacar las vulnerabilidades de una manera oportuna y contar con una infraestructura segura para sus funciones. Además de conocer el impacto que implica realizarlo de una forma que no sea la adecuada o no realizarlo, lo cual conlleva un riesgo muy alto para la organización, debido a que está expuesta a ser vulnerada por múltiples tipos de ataques que utilizan los ciberdelincuentes o incluso una amenaza interna.

Además, se logró conocer algunas metodologías que se pueden utilizar para llevar a cabo un análisis de vulnerabilidades, como las pruebas de penetración, escaneos de vulnerabilidades, análisis manuales y la gestión de riesgos.

Por último, se realizó un análisis de vulnerabilidades a una muestra de equipos de una institución financiera nacional. Gracias a esto, se pudieron obtener resultados reales de la infraestructura de la organización y con esto brindar soluciones para mejorar la seguridad en su infraestructura de producción.

Referencias

Adrián, Y. (2022, 8 de julio). *Vulnerabilidad*. Concepto de-definición de. https://conceptodefinicion.de/vulnerabilidad/

Boisson Morales, N. (2010). *Aplicación de la metodología PTES en la Clínica Medellín para la identificación de vulnerabilidades en historia clínica electrónica*. Universidad Nacional Abierta y a Distancia. https://repository.unad.edu.co/bitstream/handle/10596/40837/nboissonm--.pdf?isAllowed=y&sequence=3

Bolaños González, H.; Cruz Cuellar, J. M. y Reyes Peñaloza, J. (2018). *Identificación y propuesta de una solución de mejora a las vulnerabilidades informáticas de la red y del ambiente de servidores de preproducción de la*

entidad Keralty. Universidad El Bosque. https://repositorio.unbosque.edu.co/bitstream/handle/20.500.12495/8143/Do cumentoFinal_EPI-084.pdf?sequence=1&isAllowed=y

Business Continuity Institute. (2013). *Good Practice Guidelines: A guide to global good practice in business continuity*. Business Continuity Institute, Caversham.

Carvajal Ávila, M. (2018). *Análisis de vulnerabilidades de la infraestructura tecnológica de la organización caso de estudio*. Universidad Nacional Abierta y a Distancia. https://repository.unad.edu.co/bitstream/handle/10596/25715/%20%09maca rvajalav.pdf?sequence=4&isAllowed=y

Casas Pinto, J. G. y Ramírez León, D. F. (s. f.). *Metodología para la optimización en la gestión de vulnerabilidades en Banco de Occidente (posgrado)*. Universidad Piloto de Colombia.

Chinnasamy, V. (2021, 20 de mayo). *Explore Vulnerability Assessment Types and Methodology. Indusface*. https://www.indusface.com/blog/explore vulnerability-assessment-types-and-methodology/

Consulting. (s. f.). *Metodología para realizar el análisis de vulnerabilidades o test de intrusión*.

CrowdStrike. (2022, 15 de agosto). *What is a Cyberattack? Types and Examples.* https://www.crowdstrike.com/cybersecurity-101/cyberattacks/

Disaster Recovery Institute International (DRII). (2012). *Professional Practices for Business Continuity Practitioners*.

Enciclopedia Humanidades. (s. f.). *¿Qué es la ética?* https://humanidades.com/etica/#:~:text=La%20%C3%A9tica%2C%20o%20filosof%C3%ADa%20moral,el%20campo%20de%20la%20moralidad.

Gamboa Castillo, A. y Ruano Gamboa, E. (2019). *Estudio de vulnerabilidades, amenazas y gestión del riesgo en el Hospital Departamental Psiquiátrico Universitario del Valle E.S.E*. Universidad Nacional Abierta y a Distancia. https://repository.unad.edu.co/bitstream/handle/10596/36641/erujanog.pdf?i

sAllowed=y&sequence=3

Garzón, D.; Ratkovich Gomes, J. C. y Vergara Torres, A. (s. f.). *Metodología de análisis de vulnerabilidades para empresas de media y pequeña escala*. Pontificia Universidad Javeriana.

Guevara Rivera, J. y Téllez Castillo, H. (2020). *Análisis de seguridad de la infraestructura de red en compañía multinacional del sector industrial*. Universidad El Bosque. https://repositorio.unbosque.edu.co/bitstream/handle/20.500.12495/4448/Guevara_Rivera_Julian_David_2020.pdf

ISO 22301. (2012). *Societal security - Business continuity management systems - Requirements*.

ISO 22301. (2012). *Societal security - Business continuity management systems - Guidance ISO 22301*. (2012). - *Societal security - Terminology*.

ISO 27001. (2013). *Information security*.

Logicbus. (s. f.). *Logicbus-Que es, concepto, historia y usos de la automatización*. https://www.logicbus.com.mx/automatizacion.php

Massoni, A. (2022, 20 de noviembre). *Las ventajas de utilizar un escáner de vulnerabilidades en tu organización*. Hacknoid. https://www.hacknoid.com/hacknoid/las-ventajas-de-utilizar-un-escaner-de vulnerabilidades-en-tu-organizacion/

Mejía Jervis, T. (2017). *Entrevista de Investigación: Tipos y Características*.

Microsoft. (s. f.). *¿Qué es la ciberseguridad?* https://support.microsoft.com/es es/topic/-qu%C3%A9-es-la-ciberseguridad-8b6efd59-41ff-4743-87c8-0850a352a390

Mora Mora, L. P. (2010). *Ciberseguridad en Costa Rica*. Prosic.

Naranjo Zeledón, L. (2020). *Investigación en Informática: el enfoque alternativo*. Technology Inside by CPIC, 5, 1-15.

Navarro, M. (2020, 3 de junio). *Invertir en ciberseguridad: la necesidad obligatoria*. Revista Byte TI. https://revistabyte.es/tema-de-portada-byte-ti/invertir-en

ciberseguridad-la-necesidad-obligatoria/

Petrosyan, K. (2022, 23 de mayo). *Beneficios y riesgos de las pruebas de penetración*. EasyDMARC. https://easydmarc.com/blog/es/beneficios-y riesgos-de-las-pruebas-de-penetracion/

Real Academia Española (RAE). (s. f.). *Diccionario esencial de la lengua española*. https://www.rae.es/desen/tecnolog%2525C3%2525ADa

Sevilla Arias, A. (2022, 14 de septiembre). *Economía*. Economipedia. https://economipedia.com/definiciones/economia.html

Tagade, K. (2022, 25 de abril). *NIST Penetration Testing: Guide, Framework and How to Achieve Security Compliance*. Astra Security Blog. https://www.getastra.com/blog/security-audit/vulnerability-assessment methodology/

Tenable. (s. f.). *Herramientas y programas de gestión de vulnerabilidades y amenazas*. https://es-la.tenable.com/source/vulnerability-management

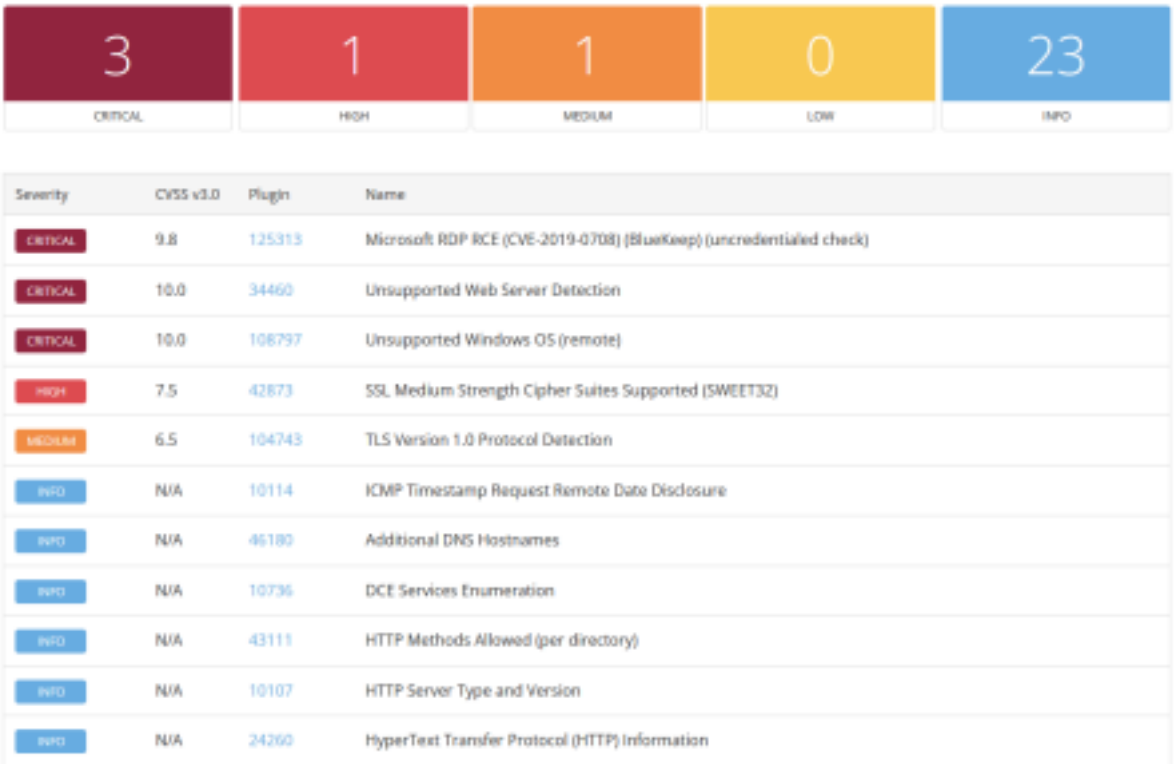
Westcon-Comstor, E. S. (s. f.). *Gestión de vulnerabilidades: ¿qué es y cómo ponerla en práctica?* https://digital.la.synnex.com/gestion-de vulnerabilidades-que-es-y-como-ponerla-en-practica

Yépez, W. (2021). *Técnicas e instrumentos de recolección de datos*. https://biblogteca.com/tecnicas-e-instrumentos-de-recoleccion-de-datos /

Apéndice A. Reportes de escaneo de los equipos

A continuación, se detallan las vulnerabilidades detectadas por la herramienta Nessus en los equipos analizados.

Equipo 1:



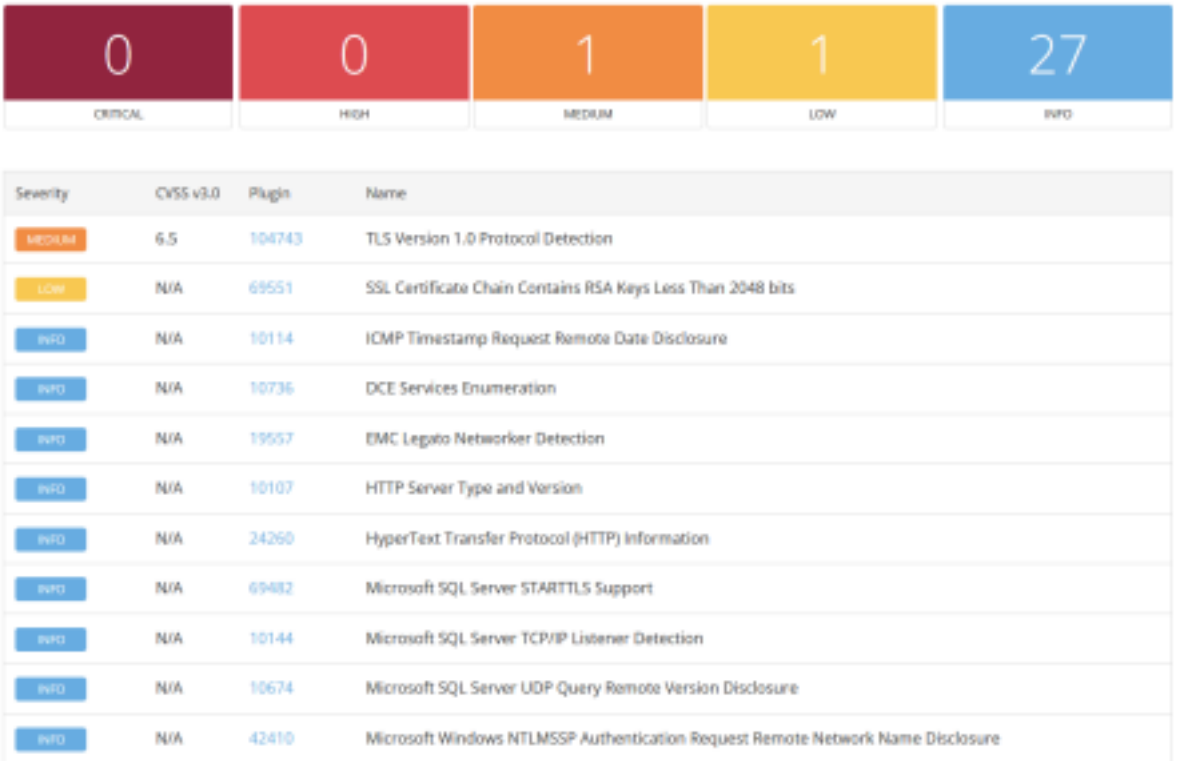
3	1	1	0	23
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	Plugin	Name
CRITICAL	9.8	125313	Microsoft RDP RCE (CVE-2019-0708) (BlueKeep) (uncredentialed check)
CRITICAL	10.0	34460	Unsupported Web Server Detection
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	104743	TLS Version 1.0 Protocol Detection
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	46180	Additional DNS Hostnames
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information

Figura 4: Herramienta Nessus

Fuente: Reporte de escaneo de la aplicación.

Equipo 2:



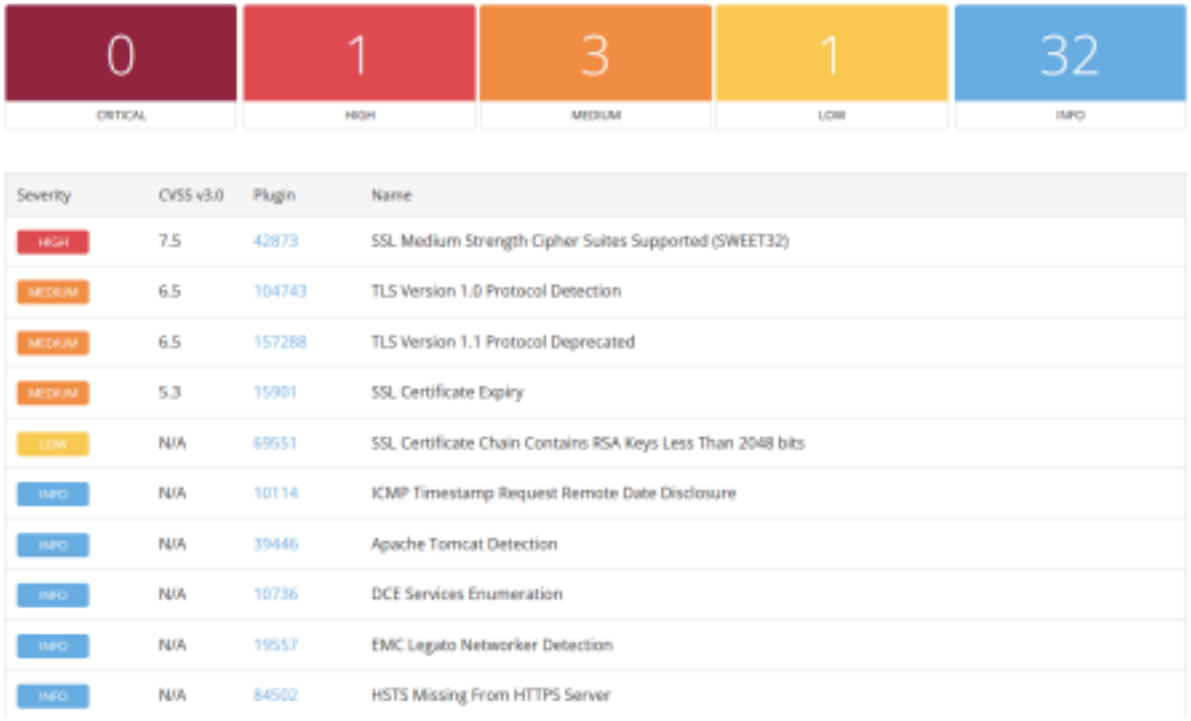
0	0	1	1	27
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	Plugin	Name
MEDIUM	6.5	104743	TLS Version 1.0 Protocol Detection
LOW	N/A	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	19557	EMC Legato Networker Detection
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	69482	Microsoft SQL Server STARTTLS Support
INFO	N/A	10144	Microsoft SQL Server TCP/IP Listener Detection
INFO	N/A	10674	Microsoft SQL Server UDP Query Remote Version Disclosure
INFO	N/A	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure

Figura 5: Herramienta Nessus

Fuente: Reporte de escaneo de la aplicación.

Equipo 3:



0	1	3	1	32
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	Plugin	Name
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	157288	TLS Version 1.1 Protocol Deprecated
MEDIUM	5.3	15901	SSL Certificate Expiry
LOW	N/A	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	39446	Apache Tomcat Detection
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	19557	EMC Legato Networker Detection
INFO	N/A	84502	HSTS Missing From HTTPS Server

Figura 6: Herramienta Nessus

Fuente: Reporte de escaneo de la aplicación.

Equipo 4:

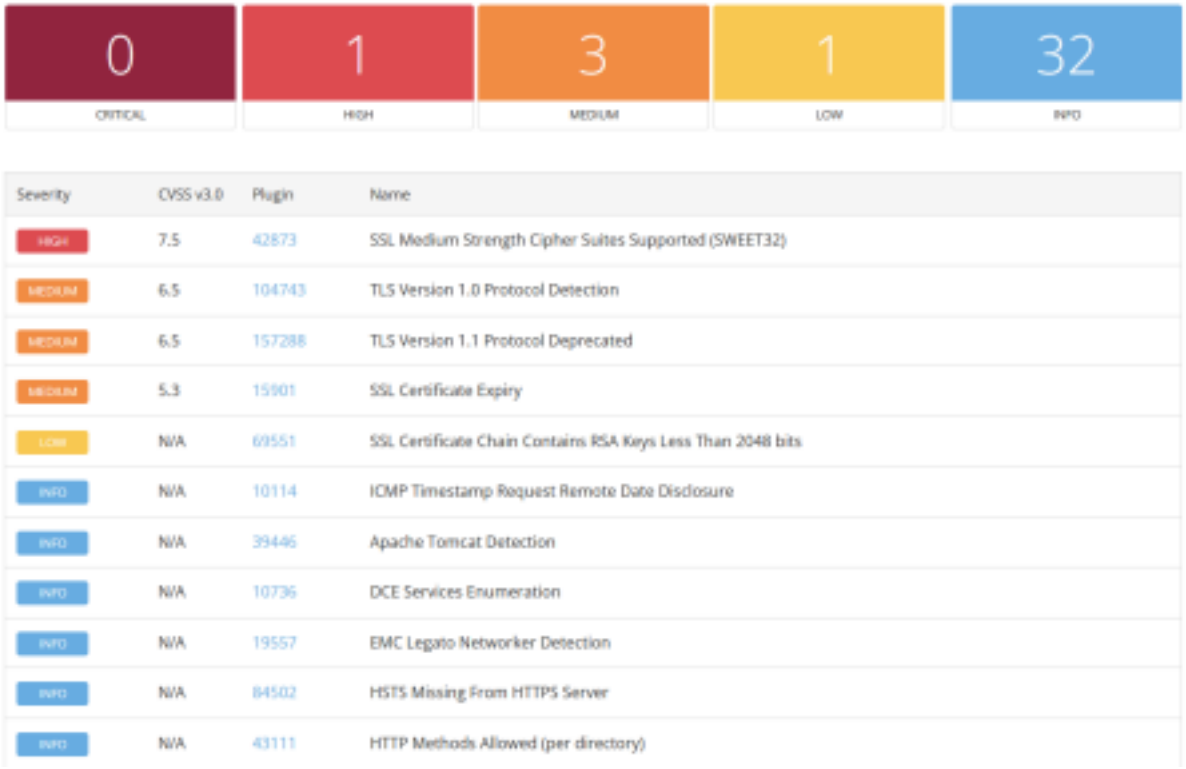


Figura 7: Herramienta Nessus

Fuente: Reporte de escaneo de la aplicación.

Equipo 5:

Severity	CVSS v3.0	Plugin	Name
CRITICAL	10.0	73756	Microsoft SQL Server Unsupported Version Detection (remote check)
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	157288	TLS Version 1.1 Protocol Deprecated
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	84502	HSTS Missing From HTTPS Server
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information

Figura 8: Herramienta Nessus

Fuente: Reporte de escaneo de la aplicación.

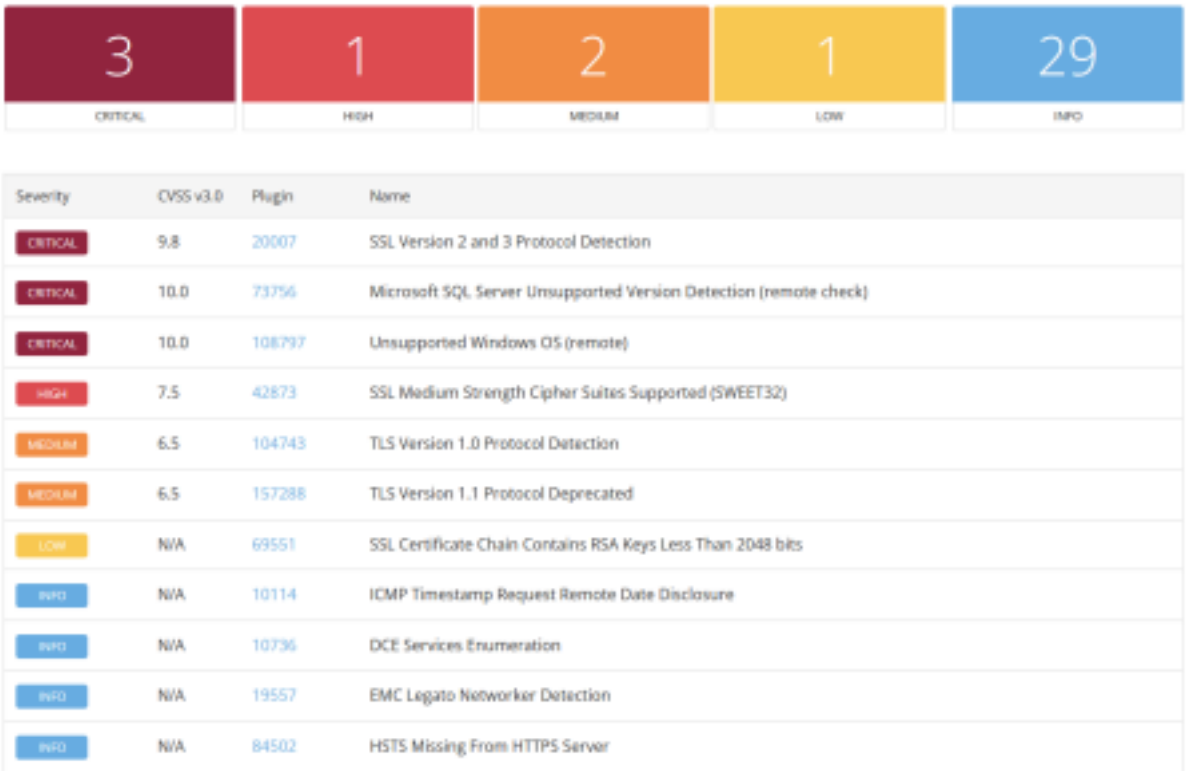
Equipo 6:

Severity	CVSS v3.0	Plugin	Name
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	142960	HSTS Missing From HTTPS Server (RFC 6797)
MEDIUM	6.5	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	157288	TLS Version 1.1 Protocol Deprecated
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	84502	HSTS Missing From HTTPS Server
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	57034	IBM WebSphere Application Server Detection
INFO	N/A	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure

Figura 9: Herramienta Nessus

Fuente: Reporte de escaneo de la aplicación.

Equipo 7:



3	1	2	1	29
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	Plugin	Name
CRITICAL	9.8	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	73756	Microsoft SQL Server Unsupported Version Detection (remote check)
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	157288	TLS Version 1.1 Protocol Deprecated
LOW	N/A	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	19557	EMC Legato Networker Detection
INFO	N/A	84502	HSTS Missing From HTTPS Server

Figura 10: Herramienta Nessus

Fuente: Reporte de escaneo de la aplicación.

Equipo 8:

Severity	CVSS v3.0	Plugin	Name
CRITICAL	9.8	20007	SSL Version 2 and 3 Protocol Detection
CRITICAL	10.0	73756	Microsoft SQL Server Unsupported Version Detection (remote check)
CRITICAL	10.0	84729	Microsoft Windows Server 2003 Unsupported Installation Detection
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
HIGH	8.1	100464	Microsoft Windows SMBv1 Multiple Vulnerabilities
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
HIGH	7.3	26920	Microsoft Windows SMB NULL Session Authentication
MEDIUM	6.8	90510	MS16-047: Security Update for SAM and LSAD Remote Protocols (3148527) (Badlock) (uncredentialed check)
MEDIUM	6.5	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.3	152102	Microsoft Windows EFSRPC NTLM Reflection Elevation of Privilege (PetitPotam) (Remote)
MEDIUM	5.1*	18405	Microsoft Windows Remote Desktop Protocol Server Man-in-the-Middle Weakness
LOW	N/A	69551	SSL Certificate Chain Contains RSA Keys Less Than 2048 bits

Figura 11: Herramienta Nessus

Fuente: Reporte de escaneo de la aplicación.

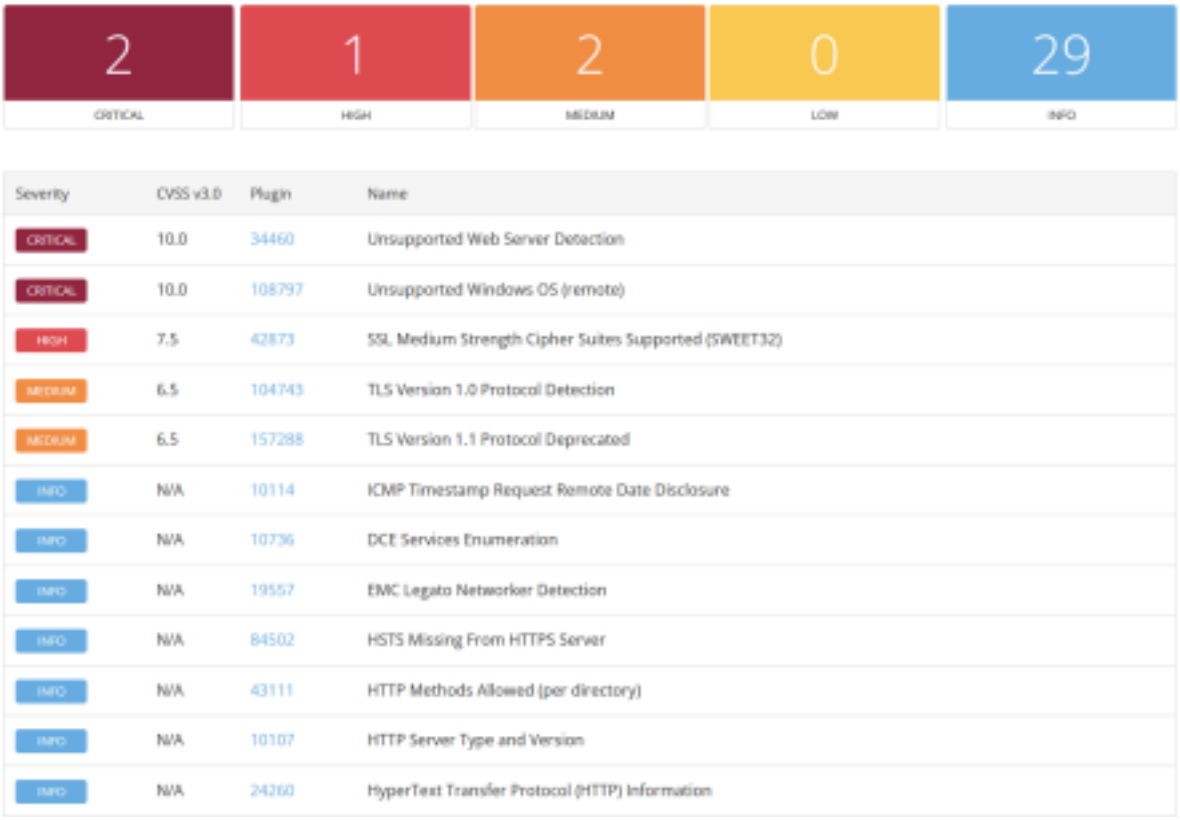
Equipo 9:

Severity	CVSS v3.0	Plugin	Name
CRITICAL	10.0	34460	Unsupported Web Server Detection
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	157288	TLS Version 1.1 Protocol Deprecated
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	19557	EMC Legato Networker Detection
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information

Figura 12: Herramienta Nessus

Fuente: Reporte de escaneo de la aplicación.

Equipo 10:



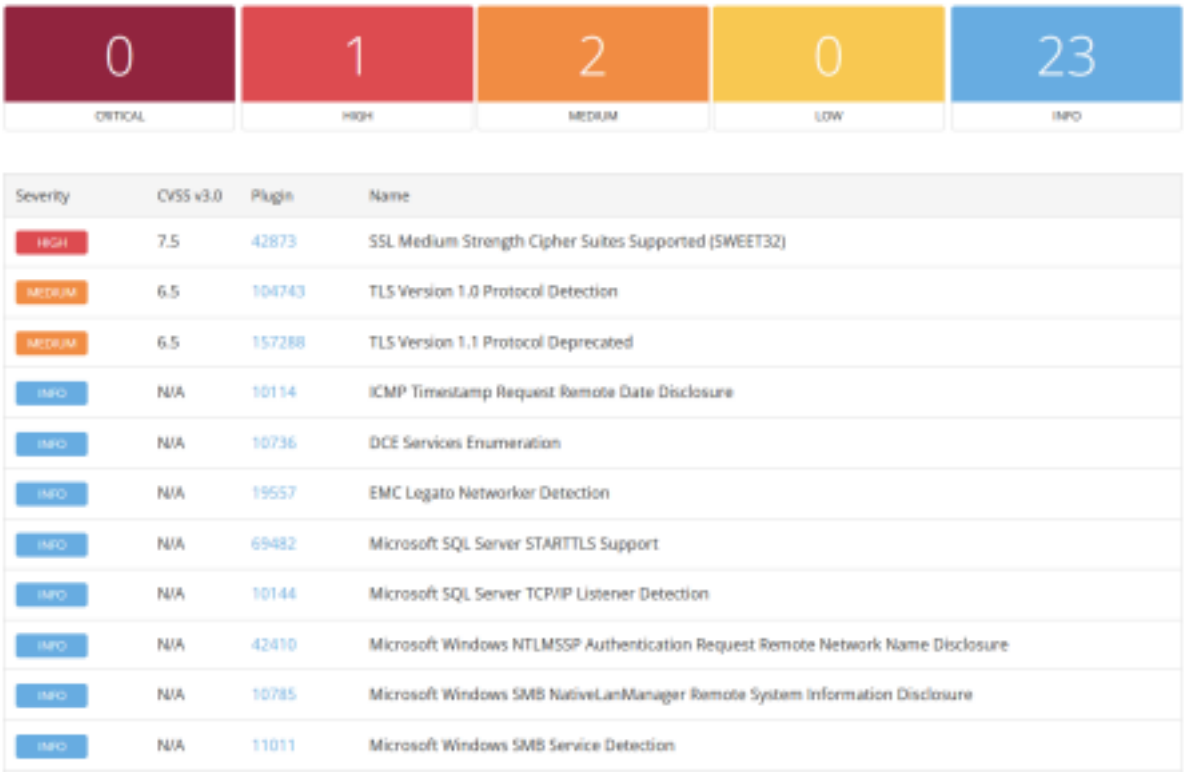
2	1	2	0	29
CRITICAL	HIGH	MEDIUM	LOW	INFO

Severity	CVSS v3.0	Plugin	Name
CRITICAL	10.0	34460	Unsupported Web Server Detection
CRITICAL	10.0	108797	Unsupported Windows OS (remote)
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	157288	TLS Version 1.1 Protocol Deprecated
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	19557	EMC Legato Networker Detection
INFO	N/A	84502	HSTS Missing From HTTPS Server
INFO	N/A	43111	HTTP Methods Allowed (per directory)
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information

Figura 13: Herramienta Nessus

Fuente: Reporte de escaneo de la aplicación.

Equipo 11:



Severity	CVSS v3.0	Plugin	Name
HIGH	7.5	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	6.5	104743	TLS Version 1.0 Protocol Detection
MEDIUM	6.5	157288	TLS Version 1.1 Protocol Deprecated
INFO	N/A	10114	ICMP Timestamp Request Remote Date Disclosure
INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	19557	EMC Legato Networker Detection
INFO	N/A	69482	Microsoft SQL Server STARTTLS Support
INFO	N/A	10144	Microsoft SQL Server TCP/IP Listener Detection
INFO	N/A	42410	Microsoft Windows NTLMSSP Authentication Request Remote Network Name Disclosure
INFO	N/A	10785	Microsoft Windows SMB NativeLanManager Remote System Information Disclosure
INFO	N/A	11011	Microsoft Windows SMB Service Detection

Figura 14: Herramienta Nessus

Fuente: Reporte de escaneo de la aplicación.

Equipo 12:

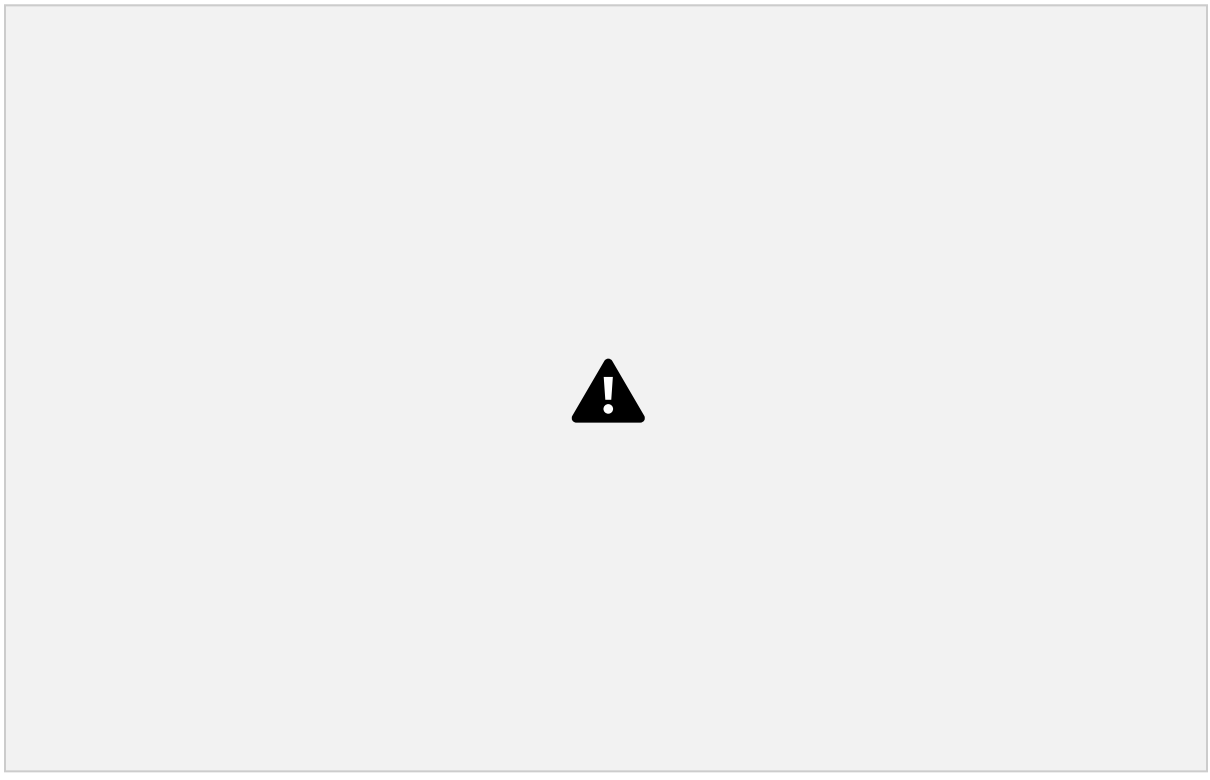


Figura 15: Herramienta Nessus

Fuente: Reporte de escaneo de la aplicación.

61

Equipo 13:

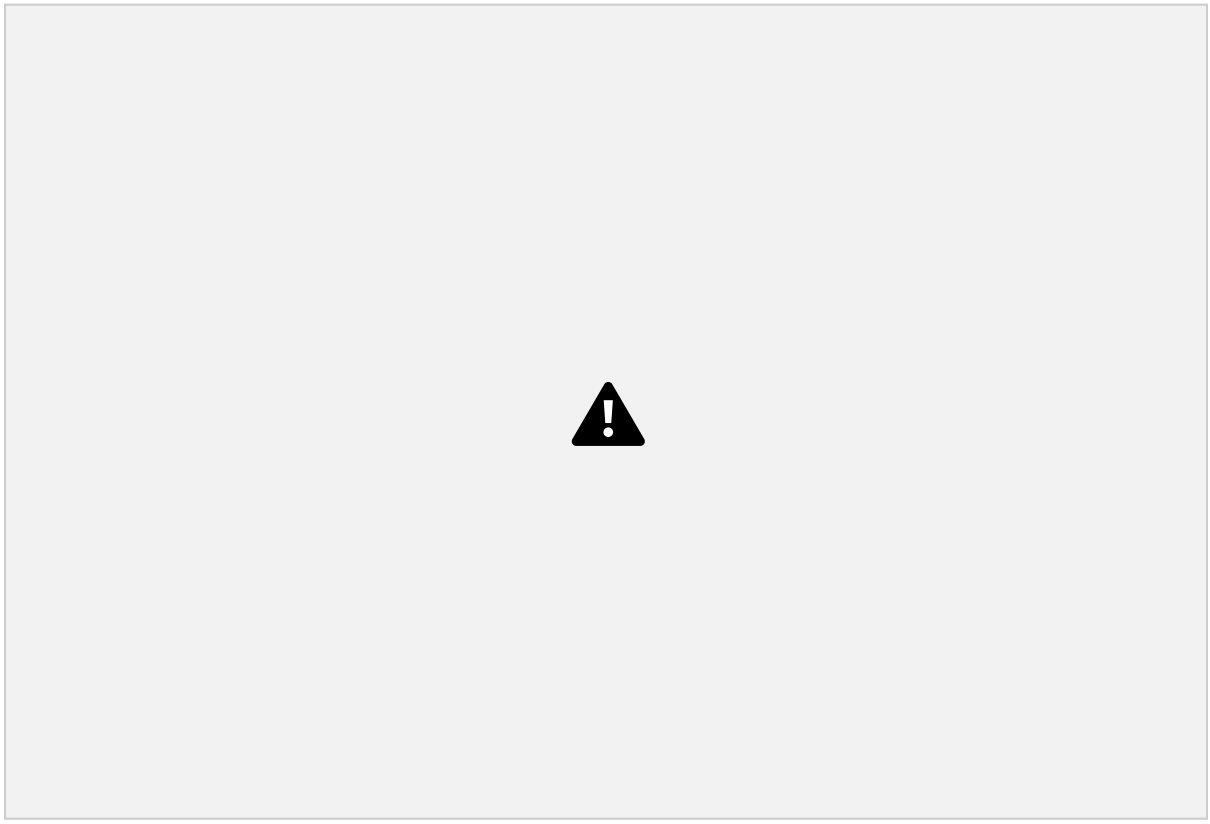


Figura 16: Herramienta Nessus

Fuente: Reporte de escaneo de la aplicación.

62

Equipo 14:

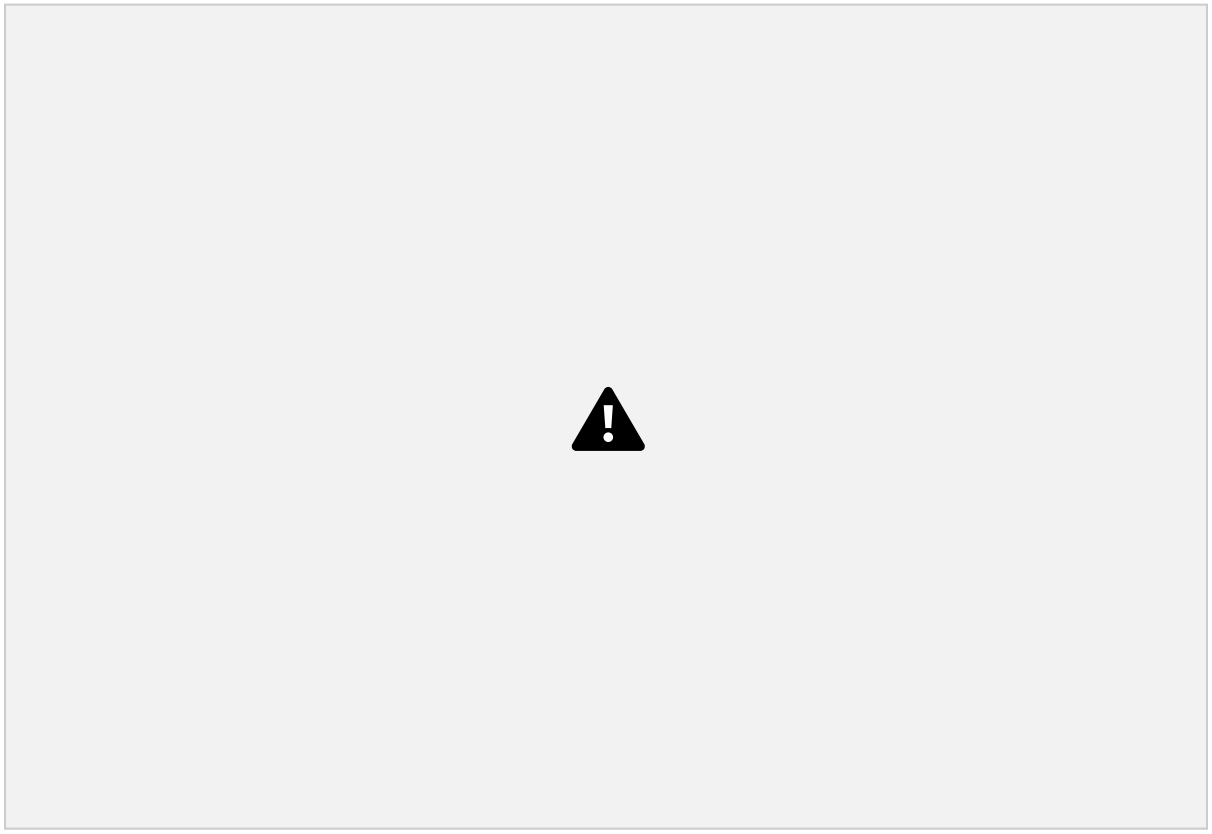


Figura 17: Herramienta Nessus

Fuente: Reporte de escaneo de la aplicación.

Equipo 15:

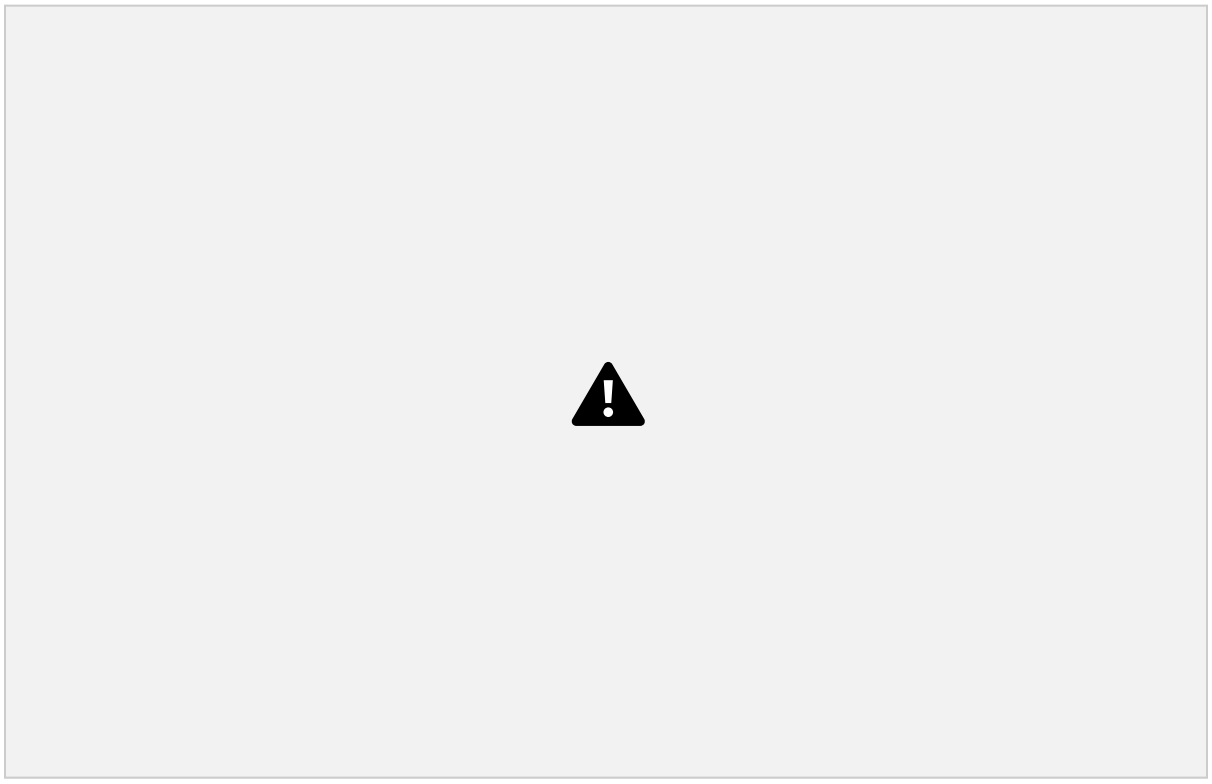


Figura 18: Herramienta Nessus

Fuente: Reporte de escaneo de la aplicación.