DISEÑO DEL SISTEMA DE SEGURIDAD BASADO EN EL ANÁLISIS DE VULNERABILIDADES IDENTIFICADAS EN LA EMPRESA NOSTRADAMUS S.A.S.

KERWIN CARLOS TORRES CASTILLO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
SINCELEJO
2021

DISEÑO DEL SISTEMA DE SEGURIDAD BASADO EN EL ANÁLISIS DE VULNERABILIDADES IDENTIFICADAS EN LA EMPRESA NOSTRADAMUS S.A.S.

KERWIN CARLOS TORRES CASTILLO

Proyecto Aplicado para optar el título de Especialista en Seguridad Informática

Director: JOHN FREDDY QUINTERO TAMAYO
Magister en Seguridad en las Tecnologías de la Información y las Comunicaciones

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA UNAD
ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA
ESPECIALIZACION EN SEGURIDAD INFORMATICA
SINCELEJO
2021

Nota de Aceptación

_____

_____

_____

_____

Presidente del Jurado

_____

Jurado

_____

Jurado

Sincelejo, 26 de abril de 2021

A El Padre de todo lo creado, que camina delante de mí como poderoso gigante, haciendo que este logro fuese posible, a mi Esposa y a mis hijos, el motor de mis sueños, que me acompañaron en el proceso y sacrificaron su tiempo junto conmigo, sin ellos esto no hubiese sido realidad.

AGRADECIMIENTOS

Agradezco a las directivas de la Universidad Nacional Abierta y a Distancia UNAD por la creación de estos espacios de desarrollo profesional a través de las nuevas tecnologías y que hoy hacen posible un logro que parecía inalcanzable, especialista en seguridad informática.

A la doctora Mónica Sierra, Secretaria General de la Alcaldía de Sincelejo, por la postulación de mi nombre al premio de incentivos laborales del año 2018, que entregó los recursos que financiaron este logro profesional.

CONTENIDO

Pág.

LISTA DE TABLAS

LISTA DE FIGURAS

Pág

LISTA DE ANEXOS

RESUMEN

La información constituye el recurso más valioso de una organización y como tal es el más acechado por ciberdelincuentes y piratas informáticos que día tras día encaminan sus esfuerzos en busca de vulnerabilidades en los sistemas que les permitan acceder a este preciado recurso. Para contrarrestar esta amenaza, las empresas han visto la necesidad de contratar profesionales en seguridad informática, que les ayuden a minimizar los riesgos en seguridad de la información presentes en sus sistemas.

La empresa Nostradamus SAS., ha sido víctima de ataques informáticos a sus sistemas de información, sufriendo la pérdida de gran parte de este activo; situación que ha afectado su imagen corporativa de manera considerable. La presente propuesta busca identificar las causas que dieron origen a la problemática presentada, mediante la simulación de ataques de manera controlada, identificando las vulnerabilidades del sistema y presentando la mejor alternativa de solución a este, minimizando los riesgos de una nueva pérdida de información por causa de un ataque informático.

1. INTRODUCCIÓN

Nostradamus S.A.S, es una empresa del sector tecnológico que brinda servicios a los sectores: educativo, corporativo y gubernamental en temas relacionados con proyectos de educación y capacitación a través del uso de TIC desde la implementación y configuración de plataformas de aprendizaje brindando capacitación y soporte 24/7. Hace pocos días la empresa fue víctima un ataque informático, que afecta la imagen corporativa de la organización debido a que el robo de información registrado compromete a su vez, la seguridad de la información de sus clientes.

Durante los últimos años la tecnología ha crecido a pasos agigantados, el uso de las Tics se ha globalizado exponencialmente; cada día crece el número de personas y empresas que hacen uso de la red para almacenar y/o compartir su información, los servicios de almacenamiento en la nube como Google Drive, Mega, iCloud, Dropbox, se han convertido en toda una tendencia mundial, el Cloud Computing, los servidores virtuales, un sin número de nuevas tecnologías que transmiten, almacenan y procesan millones de datos en la red, son producto de este crecimiento; juntamente con todo esto, surge la necesidad de mantener segura toda la información que generan las personas, empresas y organizaciones, dando lugar a la seguridad informática como la disciplina encargada de diseñar e implementar políticas y controles para la salvaguarda de la información en toda clase de sistemas informáticos. La información es el activo más importante para toda organización y como tal necesita ser resguardado, aunque no existe un sistema ciento por ciento seguro, la implementación de un eficiente sistema de seguridad de la información permite minimizar los riesgos a los que puede ser expuesta.

El desarrollo del presente proyecto aplicado busca diseñar un sistema de seguridad de la información basado en el estudio e identificación de vulnerabilidades presentes en los sistemas informáticos de la empresa Nostradamus SAS y que dieron lugar a la pérdida de información sensible de la empresa.

2. OBJETIVOS

2.1 OBJETIVO GENERAL

Gestionar desde un enfoque estratégico y directivo las políticas de seguridad de la Información basado en el análisis de vulnerabilidades realizado en los sistemas informáticos de la Empresa Nostradamus S.A.S.

2.2 OBJETIVOS ESPECÍFICOS

- ✓ Diagnosticar la situación actual del sistema informático de la empresa y las políticas de seguridad existentes.
- ✓ Determinar el nivel de riesgo existente en los activos de información de la empresa.
- ✓ Identificar posibles vulnerabilidades en el sistema de seguridad de información de la empresa mediante pruebas de penetración.
- ✓ Diseñar políticas y controles de seguridad para las áreas críticas identificadas en el análisis del riesgo y las pruebas de penetración.
- ✓ Presentar las recomendaciones necesarias para mejorar la seguridad en el sistema de información de la empresa.

3. PLANTEAMIENTO DEL PROBLEMA

3.1 DEFINICIÓN DEL PROBLEMA

Nostradamus S.A.S, es una empresa del sector tecnológico que brinda servicios a los sectores: educativo, corporativo y gubernamental en temas relacionados con proyectos de educación y capacitación a través del uso de TIC desde la implementación y configuración de plataformas de aprendizaje brindando capacitación y soporte 24/7[1].

Durante la última semana Nostradamus S.A.S, sufrió un ataque informático que afecto la imagen corporativa de la organización ocasionado por la pérdida de información crítica de clientes a partir de ataques remotos; entre los ataques identificados se encuentran, ataque a sistemas operativos Windows haciendo uso de técnicas de ingeniería social; ataque de elevación de privilegios y robo de información a sistemas operativos Windows y ataque de denegación de servicio a la intranet de la empresa.

Esta situación ha puesto en evidencia la fragilidad del sistema de seguridad existente, la falta de mecanismos de recuperación de la información, la ausencia de controles robustos para el acceso a la información y áreas críticas de la empresa, así como la necesidad de un monitoreo constante del tráfico en la red, a fin de prever la presencia de amenazas que afecten la disponibilidad, la confidencialidad y la integridad de la información. ¿De qué manera el análisis de vulnerabilidades puede aportar en el diseño de un sistema de seguridad de la información para la empresa Nostradamus S.A.S.?

3.2 JUSTIFICACIÓN

La información constituye el activo más importante de toda empresa u organización y como tal debe ser protegido, cualquier incidente que ponga en riesgo la disponibilidad, confidencialidad e integridad de la información resultaría de gran afectación para la empresa y los productos y/o servicios que ofrece, reflejándose en pérdida de credibilidad, baja rotación de productos, retiro de clientes, entre otras.

[1] Escenario propuesto para el desarrollo de proyecto aplicado como alternativa de grado. Universidad Nacional Abierta y a Distancia. Especialización en Seguridad Informática.

La empresa Nostradamus S.A.S, requiere tomar de manera inmediata las acciones necesarias para la protección de su información y sistemas informáticos, dados los últimos acontecimientos donde una posible amenaza pasó a convertirse en un ataque directo a sus sistemas informáticos, derivando en la pérdida de información crítica de la empresa.

Por lo anteriormente expuesto, las directivas de la empresa han solicitado la realización de un estudio y análisis de vulnerabilidades en los sistemas informáticos de Nostradamus S.A.S, que incluya recrear los mismos ataques de los cuales fue objeto, a fin de identificar fallas, evaluar controles y políticas de seguridad, analizar riesgos, posibles amenazas y cualquier otra situación que pueda afectar negativamente la información vital de la empresa.

4. MARCO TEÓRICO

4.1 SEGURIDAD INFORMÁTICA

Es el conjunto de técnicas, procesos y procedimientos encaminados a la protección de los equipos y/o recursos informáticos en una organización, previendo situaciones que pueden ir desde accesos no autorizados hasta ataques premeditados para el robo de información, recursos o cualquier otro activo de la organización.

Hoy en día el uso de las tecnologías de información y comunicación se ha convertido en la base fundamental para la implementación de sistemas computacionales en las entidades u organizaciones, por lo que es necesario garantizar el bienestar de los sistemas y de la información contenida dentro de un ordenador, un servidor o una red, a fin de prevenir de cualquier modo, un ciberataque o estar preparado para resistirlo.

Así las cosas, se hace necesario entender y aplicar la seguridad informática como eje fundamental para la protección de la información, junto a sus tres pilares, confidencialidad, disponibilidad e integridad. Cuando hablamos de confidencialidad es garantizar que la información esté protegida y que no sea divulgada ni transmitida por ningún medio de comunicación si no le compete a la entidad u organización. La integridad de la información implica que la información no se vea afectada por errores o por alteraciones maliciosas solo se podrá modificar la información con autorización y la disponibilidad cuando nos referimos a este término hablamos del acceso de personas u organismos a un sistema de información y que el mismo se mantenga funcionando sin ningún tipo de alteración en cuanto al acceso a la información, para ello es necesario que se garantice el acceso a los datos solo por usuarios autorizados solo si se requiere cumplir con las necesidades.

4.2 SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La información es todo conjunto de datos organizados en una entidad y que representan un valor añadido para la misma, independientemente de su origen, la forma en la que almacene transmita o su fecha de elaboración; es considerada el principal activo de toda empresa u organización.

Un sistema de gestión de la seguridad de la información SGSI[2], según la norma ISO 27001 consiste en un proceso sistemático, documentado y encaminado a preservar la confidencialidad, integridad y disponibilidad de la información, además de todos los sistemas implicados en el tratamiento de esta dentro de la organización y garantizando que su seguridad es gestionada correctamente. Estos conceptos conocidos como los pilares de la seguridad de la información se detallan a continuación.

Disponibilidad es la disposición de los servicios a ser usados cuando sea necesario. La carencia de disponibilidad supone una interrupción del servicio. Es vital para las organizaciones poder acceder a la información de manera rápida, segura y sencilla, en cualquier momento, por lo que la disponibilidad va directamente ligada con la productividad de las organizaciones.

Integridad es el mantenimiento de las características de completitud y corrección de los datos. Contra la integridad, la información puede aparecer manipulada, corrupta o incompleta. La integridad afecta directamente al correcto desempeño de las funciones de una Organización.

Confidencialidad es garantizar que la información llegue solamente a las personas autorizadas. La confidencialidad es una propiedad de difícil recuperación, que puede involucrar el incumplimiento de leyes y compromisos contractuales relativos a la custodia de los datos.

4.3 NORMA ISO/IEC 27001:2013[3]

Es una norma internacional emitida por la Organización Internacional de Normalización (ISO) y describe cómo gestionar la seguridad de la información en una empresa. La revisión más reciente de esta norma fue publicada en 2013 y ahora su nombre completo es ISO/IEC 27001:2013. La primera revisión se publicó en 2005 y fue desarrollada en base a la norma británica BS 7799-2.

ISO 27001 puede ser implementada en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Está redactada por los mejores especialistas del mundo en el tema y proporciona una metodología para

[2] Tomado de https://www.iso27000.es/sgsi.html (2019).
[3] Segovia, A. (2019). www.advisera.com.

implementar la gestión de la seguridad de la información en una organización. También permite que una empresa sea certificada; esto significa que una entidad de certificación independiente confirma que la seguridad de la información ha sido implementada en esa organización en cumplimiento con la norma ISO 27001.

El eje central de ISO 27001 es proteger la confidencialidad, integridad y disponibilidad de la información en una empresa. Esto lo hace investigando cuáles son los potenciales problemas que podrían afectar la información (es decir, la evaluación de riesgos) y luego definiendo lo que es necesario hacer para evitar que estos problemas se produzcan (es decir, mitigación o tratamiento del riesgo). Por lo tanto, la filosofía principal de la norma ISO 27001 se basa en la gestión de riesgos: investigar dónde están los riesgos y luego tratarlos sistemáticamente.

4.4 MAGERIT

Es la metodología de análisis y gestión de riesgos de los sistemas de información, elaborada por la dirección general de modernización administrativa, procedimientos e impulso de la administración electrónica de España; implementa el proceso de gestión de riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información. Magerit persigue los siguientes objetivos[4]:

- ✓ Concientizar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos.
- ✓ Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
- ✓ Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control.
- ✓ Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso.

La versión actualizada de esta metodología se encuentra organizada en tres volúmenes o guías para facilitar su correcta aplicación.

- Libro I. Método.

[4] Magerit – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid, España (2012).

- Libro II. Catálogo de elementos.
- Libro III. Guía de Técnicas.

Esta disposición permite que la gestión de riesgos según Magerit v.3.0 pueda adaptarse a cada caso y situación que surja durante el proceso, definiendo su método de aplicación de acuerdo a las tareas que se describen a continuación.

MAR.1 – Caracterización de los activos
    MAR.11 – Identificación de los activos
    MAR.12 – Dependencias entre activos
    MAR.13 – Valoración de los activos
MAR.2 – Caracterización de las amenazas
    MAR.21 – Identificación de las amenazas
    MAR.22 – Valoración de las amenazas
MAR.3 – Caracterización de las salvaguardas
    MAR.31 – Identificación de las salvaguardas pertinentes
    MAR.32 – Valoración de las salvaguardas
MAR.4 – Estimación del estado de riesgo
    MAR.41 – Estimación del impacto
    MAR.42 – Estimación del riesgo

4.5 ANÁLISIS DE VULNERABILIDADES

Una falla en un sistema informático o programa representa una vulnerabilidad en el sistema o una brecha de seguridad en el mismo, aun cuando no todos los malos funcionamientos de los programas sean concretamente un atentado contra la seguridad de la información, una vulnerabilidad de seguridad es una debilidad en un programa o servicio que puede comprometer la confidencialidad, la integridad y la disponibilidad de toda la información contenida en el sistema.

Un análisis correcto de las vulnerabilidades de un sistema permite no solo identificar las posibles fallas en la seguridad de la información, también permite clasificar el tipo de vulnerabilidad, identificar el nivel del riesgo asociado y las posibles consecuencias que generan la presencia de estas amenazas a la integridad del sistema, entregando las recomendaciones necesarias para mitigar cada uno de los riesgos identificados.

El análisis de vulnerabilidades puede tomar varios perfiles, dependiendo del tipo de aplicación y de las necesidades existentes. Una de las lógicas analíticas más utilizadas es el test dinámico de seguridad de aplicaciones (DAST). La técnica identifica defectos de seguridad mediante la alimentación de condiciones de fallas para encontrar vulnerabilidades en tiempo real. Otro análisis de vulnerabilidad común es el static application security test (SST), un análisis profundo del código de una aplicación para identificar vulnerabilidades sin ejecutar el programa[5].

Por otro lado, uno de los procedimientos de análisis de vulnerabilidades más usado es la realización de pruebas de penetración, también conocido como pentest o pentesting, esta serie de procedimientos permiten que el especialista en seguridad informática asuma el rol del atacante en busca de explotar cada una de las posibles vulnerabilidades identificadas previamente en el sistema, a fin de penetrar y obtener información confidencial de la empresa. Terminado este ejercicio el especialista en seguridad tendrá toda la información requerida para diseñar los controles y políticas que minimizaran la posibilidad de nuevos ataques.

Un pentest generalmente está conformado por cuatro etapas; enumeración, aquí se recopila toda la información necesaria sobre el objetivo; análisis de vulnerabilidades, en está fase se analiza la información recopilada anteriormente a fin de identificar brechas de seguridad; explotación, e esta etapa se busca aprovechar las brechas identificadas para comprometer el sistema objetivo y por último, informe, en esta etapa se lleva a cabo la preparación de toda la documentación correspondiente al informe detallado de los resultados obtenidos en el proceso.

4.6 LEY 1273 DE 2009[6]

Permitió introducir una reforma al Código Penal Colombiano, identificando y penalizando las conductas que atentan contra la seguridad de la información, los datos personales y los sistemas informáticos, con penas que van desde los 36 hasta los 120 meses de prisión.

Acceso abusivo a un sistema de información. Todo acceso no autorizado a un sistema informático y su permanencia en el, es considerado ilegal y tiene una pena

[5] Tomado de https://ostec.blog/es/generico/primeros-pasos-para-realizar-un-analisis-de-vulnerabilidad-en-redes-corporativas/#
[6] Tomado de https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009.

de prisión de hasta 96 meses y una multa de hasta 1000 SMMLV. Dentro de las conductas más comunes que se clasifican en este tipo de delito están la ingeniería social y el Trashing.

Obstaculización ilegitima de un sistema informático o red de telecomunicación. El bloqueo de un sistema o sistema de comunicaciones por algún medio constituye una violación a la ley colombiana; dentro de este delito están tipificadas conductas como el hackeo de páginas web, la denegación de servicios y el instalar equipos de telecomunicaciones para desviar señales y demás; con penas hasta de 96 meses y una multa de hasta 1000 SMMLV.

Interceptación de datos informáticos. Contempla la interceptación tanto de redes cableadas como wifi; así que el hackeo de contraseñas y redes wifi constituye una conducta castigable hasta con 72 meses de prisión. Así mismo, conductas como el phishing y el web spoofing.

Daño Informático. Corresponde a todo aquello que se hace encaminado a dañar un sistema de información en su componente informático; borrado intencional o accidental de archivos, alteración de la información, entre otras. Los malwares, exploit y bombas lógicas entran en esta clasificación. Tiene una pena de hasta 96 meses de prisión.

Uso de software malicioso. Definitivamente corresponde al uso de virus, troyanos, exploits, malware, bombas lógicas y cualquier otro tipo de software diseñado para afectar la integridad de un sistema informático y cuyo principal objetivo es la captura de la información en el contenida. Tiene una pena de hasta 96 meses de prisión.

Violación de datos personales. Es quizá el delito informático más escuchado últimamente, el robo de cuentas de redes social, el carding y la sustracción de información de bases de datos de entidades bancarias, personas y empresas. Constituye una pena de hasta 96 meses de prisión.

Suplantación de sitios web para capturar datos personales. Otro de los delitos más comunes y utilizados por los ciberdelincuentes, el muy conocido y efectivo phishing que junto con el web spoofing son las conductas más recurrentes enmarcadas en este delito. Tiene una pena de hasta 48 meses de prisión.

4.7 RIESGO

Es la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a una organización. El riesgo indica lo que le podría pasar a los activos de una organización si no son protegidos adecuadamente[7].

4.8 ANÁLISIS Y TRATAMIENTO DE RIESGOS

Proceso sistemático que permite estimar la magnitud de los riesgos a que está expuesta una organización, minimizando su impacto en esta. El análisis de riesgos identifica cómo es, cuánto vale y el nivel de protección del sistema. En coordinación con los objetivos, estrategia y política de la organización, las actividades de tratamiento de los riesgos permiten elaborar un plan de seguridad que, implantado y operado, satisfaga los objetivos propuestos con el nivel de riesgo que acepta las directivas de la empresa[8]. Esto es lo que se conoce como Proceso de Gestión de Riesgos.

[7] Garavito, H. (2015). Análisis y gestión del riesgo de la información en los sistemas de información misionales de una entidad del estado.
[8] MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. Madrid, España (2012).

5. METODOLOGIA

El desarrollo del presente proyecto aplicado se lleva a cabo en cuatro fases, Diagnostico, Análisis de vulnerabilidades, Definición de políticas y controles, para terminar con el Diseño del nuevo sistema de seguridad de la información que permitirá minimizar la probabilidad de futuros ataques a la empresa Nostradamus S.A.S.

5.1 FASE 1: DIAGNOSTICO

Es necesario identificar la situación actual de la empresa en cuanto a la seguridad de la información, por lo tanto, esta fase inicia con la consulta de documentación organizacional existente, así como otras fuentes de información y material bibliográfico relacionado con el objeto de estudio del proyecto; incluye también el levantamiento de activos y el análisis y gestión de riesgos basado en la metodología Magerit versión 3.0.

5.2 FASE 2: ANALISIS DE VULNERABILIDADES

En esta etapa se pretende identificar las posibles vulnerabilidades existentes en el sistema informático de la empresa, iniciara con un escaneo de la red y los servidores de Nostradamus, buscando activos expuestos o con brechas de seguridad, para concluir, se recrean los ataques ya identificados y de los cuales fue víctima la empresa, así como la realización de algunas pruebas adicionales determinadas en base a los hallazgos de los análisis previos, que permitan minimizar cualquier amenaza que represente un riesgo para la seguridad de la información en Nostradamus S.A.S.

5.3 FASE 3: DEFINICIÓN DE CONTROLES Y POLÍTICAS DE SEGURIDAD

Terminado el proceso de identificación de vulnerabilidades, se procederá a realizar el análisis correspondiente de los hallazgos encontrados a fin de diseñar las políticas de seguridad necesarias para la empresa y determinar los controles a implementar basados en la norma ISO/IEC 27001:2013, necesarios para mitigar la probabilidad de que se repitan este tipo de ataques.

5.4 FASE 4: DISEÑO DEL SISTEMA DE SEGURIDAD

El nuevo sistema de seguridad de la información para Nostradamus S.A.S, resulta luego de la definición de cada uno de los controles necesarios e identificados priorizando las áreas más críticas, así como el establecimiento y socialización de las políticas de seguridad en cada una de las dependencias de la entidad. En consecuencia, se presenta a la empresa el diseño del sistema de seguridad de la información a implementar, con el fin de prevenir nuevos ataques a la infraestructura tecnológica de la entidad.

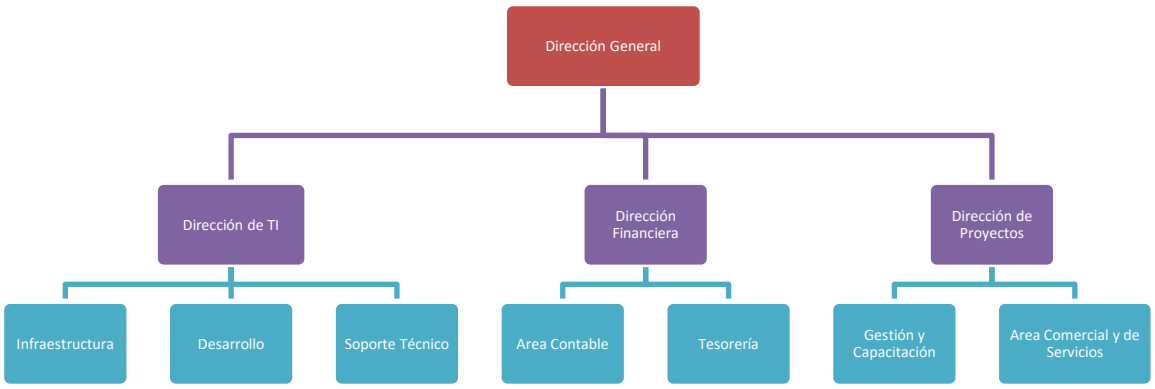
6. DESARROLLO DEL PROYECTO

6.1 FASE 1 : DIAGNOSTICO

6.1.1 Descripción de la organización. Nostradamus S.A.S, es una empresa del sector tecnológico que brinda servicios a los sectores: educativo, corporativo y gubernamental en temas relacionados con proyectos de educación y capacitación a través del uso de TIC desde la implementación y configuración de plataformas de aprendizaje brindando capacitación y soporte 24/7. Actualmente cuenta con 120 colaboradores entre directivos, administrativos y operativos, quienes hacen uso de forma regular de los medios tecnológicos disponibles y alrededor de 1800 clientes que hacen uso de sus servicios.

6.1.2 Estructura organizacional.

Figura 1. Organigrama Nostradamus.



Fuente: Elaborada por el autor.

6.1.3 Estructura de la dirección de TI.

- Director de TI. Es el encargado de planear, desarrollar y mantener toda la infraestructura tecnológica del Nostradamus s.a.s, proporcionando el soporte

óptimo de los sistemas de información existentes de acuerdo a las políticas, procesos y procedimientos establecidos.

- Director técnico de infraestructura. Bajo su responsabilidad se encuentra el brindar soporte al acceso a la red corporativa, internet y plataformas tecnológicas de la entidad, así como la revisión periódica de diseños de cableado estructurado.

- Director técnico de desarrollo. Brinda apoyo técnico a las áreas administrativas de la entidad en desarrollo de medios eficientes para lograr actividades basadas en usos de tecnologías de la informática y las telecomunicaciones.

- Director técnico de soporte. A su cargo se encuentra el mantenimiento periódico de computadores, la generación de conceptos técnicos para tramitar baja de equipos y la realización de copias de seguridad de los sistemas de información y servidores que se encuentran en las dependencias de la entidad.

6.1.4 Funciones de la dirección de TI. Entre las funciones que cumple la dirección de TI de Nostradamus s.a.s, se encuentran.

- Garantizar el acceso a los servicios de plataformas institucionales y correo electrónico institucional.

- Proporcionar medios de almacenamiento para clientes y dependencias que lo requieran.

- Brindar el mantenimiento de los activos informáticos de la entidad

- Desarrollar soluciones de software operativo y aplicativo

- Gestionar todo el equipamiento tecnológico que se requiera para ayudar a dar cumplimiento al objeto social de la entidad.

6.1.5 Alcance. Se define dentro del alcance del presente proyecto los siguientes puntos.

- Infraestructura tecnológica de la empresa a cargo de la Dirección de TI.

- Activos relacionados directamente con los servicios ofrecidos por la empresa.

- Procesos y procedimientos que involucran el tratamiento de la información.

- Gestión y tratamiento de riesgos identificados como importantes y críticos.

En conclusión, el alcance involucra toda la infraestructura tecnológica de Nostradamus que da soporte a los servicios ofrecidos por la empresa y el área encargada de la misma, la cual corresponde a la Dirección de TI de la empresa Nostradamus S.A.S.

6.1.6 Análisis y gestión de riesgos. La aplicación de la metodología Magerit v.3.0 permite analizar la situación presentada en la empresa Nostradamus s.a.s identificando el nivel de riesgo informático en el que se encuentra la empresa para luego determinar los controles necesarios a implementar para mitigar cualquier tipo de amenaza al sistema.

6.1.7 Caracterización de los activos. La tarea MAR.1, según Magerit, comprende las actividades que permiten identificar los activos relevantes pertenecientes a la entidad, clasificándolos entre los 10 tipos de activos definidos por esta metodología, estableciendo las relaciones de dependencias entre ellos, así como su importancia para cada una de las dimensiones de seguridad y su valoración[9].

6.1.8 Identificación de los activos. La tarea MAR.11 es crítica dentro del análisis de riesgos, una adecuada identificación de los activos a cargo de la dirección de TI de Nostradamus materializa con precisión el alcance del proyecto. Para el presente caso, en la definición de cada uno de los activos identificados se determinan las siguientes características.

- Código. Compuesto por tres grupos de caracteres, el primero determina el tipo de activo, el segundo la entidad a la que pertenece y el tercer grupo el nombre corto según el catálogo de elementos de Magerit. *D(tipo de activo)_NOS(entidad)_SOURCE(nombre corto).*
- Unidad responsable del activo. Corresponde al proceso propietario del activo.
- Persona responsable. Cargo responsable del activo dentro de la entidad.

[9] MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método. Madrid, España (2012).

Tabla 1. Identificación de activos

Item	Tipo de activo	Nombre del activo de información
1	[D] DATOS	[D_NOS_BACKUP] Copias de Seguridad de la información.
2		[D_NOS_SOURCE] Código Fuente de las aplicaciones desarrolladas.
3		[D_NOS_ACL] Datos de Acceso a Servidores.
4		[D_NOS_PASS] Datos de Acceso Usuarios del Sistema.
5	[S] SERVICIOS	[S_NOS_RCE] Servicio Proyectos de Capacitación y Educación.
6		[S_NOS_CAMPUS] Servicio de Aula virtual Institucional.
7		[S_NOS_EMAIL] Servicio de Correo Electrónico Institucional.
8		[S_NOS_LIBRARY] Servicio de Biblioteca Virtual.
9	[SW] SOFTWARE	[SW_NOS_CONT] Sofware Contable Cloud.
10		[SW_NOS_ARCA] Plataforma tecnológica Institucional
11		[SW_NOS_WEB] Portal Web Nostradamus.
12		[SW_NOS_DEV] Paquete de Entorno de Desarrollo.
13		[SW_NOS_OS] Sistemas Operativos.
14		[SW_NOS_OFFICE] Aplicaciones Ofimáticas.
15		[SW_NOS_SMAIL] Cliente de Correo Electrónico.
16		[SW_NOS_AV] Software Antivirus.
17	[HW] HARDWARE	[HW_NOS_SRI] Dell Torre PowerEdge T440.
18		[HW_NOS_SRFTP] Dell Torre PowerEdge T130.
19		[HW_NOS_SRCA] Dell Torre PowerEdge T440
20		[HW_NOS_SRDHCP] Dell Torre PowerEdge T440
21		[HW_NOS_PC] Equipos de Cómputo.

Tabla 2. (Continuación)

Item	Tipo de activo	Nombre del activo de información
22	[HW] EQUIPAMENTO INFORMÁTICO	[HW_NOS_PRINT1] Impresora HP LaserJet Enterprise serie 600
23		[HW_NOS_PRINT2] Impresora SMART MultiXpress M4370LX.
24		[HW_NOS_FIREWALL] Cortafuegos Cisco ASA 5505
25		[HW_NOS_SWITCH] Switches Cisco Catalyst 2960
26		[HW_NOS_HUB] Puntos de acceso alámbricos
27		[HW_NOS_WAP] Puntos de acceso inalámbricos.
28		[HW_NOS_TELIP] Teléfonos IP
29	[COM] REDES DE COMUNICACIONES	[COM_NOS_INTERNET] Canal de Internet Dedicado.
30		[COM_NOS_LAN] Red Local Institucional.
31		[COM_NOS_WLAN] Red Wifi Institucional.
32		[COM_NOS_TEL] Red telefónica.
33	[AUX] EQUIPAMENTO AUXILIAR	[AUX_NOS_POWER] Sistema eléctrico.
34		[AUX_NOS_CE] Cableado Estructurado.
35		[AUX_NOS_UPS] Sistema de alimentación sin Interrupciones.
36	[L] INSTALACIONES	[L_NOS_DEP] Área de la Dirección de TI.
37	[P] PERSONAL	[P_NOS_TECM] Técnicos de Mantenimiento a Equipos de Cómputo.
38		[P_NOS_DEVS] Ingenieros Desarrolladores
39		[P_NOS_NETS] Ingenieros de Infraestructura y Redes.
40		[P_NOS_TRED] Técnicos de Infraestructura y Redes.

Fuente: Elaborada por el autor basado en el libro II “catálogo de elementos” de la metodología Magerit v.3.

6.1.9 Valoración de activos. Se busca identificar los activos valiosos para la empresa Nostradamus y que representan un mayor riesgo ante los ataques de los que fue objeto, teniendo en cuenta cada una de las dimensiones de la seguridad de la información, confidencialidad, integridad y disponibilidad, adicionalmente se agregan autenticidad y trazabilidad. (Dirección General de Modernización Administrativa de España, 2012). La valoración de los activos identificados en Nostradamus se realiza en base a los criterios descritos en la tabla 2.

Tabla 3. Criterios de valoración

	Valoración Cualitativa	Categoría	Valoración Cuantitativa
Valoración del riesgo	MA	**Critico**	21 a 25
	A	**Importante**	16 a 20
	M	**Apreciable**	10 a 15
	B	**Bajo**	5 a 9
	MB	**Despreciable**	1 a 4

Fuente: Elaborada por el autor basado en el libro II “catálogo de elementos” de la metodología Magerit v.3.

Tabla 4. Valoración cualitativa de los activos de Nostradamus S.A.S.

Datos del activo de información		Dimensión				
Item	Nombre del activo de información	Autenticidad	Trazabilidad	Confidencilidad	Integridad	Disponibilidad
1	[D_NOS_BACKUP] Copias de Seguridad de la información.	B	B	MA	A	A
2	[D_NOS_SOURCE] Codigo Fuente de las aplicaciones desarrolladas.	B	B	B	A	A
3	[D_NOS_ACL] Datos de Acceso a Servidores.	A	B	A	A	A
4	[D_NOS_PASS] Datos de Acceso Usuarios del Sistema.	A	B	A	A	A
5	[S_NOS_RCE] Servicio Proyectos de Capacitación y Educación.	MA	MA	MA	MA	MA
6	[S_NOS_CAMPUS] Servicio de Aula virtual Institucional.	A	A	A	A	A
7	[S_NOS_EMAIL] Servicio de Correo Electronico Institucional.	B	B	A	B	B
8	[S_NOS_LIBRARY] Servicio de Biblioteca Virtual.	B	B	B	B	B
9	[SW_NOS_CONT] Sofware Contable Cloud.	A	A	A	A	A
10	[SW_NOS_ARCA] Plataforma tecnologica Institucional	MA	MA	MA	MA	MA
11	[SW_NOS_WEB] Portal Web Nostradamus.	A	A	A	A	A
12	[SW_NOS_DEV] Paquete de Entorno de Desarrollo.	B	B	B	B	B
13	[SW_NOS_OS] Sistemas Operativos.	B	M	B	B	M
14	[SW_NOS_OFFICE] Aplicaciones Ofiimatica.	MB	MB	B	A	A
15	[SW_NOS_SMAIL] Cliente de Correo Electronico.	B	B	B	B	B
16	[SW_NOS_AV] Software Antivirus.	B	B	B	A	A
17	[HW_NOS_SRI] Dell Torre PowerEdge T440.	M	M	M	M	M
18	[HW_NOS_SRFTP] Dell Torre PowerEdge T130.	A	A	A	A	A
19	[HW_NOS_SRCA] Dell Torre PowerEdge T440	MA	MA	MA	MA	MA
20	[HW_NOS_SRDHCP] Dell Torre PowerEdge T440	A	A	A	A	A
21	[HW_NOS_PC] Equipos de Computo.	B	B	B	M	M

Tabla 5. (Continuación)

Datos del activo de información		Dimensión				
Item	Nombre del activo de información	Autenticidad	Trazabilidad	Confidencilidad	Integridad	Disponibilidad
22	[HW_NOS_PRINT1] Impresora HP LaserJet Enterprise serie 600	B	B	B	B	B
23	[HW_NOS_PRINT2] Impresora SMART MultiXpress M4370LX.	B	B	B	B	B
24	[HW_NOS_FIREWALL] Cortafuegos Cisco ASA 5505	A	A	A	A	A
25	[HW_NOS_SWITCH] Switches Cisco Catalyst 2960	M	M	M	M	M
26	[HW_NOS_HUB] Puntos de acceso alámbricos	M	M	M	M	M
27	[HW_NOS_WAP] Puntos de acceso inalámbricos.	M	M	M	M	M
28	[HW_NOS_TELIP] Telefonos IP	B	B	B	B	B
29	[COM_NOS_INTERNET] Canal de Internet Dedicado.	A	A	A	A	MA
30	[COM_NOS_LAN] Red Local Institucional.	A	A	A	A	A
31	[COM_NOS_WLAN] Red Wifi Institucional.	M	M	M	M	M
32	[COM_NOS_TEL] Red Telefonica.	M	M	M	M	M
33	[AUX_NOS_POWER] Sistema Electrico.	M	M	M	MA	MA
34	[AUX_NOS_CE] Cableado Estructurado.	M	M	M	M	M
35	[AUX_NOS_UPS] Sistema Alimentacion sin Interrupciones.	M	M	M	M	M
36	[L_NOS_DEP] Area de la Dirección de TI.	B	B	B	B	B
37	[P_NOS_TECM] Tecnicos de Mantenimiento a Equipos de Computo.	A	A	A	A	A
38	[P_NOS_DEVS] Ingenieros Desarrolladores	A	A	A	A	A
39	[P_NOS_NETS] Ingenieros de Infraestructura y Redes.	A	A	A	A	A
40	[P_NOS_TRED] Técnicos de Infraestructura y Redes.	A	A	A	A	A

Fuente: Elaborada por el autor basado en el libro II “catálogo de elementos” de la metodología Magerit v.3.

Tabla 6. Valoración cuantitativa de los activos de Nostradamus S.A.S.

	Nombre	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Valor	Categorización
1	[D_NOS_BACKUP] Copias de Seguridad de la información.	9	9	25	20	20	17	IMPORTANTE
2	[D_NOS_SOURCE] Codigo Fuente de las aplicaciones desarrolladas.	9	9	9	20	20	13	APRECIABLE
3	[D_NOS_ACL] Datos de Acceso a Servidores.	20	9	20	20	20	18	IMPORTANTE
4	[D_NOS_PASS] Datos de Acceso Usuarios del Sistema.	20	9	20	20	20	18	IMPORTANTE
5	[S_NOS_RCE] Servicio Proyectos de Capacitación y Educación.	25	25	25	25	25	25	CRITICO
6	[S_NOS_CAMPUS] Servicio de Aula virtual Institucional.	20	20	20	20	20	20	IMPORTANTE
7	[S_NOS_EMAIL] Servicio de Correo Electronico Institucional.	9	9	20	9	9	11	APRECIABLE
8	[S_NOS_LIBRARY] Servicio de Biblioteca Virtual.	9	9	9	9	9	9	BAJO
9	[SW_NOS_CONT] Sofware Contable Cloud.	20	20	20	20	20	20	IMPORTANTE
10	[SW_NOS_ARCA] Plataforma tecnologica Institucional	25	25	25	25	25	25	CRITICO
11	[SW_NOS_WEB] Portal Web Nostradamus.	20	20	20	20	20	20	IMPORTANTE
12	[SW_NOS_DEV] Paquete de Entorno de Desarrollo.	9	9	9	9	9	9	BAJO
13	[SW_NOS_OS] Sistemas Operativos.	9	15	9	9	15	11	APRECIABLE
14	[SW_NOS_OFFICE] Aplicaciones Ofiimatica.	4	4	9	20	20	11	APRECIABLE
15	[SW_NOS_SMAIL] Cliente de Correo Electronico.	9	9	9	9	9	9	BAJO
16	[SW_NOS_AV] Software Antivirus.	9	9	9	20	20	13	APRECIABLE
17	[HW_NOS_SRI] Dell Torre PowerEdge T440.	15	15	15	15	15	15	APRECIABLE
18	[HW_NOS_SRFTP] Dell Torre PowerEdge T130.	20	20	20	20	20	20	IMPORTANTE
19	[HW_NOS_SRCA] Dell Torre PowerEdge T440	25	25	25	25	25	25	CRITICO
20	[HW_NOS_SRDHCP] Dell Torre PowerEdge T440	20	20	20	20	20	20	IMPORTANTE

Tabla 4. (Continuación)

	Nombre	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Valor	Categorización
21	[HW_NOS_PC] Equipos de Computo.	9	9	9	15	15	11	APRECIABLE
22	[HW_NOS_PRINT1] Impresora HP LaserJet Enterprise serie 600	9	9	9	9	9	9	BAJO
23	[HW_NOS_PRINT2] Impresora SMART MultiXpress M4370LX.	9	9	9	9	9	9	BAJO
24	[HW_NOS_FIREWALL] Cortafuegos Cisco ASA 5505	20	20	20	20	20	20	IMPORTANTE
25	[HW_NOS_SWITCH] Switches Cisco Catalyst 2960	15	15	15	15	15	15	APRECIABLE
26	[HW_NOS_HUB] Puntos de acceso alámbricos	15	15	15	15	15	15	APRECIABLE
27	[HW_NOS_WAP] Puntos de acceso inalámbricos.	15	15	15	15	15	15	APRECIABLE
28	[HW_NOS_TELIP] Telefonos IP	9	9	9	9	9	9	BAJO
29	[COM_NOS_INTERNET] Canal de Internet Dedicado.	20	20	20	20	25	21	CRITICO
30	[COM_NOS_LAN] Red Local Institucional.	20	20	20	20	20	20	IMPORTANTE
31	[COM_NOS_WLAN] Red Wifi Institucional.	15	15	15	15	15	15	APRECIABLE
32	[COM_NOS_TEL] Red Telefonica.	15	15	15	15	15	15	APRECIABLE
33	[AUX_NOS_POWER] Sistema Electrico.	15	15	15	25	25	19	IMPORTANTE
34	[AUX_NOS_CE] Cableado Estructurado.	15	15	15	15	15	15	APRECIABLE
35	[AUX_NOS_UPS] Sistema Alimentacion sin Interrupciones.	15	15	15	15	15	15	APRECIABLE
36	[L_NOS_DEP] Area de la Dirección de TI.	9	9	9	9	9	9	BAJO
37	[P_NOS_TECM] Tecnicos de Mantenimiento a Equipos de Computo.	20	20	20	20	20	20	IMPORTANTE
38	[P_NOS_DEVS] Ingenieros Desarrolladores	20	20	20	20	20	20	IMPORTANTE
39	[P_NOS_NETS] Ingenieros de Infraestructura y Redes.	20	20	20	20	20	20	IMPORTANTE
40	[P_NOS_TRED] Técnicos de Infraestructura y Redes.	20	20	20	20	20	20	IMPORTANTE

Fuente: Elaborada por el autor basado en el libro II “catálogo de elementos” de la metodología Magerit v.3.

6.1.10 Identificación de amenazas. La tarea MAR 2.1 de Magerit permite identificar las amenazas más relevantes sobre cada uno de los activos informáticos de Nostradamus (Dirección General de Modernización Administrativa de España, 2012). A continuación, se listan las amenazas identificadas para los activos de Nostradamus S.A.S, clasificándose de acuerdo con las cuatro categorías que proporciona la metodología (véase el Anexo A).

[N*] Desastres naturales
- [N1] Fuego
- [N2] Daños por agua

[I*] Desastres industriales
- [I1] Fuego
- [I2] Daños por agua
- [I4] Contaminación electromagnética
- [I5] Avería de origen físico o lógico
- [I6] Corte del suministro eléctrico
- [I7] Condiciones inadecuadas de temperatura o humedad
- [I8] Fallo de servicios de comunicaciones

[E] Errores y fallos no intencionados
- [E1] Errores de los usuarios
- [E15] Alteración accidental de la información
- [E2] Errores del administrador
- [E20] Vulnerabilidades de los programas (software)
- [E21] Errores de mantenimiento / actualización de programas (software)
- [E23] Errores de mantenimiento / actualización de equipos (hardware)
- [E24] Caída del sistema por agotamiento de recursos
- [E28] Indisponibilidad del personal
- [E4] Errores de configuración
- [E8] Difusión de software dañino
- [E9] Errores de [re-]encaminamiento

[A] Ataques deliberados
- [A11] Acceso no autorizado
- [A12] Análisis de tráfico
- [A14] Interceptación de información (escucha)
- [A18] Destrucción de información
- [A23] Manipulación de los equipos

[A24] Denegación de servicio
[A27] Ocupación enemiga
[A30] Ingeniería social (picaresca)
[A4] Manipulación de la configuración
[A5] Suplantación de la identidad del usuario
[A6] Abuso de privilegios de acceso

6.1.11 Valoración de las amenazas. El objetivo de la tarea MAR.22 es determinar la frecuencia y el porcentaje de degradación de las amenazas, es decir la probabilidad de que ocurra y el daño causado por la materialización de estos incidentes en Nostradamus (véase Anexo B). Para el cumplimiento de esta tarea se hace uso de las tablas descritas a continuación.

Tabla 7. Frecuencia.

	Nomenclatura	Categoría	Valoración
Probabilidad	MA	Prácticamente seguro	5
	A	Probable	4
	M	Posible	3
	B	Poco probable	2
	MB	Muy raro	1

Fuente: Elaborada por el autor basado en el libro I de la metodología Magerit v.3.

Tabla 8. Degradación

	Nomenclatura	Categoría	Valoración
Impacto	MA	Muy Alto	100%
	A	Alto	80%
	M	Medio	50%
	B	Bajo	10%
	MB	Muy Bajo	1%

Fuente: Elaborada por el autor basado en el libro I de la metodología Magerit v.3.

6.1.12 Identificación de salvaguardas existentes. Equivale a las medidas de protección y/o controles existentes en Nostradamus s.a.s y su correspondiente categorización en Magerit, permitiendo determinar el grado de seguridad que

presenta el sistema de información de la empresa. (Dirección General de Modernización Administrativa de España, 2012).

- Protecciones generales u horizontales. Nostradamus S.A.S tiene definidas algunas políticas de seguridad para sus operaciones diarias, a la vez cuenta con un manual de procesos y procedimientos que define claramente las actividades relevantes dentro del sistema de información de la empresa, principalmente las relacionadas con los procesos tecnológicos y que involucran a la Dirección de TI.

    - Control de acceso lógico. La empresa cuenta con la implementación de un firewall en su red corporativa, aplicando restricciones de acceso a contenidos, acceso de usuarios y aplicaciones. Los usuarios para el acceso al sistema, plataformas y correo electrónico son controlados y asignados por la Dirección de TI.

    - Segregación de tareas. El soporte y atención de los diferentes servicios está debidamente delegado de acuerdo con cada área. Cada profesional tiene asignadas funciones específicas dentro del sistema.

    - Herramienta contra código dañino. El firewall proporciona un servicio de protección contra amenazas que monitorea los equipos en la red corporativa, adicionalmente cada equipo tiene activo antivirus free o en versión de prueba.

    - Herramienta de monitorización de tráfico. El firewall instalado incluye la opción de monitorear el tráfico de la red.

- Protección de los datos / información. La información de los proyectos y actividades educativas que maneja la empresa, así como las bases de datos de usuarios y clientes son protegidas por Nostradamus mediante procedimientos definidos para copias de seguridad y restricciones de acceso.

    - Copias de seguridad de los datos (backup). Existe un procedimiento escrito para la realización de copias de seguridad de las bases de datos y los principales servidores de la empresa, con una frecuencia mensual.

    - Cifrado de la información. La empresa no hace uso de técnicas criptográficas en ninguno de sus procesos de manejo y procesamiento de información.

- Uso de firmas electrónicas. Las firmas electrónicas en Nostradamus solo son utilizadas en documentos de tipo financiero, para transacciones bancarias u otros procesos relacionados.

- Protección de los servicios. Nostradamus ofrece servicios en proyectos de educación y capacitación en uso de las tics como su principal actividad y como tal, requiere brindar seguridad a sus usuarios y clientes en todas sus actividades.

  - Aseguramiento de la disponibilidad. Las actividades educativas son coordinadas mediante un cronograma a fin de controlar y reducir el número de conexiones simultaneas a su plataforma tecnológica. El firewall implementado garantiza un nivel aceptable de seguridad en sus conexiones.

  - Se aplican perfiles de seguridad. Existen perfiles de usuario definidos con contraseñas generadas desde la dirección de TI.

  - Protección de servicios y aplicaciones web. Los proveedores de hosting para la plataforma tecnológica de Nostradamus proporcionan medidas de seguridad en la nube.

  - Protección del correo electrónico. El proveedor de correo electrónico corporativo provee medidas de seguridad integradas en línea.

  - Protección del directorio. El árbol de carpetas no es accesible desde el sitio web.

- Protección de las aplicaciones. Los sistemas que componen la plataforma tecnológica y educativa de Nostradamus implementan medidas que buscan garantizar un nivel de protección adecuado para sus actividades diarias.

  - Copias de seguridad (backup). Existe un procedimiento definido en el manual de procedimientos que contempla esta actividad.

  - Cambios (actualizaciones y mantenimiento). Los datos son almacenados en servidores para contar con la información actualizada.

- Protección de los equipos. Son contemplados los servidores que contienen las aplicaciones y las bases de datos de los sistemas educativo, financiero y proyectos, los servidores ftp, bases de datos, dominio; también los switches, routers principales, el firewall y los equipos de cómputo de todas las dependencias.

    - Se aplican perfiles de seguridad. Los equipos se encuentran instalados en la sala de servidores de la dirección de TI, solo tiene acceso a ellos el personal del área de infraestructura. Todos los controles de acceso al área son básicos y físicos, no existen controles de acceso lógicos, tecnológicos o de alta seguridad.

    - Aseguramiento de la disponibilidad. La protección de servidores y demás equipos que hacen parte de la infraestructura tecnológica de Nostradamus se centra en un firewall administrable con funciones de IDS. No cuenta con DMZ o cualquier otro sistema de protección. La disponibilidad de los servicios ofrecidos depende de capacidad de gestión del firewall corporativo.

    - Cambios (actualizaciones y mantenimiento). Son determinados de acuerdo a un cronograma definido de mantenimiento.

- Protección de las comunicaciones.

    - Protección de la integridad de los datos Intercambiados. La red local de la empresa permite la comunicación constante entre todas las dependencias para el procesamiento oportuno de los datos. La empresa hace uso de telefonía IP interna.

    - Internet. La empresa utiliza un servicio de internet dedicado con varias líneas para el acceso y puesta en marcha de su plataforma tecnológica.

- Protección de los soportes de información. La mayor parte de la información se encuentra almacenada en los servidores, las copias de seguridad se realizan en discos extraíbles custodiados en la dirección general y en forma física almacenada en folios ordenados por periodos en cada una de las áreas.

- Protección de los elementos auxiliares. En la dirección de TI se cuenta con un sistema de respaldo eléctrico que evita los cortes prolongados de energía en los servidores y mantiene los servicios de la empresa en alta, a la vez cuenta con un sistema de climatización encargado de mantener a una temperatura adecuada la sala de servidores.

    - Protección del cableado. Las conexiones cableadas representan un 70% de la red corporativa y el 30% restante es inalámbrica. Todo el cableado está centralizado en la dirección de TI y parte desde esta hacia todas y cada una de las dependencias de la empresa.

- Seguridad física – Protección de las instalaciones. La dirección de TI, la componen las dependencias de infraestructura, desarrollo y soporte, todas funcionando en una misma sede; la empresa cuenta con vigilancia privada que ofrece un control regular de acceso a las instalaciones.

    - Control de los accesos físicos. El acceso a la dirección de TI es abierto al personal de la empresa, excepto a las áreas que la componen infraestructura, desarrollo y soporte. El acceso a la sala de servidores está a cargo del área de infraestructura y su acceso se limita a mantenerse cerrado bajo llave. No posee controles biométricos o de otro tipo de tecnología.

    - Aseguramiento de la disponibilidad. La opción del ingreso a la sala de servidores se encuentra a cargo del director técnico de infraestructura, sin embargo todo el personal que labora en la dependencia, directa o indirectamente puede tener acceso ocasional al área de servidores.

- Salvaguardas relativas al personal. La dirección de TI cuenta actualmente con un grupo de 10 profesionales, y el apoyo de pasantes en prácticas estudiantiles de los últimos semestres del programa de ingeniería de sistemas, pertenecientes a corporaciones universitarias locales. No posee profesionales especialistas en Seguridad informática, ni su equivalente como oficial de seguridad. No se evidencia capacitación y/o socialización en seguridad de la información al personal de la empresa.

6.2 FASE 2: ANALISIS DE VULNERABILIDADES.

La situación que da origen al presente estudio contempla los ataques remotos de los cuales fue objeto Nostradamus S.A.S, entre los que se logró identificar el ataque a los sistemas operativos Windows haciendo uso de técnicas de ingeniería social; ataque de elevación de privilegios y robo de información a sistemas operativos Windows y por último, el ataque de denegación de servicios a la intranet de la empresa.

Por lo anteriormente expuesto, se procede a realizar un análisis de vulnerabilidades en el sistema informático de Nostradamus mediante la herramienta de escaneo Nessus, con el fin de identificar vulnerabilidades existentes y que probablemente fueron explotadas por los atacantes.

6.2.1 Escaneo de vulnerabilidades. Preparado el ambiente de trabajo y haciendo uso de la herramienta Nessus, se procede a realizar el escaneo de vulnerabilidades en el servidor principal de la red de Nostradamus, desde una maquina externa a la red corporativa, buscando identificar posibles riesgos de seguridad que comprometan a los activos de la empresa.

Figura 2. Resultados del escaneo de vulnerabilidades en la red Nostradamus.

Vulnerabilities — Total: 52

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	140532	PHP 7.2.x / 7.3.x < 7.3.22 Memory Leak Vulnerability
MEDIUM	5.0	142591	PHP < 7.3.24 Multiple Vulnerabilities
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	15901	SSL Certificate Expiry
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm

Fuente: Informe Nessus Essentials. Elaborada por el autor.

El escaneo realizado arroja un total de 52 posibles vulnerabilidades, de las cuales 13 son catalogadas con un nivel de explotación medio, 1 con nivel bajo y 38 de tipo informativo como se puede observar en la figura 2. Las vulnerabilidades de nivel medio identificadas permiten la explotación remota y están calificadas con CVSS entre 4 y 7 de score (véase Anexo D).

Analizados los resultados obtenidos en el escaneo, se puede concluir de manera preliminar que dado el tipo de las vulnerabilidades relevantes identificadas, existe una gran probabilidad que estas fueran explotadas por los autores de los ataques remotos, de los cuales fue víctima la empresa Nostradamus; así las cosas, se procede a realizar las consultas necesarias para determinar los mecanismos de solución a fin de corregir cada una de estas vulnerabilidades; así mismo con el objeto de determinar, fortalecer y complementar el planteamiento de las alternativas de solución, se determina realizar una serie de pruebas de penetración, recreando cada uno de los ataques sufridos por la empresa, las cuales se describen a continuación.

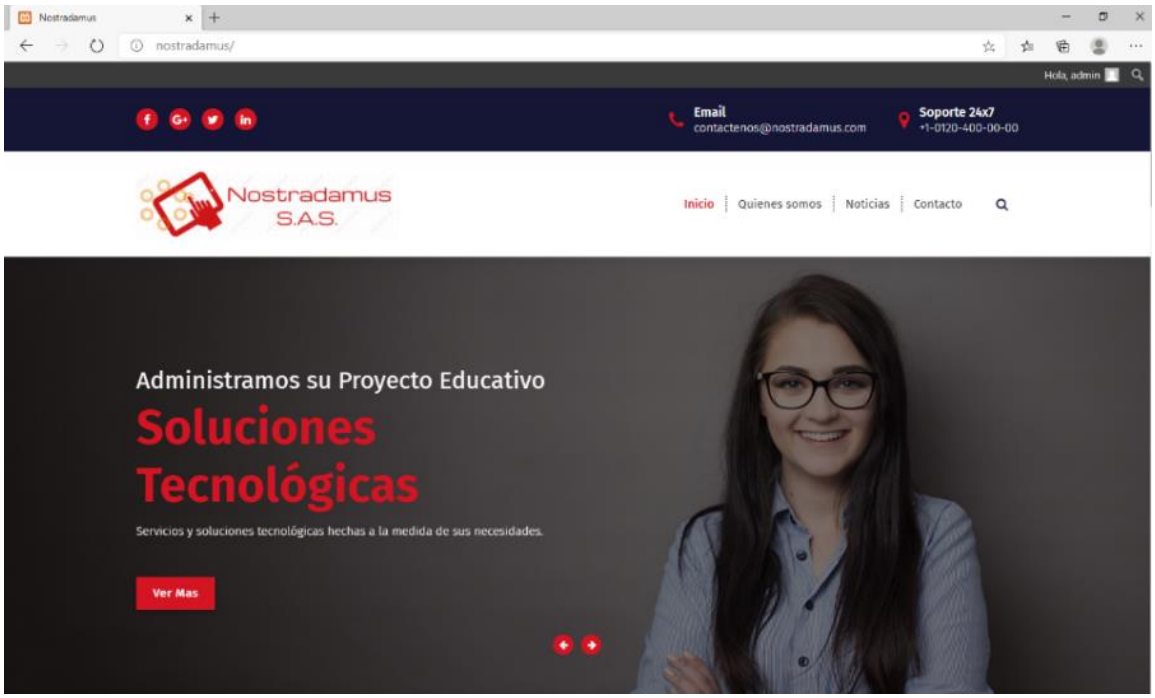
6.2.2 Ataque con Ingeniería social. La ingeniería social es el principio básico de casi todos los tipos de ataques existentes hoy en día, uno de los más comunes y todavía muy efectivo es el conocido como phishing, el cual basa su efectividad en las técnicas de la ingeniería social.

6.2.1.1 Suplantación del sitio web corporativo de Nostradamus. El phishing, es un delito informático que utiliza la ingeniería social para adquirir información confidencial de personas, empresas y organizaciones de forma fraudulenta. Son muchas y variadas las técnicas de ingeniería social que puede aplicar un atacante en combinación con un phishing, lo que pone de limite la imaginación del mismo.

Para el caso en estudio, el dominio www.nostradamus.com correspondiente al sitio web de Nostradamus S.A.S, puede ser fácilmente suplantado con el uso de caracteres Unicode en un ataque phishing, también conocido como ataque homográfico; esto consiste en suplantar parcial o totalmente las letras del dominio por caracteres de fuentes tipo Unicode, lo que permite poner en línea un sitio copia del original y aparentemente bajo el mismo dominio, alojado en un servidor malicioso y al cual los clientes y usuarios habituales de Nostradamus pueden verse expuestos entregando información confidencial de la empresa como credenciales de acceso y direcciones de correos corporativos y personales, entre otras. Este tipo

de ataque por lo general se convierte en el predecesor de ataques más complejos, basándose en el volumen y la calidad de la información que puede recopilar.

Figura 3. Sitio web Nostradamus S.A.S



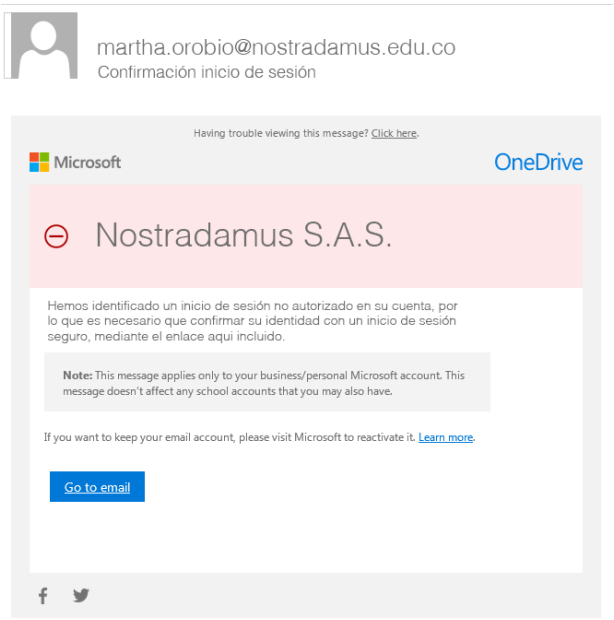
Fuente: Elaborada por el autor.

6.2.1.2 Suplantación del correo corporativo de Nostradamus. En el primer ataque expuesto, las credenciales de acceso de los usuarios registrados y clientes se presume que fueron expuestas ante los atacantes, pero las posibilidades de acceso a la información con mayor relevancia o un control total de la máquina víctima, son relativamente bajas, lo que requiere de la puesta en marcha de un nuevo ataque de phishing que no solo puede entregar a los atacantes información de la empresa sino también información personal de cada uno de sus clientes y usuarios.

Con las direcciones de correos de usuarios y clientes plenamente identificadas, resulta sencillo lanzar un nuevo ataque phishing dirigido a los clientes de Nostradamus S.A.S, el cual consiste en enviar un correo electrónico falso a cada una de las direcciones identificadas, haciéndose pasar como un correo procedente de la empresa, informando de una situación especial como un fallo de seguridad o una actualización de la plataforma, acompañado de un enlace al que se requiere

entrar para confirmar dicho evento, siendo direccionado a un login idéntico al original, donde el usuario procederá a digitar sus credenciales de acceso, entregando así la información requerida por el atacante; así mismo se puede dar la descarga de un archivo malware que permitirá al atacante tomar el control de la máquina del cliente.

Figura 4. Mensaje suplantando un correo corporativo de Nostradamus



Fuente: Elaborada por el autor.

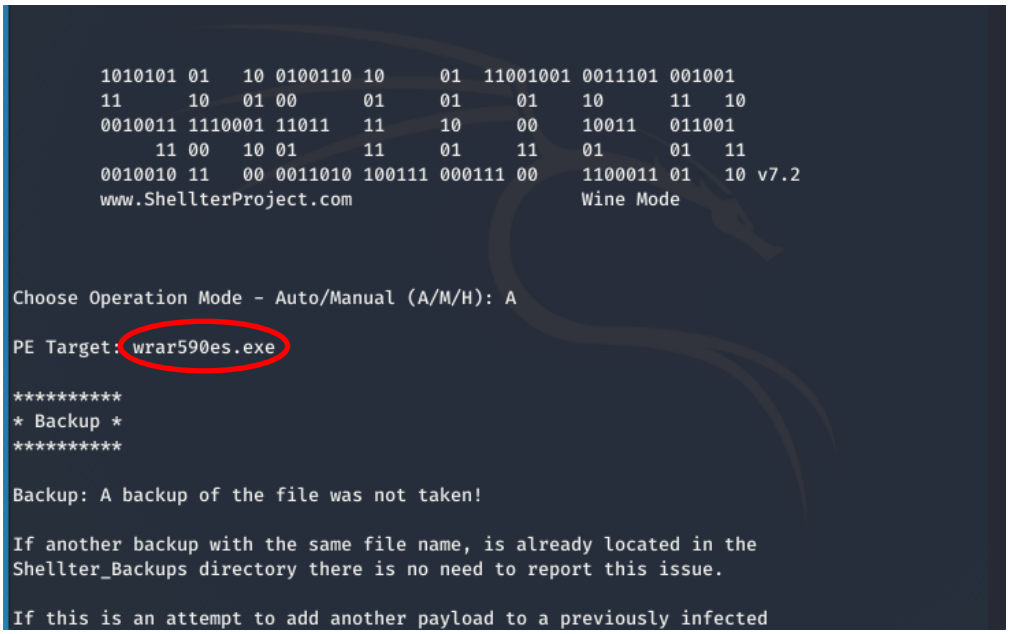
6.2.2 Ataque de escalada de privilegios. La escalada de privilegios es un tipo de ataque que se centra en identificar vulnerabilidades en un sistema informático con el fin de obtener acceso al mismo y una vez dentro, poder subir en privilegios obteniendo mayor acceso a la información en el sistema víctima.

Según las estadísticas publicadas por el portal cve.mitre.org el sistema operativo Windows 7, presenta alrededor de 336 vulnerabilidades que permiten el escalonamiento de privilegios en el sistema y alrededor de otras 372 que permiten la ejecución de código remoto, esto sin mencionar otros tipos de vulnerabilidades identificadas. En la lista también aparecen los sistemas operativos Windows 10 con un total de 130 vulnerabilidades de elevación de privilegios, Windows Server 2012 con 293 y Windows Server 2016 con 38 todas desde la salida al mercado de cada versión. La siguiente prueba describe uno de los posibles procedimientos adoptados

por los atacantes para vulnerar equipos de la empresa y escalar privilegios al interior del sistema informático de Nostradamus S.A.S.

Haciendo uso de la herramienta Shellter es posible tomar un archivo de una aplicación conocida y esconder malware dentro de los binarios de un archivo de instalación como .exe; para el presente caso se utilizara el instalador de la aplicación winrar, con nombre wrar590es.exe, inyectándolo con un payload capaz de crear un backdoor en el sistema infectado, una vez se complete el proceso con éxito, el cual puede incluir el uso de las técnicas que proporciona la ingeniería social en combinación con otras herramientas de explotación. En la figura 5, se observa la preparación del archivo malicioso.

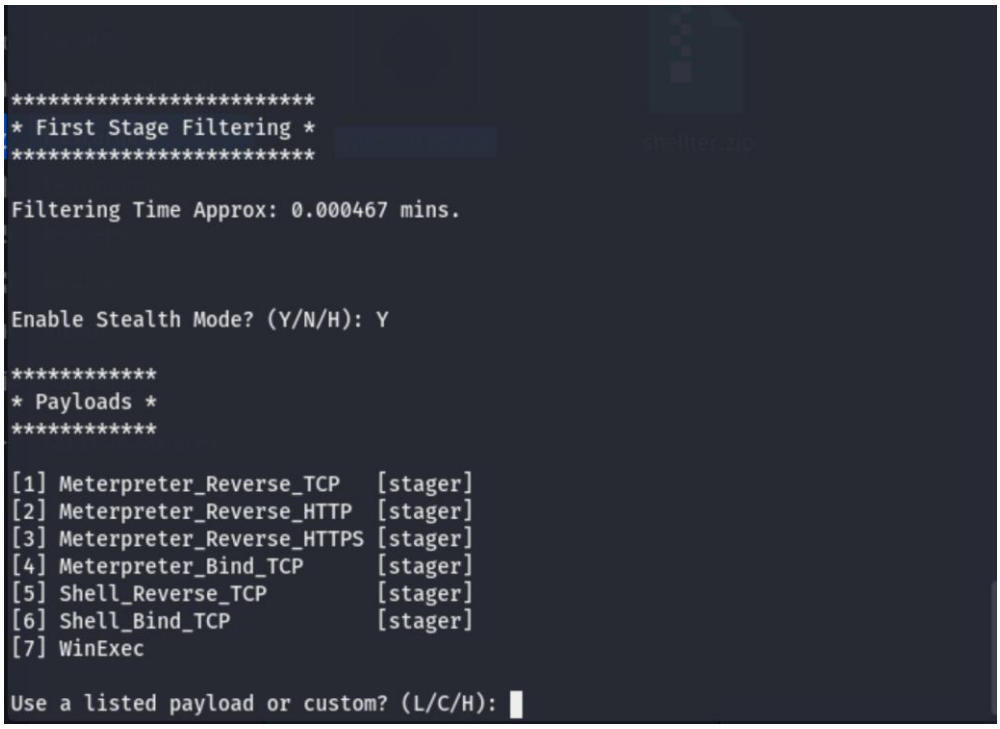
Figura 5. Pantalla de ejecución de la herramienta Shellter.



Fuente: Elaborada por el autor, ejecución de Shellter.

Shellter tiene una gran eficiencia frente a la mayoría de antivirus, siendo casí indetectable por los mismos, lo cual ofrece un alto porcentaje de éxito. Una vez es seleccionado el archivo a infectar, el programa realiza todo el proceso de forma automática hasta llegar a una segunda pantalla, donde solicita escoger el payload a utilizar, como se observa en la figura 6.

Figura 6. Configuración de payload en la herramienta Shellter.

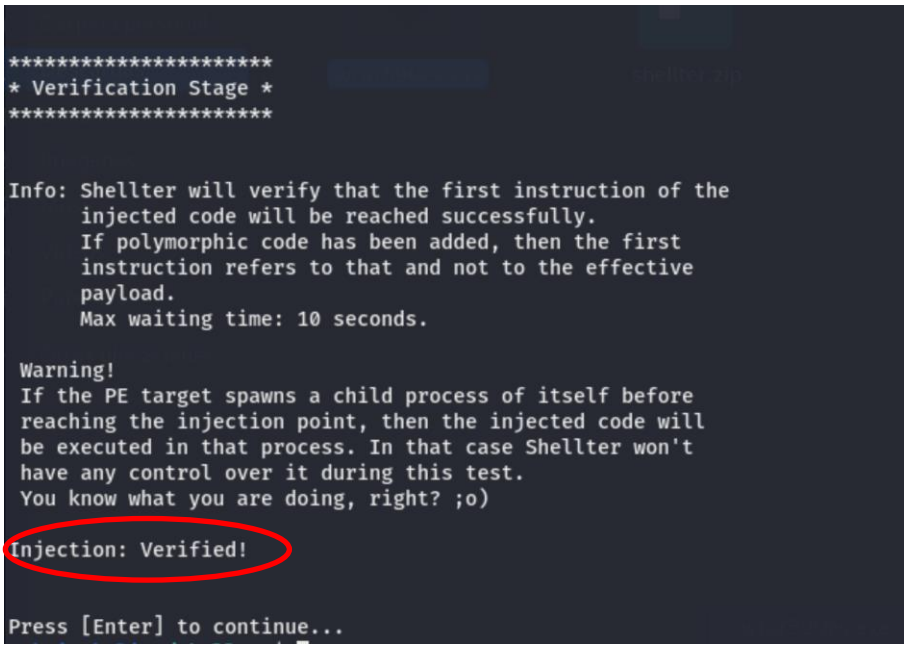


Fuente: Elaborada por el autor, ejecución de Shellter.

Para finalizar, se escoge del listado el payload meterpreter_reverse_tcp, que permitirá la creación del backdoor en la víctima, así mismo, se configura la ip y el puerto de la máquina que escuchará la conexión, después de esto la herramienta termina el proceso automáticamente, confirmando que el ejecutable está preparado para ser enviado.

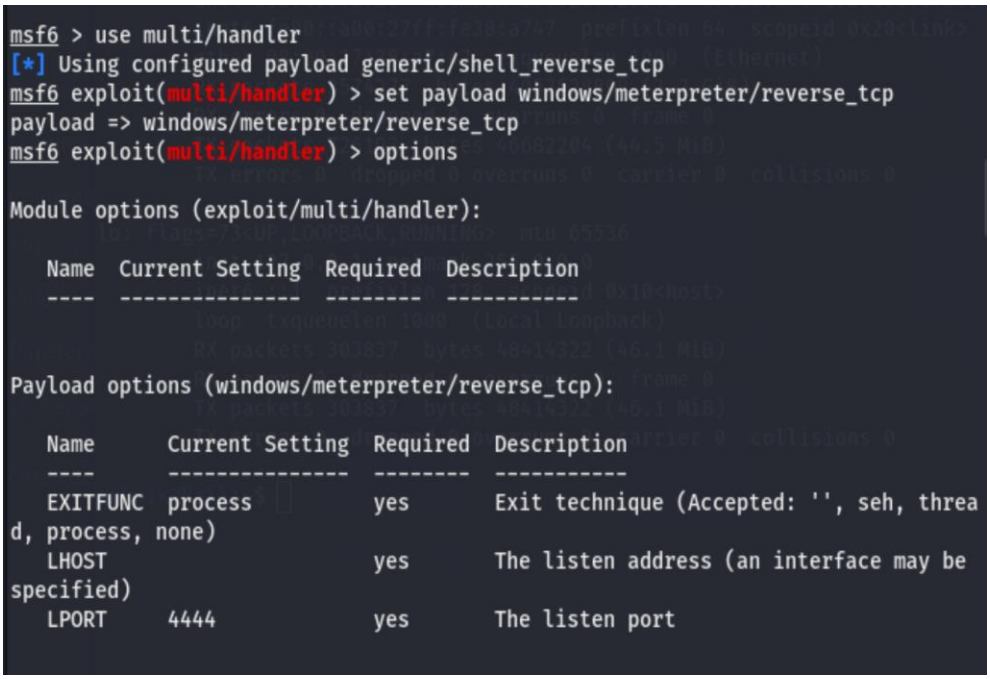
Por otro lado, se procede a realizar la configuración correspondiente para metasploit en la máquina que recibirá la conexión remota, esto se logra utilizando el exploit multi/handler con el payload windows/meterpreter/reverse_tcp como se observa en la figura 8. Luego mediante la manipulación de una cuenta de correo electrónico conocida, tal y como se describió en el punto 6.2.1.2, el archivo infectado es enviado a la empresa haciéndolo parecer que procede de una fuente conocida y confiable, a fin de lograr que un usuario al interior de la red corporativa lo descargue e intente abrirlo, hecho esto, el atacante recibirá una conexión remota comprometiendo no solo la seguridad sino toda la información del sistema de la empresa Nostradamus.

Figura 7. Inyección de payload completa con Shellter.



Fuente: Elaborada por el autor, ejecución de Shellter.

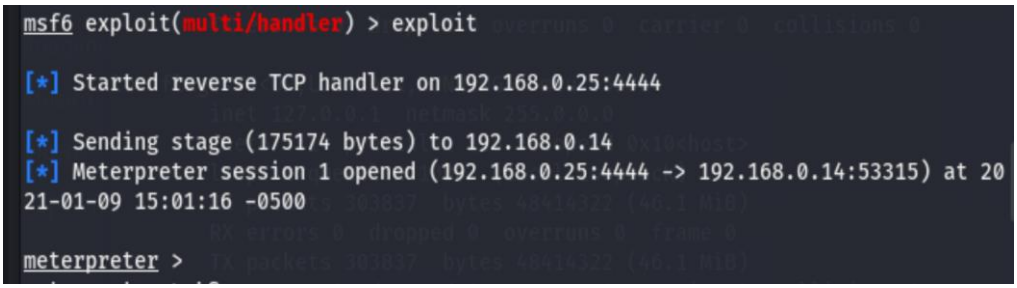
Figura 8. Configuración de metasploit



Fuente: Elaborada por el autor

Cumplido el objetivo primario, en metasploit se crea de manera inmediata una sesión en meterpreter, abriendo una consola directamente en la máquina victima lo que permitirá escalar privilegios hasta comprometer todo el sistema de la empresa; a esta sesión se le puede configurar lo que se conoce como persistencia, permitiendo que el atacante no pierda el control pese a los reinicios de la víctima.

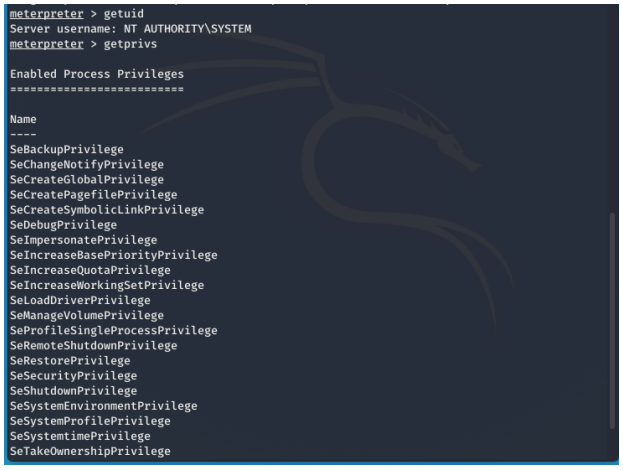
Figura 9. Sesión de meterpreter abierta en la victima con metasploit



Fuente: Elaborada por el autor

Con la sesión iniciada en la víctima, el paso a seguir es adquirir los permisos necesarios para acceder a toda la información almacenada en la maquina infectada y comprometer todas las maquinas posibles conectadas a la red corporativa, por lo que es necesario adquirir privilegios de administrador, esto se logra ingresando los comandos getuid y getprivs

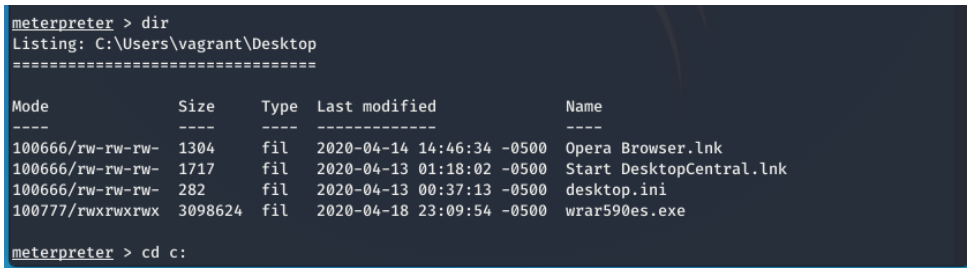
Figura 10. Escalada de privilegios en la victima con sesión de meterpreter.



Fuente: Elaborada por el autor

Con los permisos de administrador adquiridos, el atacante tiene el acceso a la información almacenada en el equipo, e incluso la almacenada en red corporativa, con tan solo digitar unos pocos comandos básicos. Como se observa en la figura 11, el atacante ya tiene acceso y control total de su víctima.

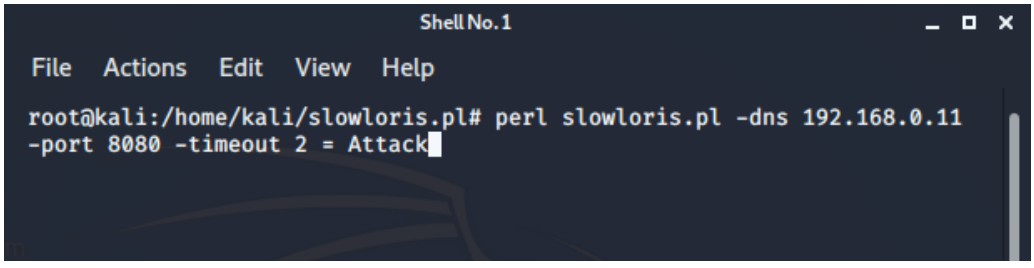
Figura 11. Ataque completo con acceso total y remoto.



Fuente: Elaborada por el autor

6.2.3 Ataque denegación de servicios. Este tipo de ataques conocidos como Dos o DDoS, consisten en enviar un número elevado de peticiones a una dirección ip o dominio específico, buscando que el servidor objeto del ataque, o incluso todo un sistema informático, sea incapaz de gestionar todas las peticiones, haciendo que el tráfico recibido sea difícil de distinguir del tráfico normal comprometiendo en gran manera la disponibilidad y capacidad del sitio, forzando la detención o reinicio de todos los servicios.

Figura 12. Configuración de un ataque de denegación de servicios con Slowloris.



Fuente: Elaborada por el autor. Terminal maquina atacante con Slowloris.

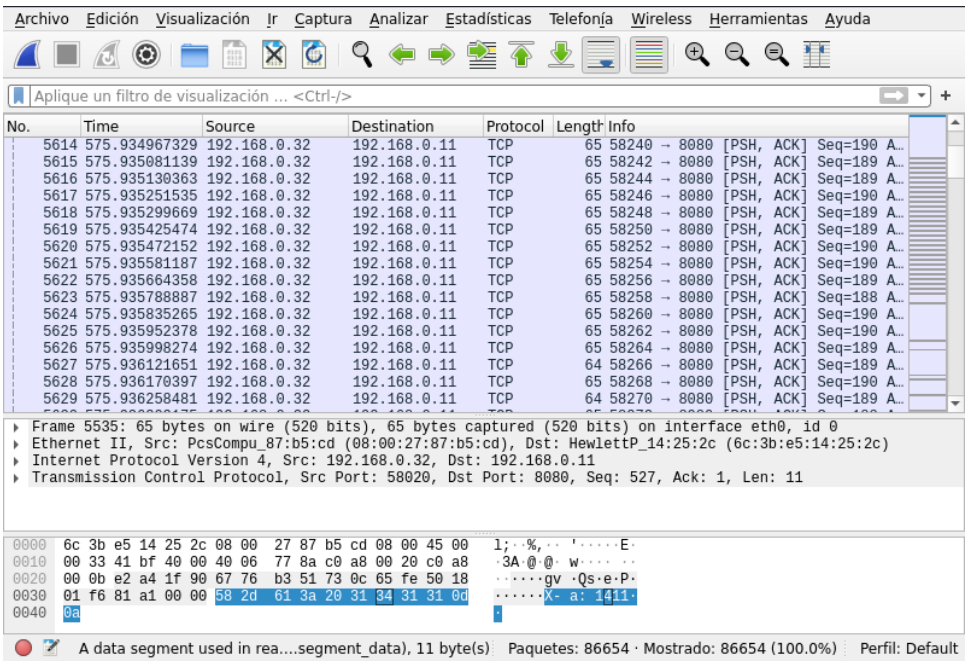
Por lo general, para llevar a cabo este tipo de ataques se necesita de lo que se conoce como “botnet” o “red zombie”, la cual consiste en una red compuesta por

miles de computadores, dispositivos IoT o cualquier otro dispositivo conectado a internet, infectados previamente con un tipo de malware, que permite controlarlos de forma remota.

Para el desarrollo de la siguiente prueba se utiliza una herramienta con la capacidad de generar una gran cantidad de tráfico desde una sola máquina, cuyo nombre es Slowloris, esta herramienta puede realizar un ataque de denegación de servicios a un servidor web o un servidor proxy utilizando tráfico legítimo, enviando solicitudes en intervalos controlados, hasta agotar todas las conexiones disponibles en el servidor.

Una vez configuradas todas las opciones necesarias para el ataque desde la maquina con Slowloris, como muestra la figura 12, se inicia el ataque hacia el servidor que aloja la intranet de la empresa Nostradamus; por otro lado, haciendo uso del programa Wireshark se analiza todo el trafico generado durante este ataque.

Figura 13. Identificación de un ataque DOS en ejecución con Wireshark.



Fuente: Elaborada por el autor.

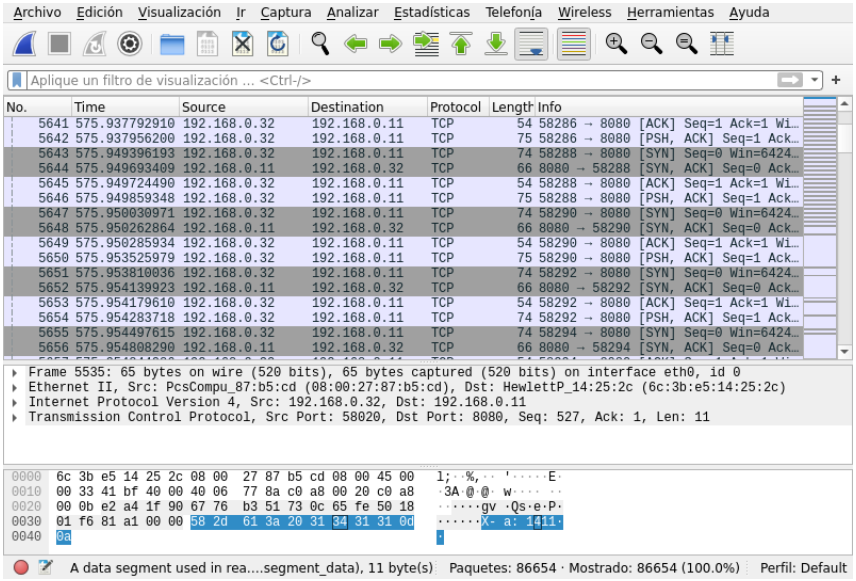
Nostradamus, posee una buena infraestructura de red que cuenta entre sus medidas de protección con un dispositivo firewall e IDS incorporado, aunque

proporciona un nivel de protección alto, queda evidenciado que puede resultar insuficiente ante la posibilidad de ocurrencia de ataques más complejos e intensos, como el que motivó el desarrollo del presente estudio.

En la figura 13, se puede observar la captura de tráfico con Wireshark, donde aparecen todas las peticiones realizadas desde la maquina Slowloris al servidor web de Nostradamus, evidenciando la presencia de un posible ataque malicioso, a su vez, el programa aporta información relevante sobre el mismo, como lo son las direcciones ip de origen y destino, los puertos involucrados o comprometidos en el ataque y la información de cada una de las capas que componen los diferentes paquetes.

Al cabo de un corto periodo de tiempo el ataque empieza a cumplir con su objetivo, saturando de peticiones al servidor web, haciendo parecer que se trata de un tráfico legítimo, como muestra la figura 14, donde se evidencian las tramas completas de un three way handshake, indicando una conexión estable entre la máquina maliciosa y el servidor web sobrecargando la capacidad de respuesta de este último.

Figura 14. Análisis del ataque DOS en ejecución con Wireshark

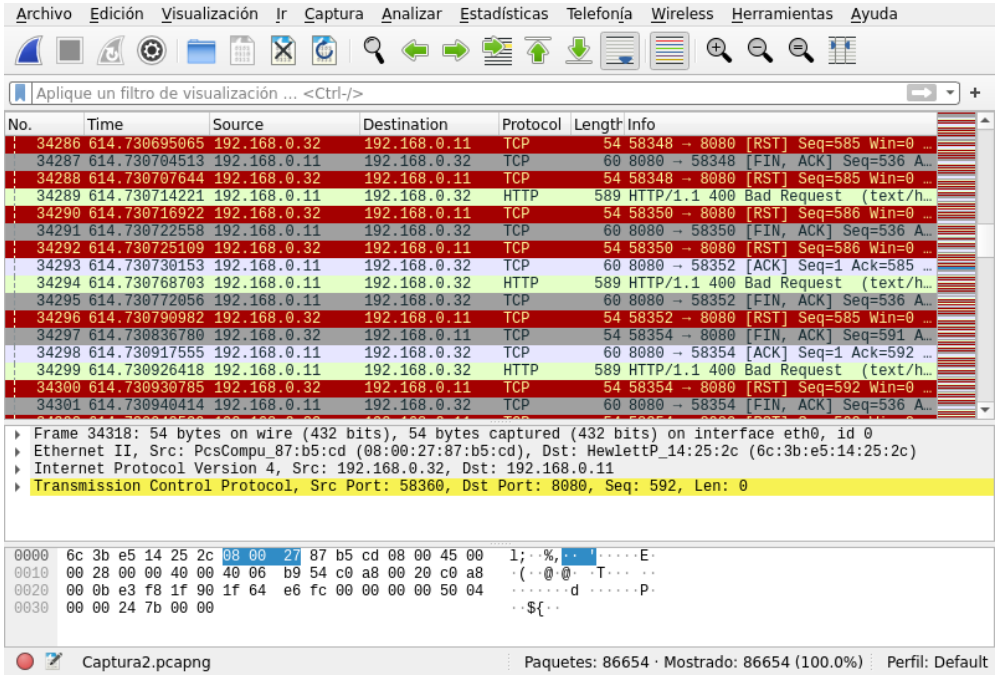


Fuente: Elaborada por el autor.

Poco a poco el servidor de Nostradamus empieza a perder eficiencia ante el numero elevado de peticiones recibidas, sobrepasando la capacidad de sus recursos al no

poder procesarlas ni darles respuesta, con una conexión inestable el servidor queda fuera de línea, como muestra el análisis de tráfico con Wireshark en la figura 15.

Figura 15. Ataque DOS exitoso analizado con Wireshark



Fuente: Elaborada por el autor.

6.3 FASE 3: DEFINICIÓN DE CONTROLES Y POLÍTICAS DE SEGURIDAD.

6.3.1 Hallazgos del análisis y gestión del riesgo. Realizado el proceso de análisis y gestión del riesgo al que se encuentran expuestos los activos de información de la empresa Nostradamus S.A.S y en consecuencia con lo definido en el alcance del mismo estudio, se concluye realizar acciones de tratamiento sobre los activos con riesgos identificados como importantes y críticos.

El análisis arroja un total de 19 activos con alto riesgo acumulado, de los cuales 4 corresponden a la categoría de críticos y 15 a la categoría de importante. Entre los activos críticos se contempla el servidor de bases de datos, la plataforma tecnológica institucional y los servicios de capacitación y educación ofrecidos por la empresa; entre los activos con un riesgo importante aparecen las copias de

seguridad de la información, el portal web de la empresa, el sistema eléctrico y el personal de la dirección de TI (véase el Anexo C).

Según la calificación del riesgo para estos activos, el riesgo acumulado es muy similar situándolos en un rango superior entre 17 y 25 de acuerdo con la tabla de criterios de valorización del riesgo; esto significa que las amenazas identificadas son similares para estos activos y pueden tratarse con controles y/o políticas globales, así las cosas, según su nivel de riesgo y prioridad, las siguientes son las afectaciones más representativas para el sistema informático de Nostradamus S.A.S.

- Posible ataque de escalada de privilegios con una alta probabilidad de compromiso de la integridad y disponibilidad del sistema de información de Nostradamus S.A.S.

- Posible suplantación de usuarios del sistema debido a debilidades en la protección de contraseñas, afectando la confidencialidad e integridad de la información.

- Errores de mantenimiento y actualización en servidores, equipos de cómputo y dispositivos de red, que conducen a una probable afectación de la disponibilidad de los servicios ofrecidos por la empresa.

- Uso incorrecto de los activos informáticos y/o recursos del sistema de información, debido a la falta de políticas que lo regulen.

- Fallas en la administración, configuración y/o manipulación del sistema, derivadas en una probable afectación a la disponibilidad, confidencialidad e integridad del mismo.

- Ausencia de un sistema de detección temprana de amenazas y/o vulnerabilidades en la infraestructura informática de Nostradamus S.A.S.

6.3.2 Hallazgos del análisis de vulnerabilidades. A partir de la realización del escaneo de vulnerabilidades con la herramienta Nessus, junto a las pruebas de vulnerabilidad que recrearon los ataques al sistema informático de Nostradamus S.A.S, se evidenciaron brechas de seguridad presuntamente explotadas durante los ataques de los cuales la empresa fue objeto y que afectaron sus servicios y la

disponibilidad, confidencialidad e integridad de su plataforma tecnológica, a continuación, se listan los riesgos encontrados.

- Falta de actualizaciones de seguridad en servidores y equipos de seguridad y administración de la red.
- Certificados SSL no confiables, vencidos y autofirmados
- Detección de protocolo TLS Versión 1.0
- Métodos HTTP TRACE / TRACK activos
- Vulnerabilidades de desbordamiento y fuga de memoria
- Vulnerabilidad de autenticación en SMB
- Detección remota de la red mediante mDNS
- Vulnerabilidades por falta de actualización de parches de seguridad en equipos con sistema operativo Windows.
- Contraseñas débiles para el acceso a dispositivos de red.
- Fallas en los controles de acceso y autenticación en la red inalámbrica de la entidad.

6.3.3 Declaración de aplicabilidad. En este documento están incluidos todos los controles de seguridad correspondientes a Nostradamus S.A.S, conforme a la norma ISO/IEC 27001:2013, con información de su estado y aplicabilidad (véase Anexo E).

6.3.4 Políticas generales para la seguridad de la información. Atendiendo las necesidades identificadas en materia de seguridad informática y en aras de preservar la disponibilidad, integridad y confidencialidad de la información propia de cada uno de los procesos gestionados por Nostradamus S.A.S, se definen las siguientes políticas de seguridad de la información, como parte de la propuesta del nuevo sistema de seguridad para Nostradamus S.A.S.

- Creación del comité de riesgos y seguridad de la información, cuyas funciones están encaminadas al mantenimiento, evaluación y mejora del sistema de seguridad de la información de la empresa con una periodicidad semestral recomendada.

- Establecer compromisos periódicos en materia de seguridad de la información, los cuales deben ser socializados y asumidos por todo el personal vinculado laboralmente con la empresa y los clientes o usuarios que hacen uso de sus servicios.

- Todos los equipos de cómputo que hacen parte de la red de Nostradamus estarán unidos a un servidor de dominio corporativo, no se aceptan equipos personales de funcionarios, contratistas o usuarios unidos a los mismos segmentos de red utilizados para las labores propias de la empresa. El personal visitante u ocasional podrá hacer uso de una red wifi controlada y dispuesta estos casos.

- La asignación de usuarios y contraseñas para el acceso a las herramientas y recursos informáticos de la empresa, así como el correo electrónico corporativo, estará a cargo de la dirección de TI y deberá contar con unos requisitos de seguridad específicos, políticas de grupo y acceso definidas, así como doble factor de autenticación.

- Solo se permite el uso de software licenciado en los equipos de cómputo y servidores de Nostradamus. Cualquier requerimiento de instalación de software adicional deberá ser autorizado por la dirección de TI e instalado con su licencia respectiva, por personal autorizado de dicha dependencia.

- La realización de las copias de seguridad o backup de información, estará a cargo de la dirección técnica de soporte en cabeza de la dirección de TI, quien garantizará el almacenamiento y respaldo de toda la información corporativa, definiendo criterios de respaldo, clasificación, niveles de seguridad, tiempo de retención , pruebas de restauración y contratos de custodia y almacenamiento externos a la empresa.

- Toda la información tanto física como digital, producto de los procesos internos de Nostradamus S.A.S debe ser catalogada por el funcionario custodio o el área responsable de la misma, conforme a las directrices emitidas por el comité de riesgos y seguridad de la información, garantizando los principios de la confidencialidad, integridad y disponibilidad de la información.

- Los funcionarios y usuarios del sistema informático de la empresa tienen la obligación de reportar cualquier incidente o evento sospechoso que se presuma

pueda afectar la seguridad de la información, así como el mal uso de los recursos informáticos; los cuales deben ser debidamente documentados por la dirección de TI para su seguimiento y control.

- El personal que labora en la empresa, así como las nuevas contrataciones y/o vinculaciones, será capacitado regularmente en materia de seguridad de la información, a fin de mitigar la probabilidad de riesgo originada por errores humanos, esta actividad estará a cargo de la dirección de TI.

- La red corporativa contará con un análisis de tráfico y monitoreo permanente, junto con otras medidas de protección como, filtrado de contenidos, filtrado por MAC y protección antivirus, apoyadas en la implementación y configuración de dispositivos y herramientas de alto desempeño.

- La dirección de TI deberá garantizar el correcto funcionamiento de los servidores, equipos de cómputo, red corporativa, red eléctrica y red de telecomunicaciones de la empresa, así como los elementos auxiliares que hagan parte de estas, mediante un plan estratégico de mantenimientos correctivos y preventivos programados regularmente.

- Es responsabilidad de la dirección general de Nostradamus S.A.S garantizar el funcionamiento del sistema de seguridad de la información y la continuidad del negocio.

6.3.5 Política de seguridad física. Se presenta la política de seguridad para los activos y/o recursos físicos de Nostradamus S.A.S.

- El acceso al área de servidores y centro de cableado deberá estar protegida mediante mecanismos de autenticación biométrica y tarjetas de proximidad.

- El área de servidores deberá contar con un sistema de control ambiente que garantice las condiciones óptimas de temperatura y humedad para el buen funcionamiento de los equipos.

- El acceso a las instalaciones de la empresa será controlado mediante personal de seguridad privada apoyado con un sistema de video interno.

- La red corporativa deberá contar con seguridad perimetral, verificando constantemente los servicios activos con el apoyo de herramientas de monitoreo debidamente actualizadas.

6.3.6 Política de uso de recursos informáticos. A continuación, se presentan las directrices para el uso de los equipos de cómputo, medios de almacenamiento y periféricos en Nostradamus S.A.S.

- La dotación y disposición de equipos en las diferentes áreas de la empresa estará determinada por la dirección de TI.

- El personal de la empresa, contratistas o terceros no están autorizados para modificar la disposición y configuración de los equipos y periféricos dispuestos en las áreas de trabajo.

- Se prohíbe el uso de dispositivos de almacenamiento particulares o personales en las instalaciones de Nostradamus S.A.S; los medios de almacenamiento autorizados serán los dispuestos por la dirección de TI.

- En los equipos de cómputo de Nostradamus S.A.S se debe cumplir con la práctica de escritorio limpio, no se deben almacenar archivos en esta parte del equipo a fin de evitar cualquier tipo de fuga de información.

6.4 FASE 4: DISEÑO DEL SISTEMA DE SEGURIDAD DE LA INFORMACION

En consecuencia, con los riesgos, amenazas y vulnerabilidades identificadas en la plataforma tecnológica de Nostradamus S.A.S, al igual que con los criterios de aceptación del riesgo definidos, se desarrolla a continuación, la propuesta de diseño del sistema de seguridad de la información para la empresa Nostradamus S.A.S.

6.4.1 Gestión de incidentes técnicos de seguridad informática. El objetivo de esta actividad es prevenir la explotación de vulnerabilidades de tipo técnico en Nostradamus S.A.S y estará bajo la responsabilidad del comité de riesgos y seguridad de la información, sus tareas específicas son.

- Promulgar mediante actuación administrativa las políticas de seguridad de la información diseñadas para Nostradamus S.A.S.

- Establecer los roles y responsabilidades necesarios para llevar a cabo una eficiente gestión de vulnerabilidades.

- Definir herramientas de escaneo permanente del tráfico de la red para la identificación de eventos que puedan derivar en la explotación de posibles vulnerabilidades en la plataforma tecnológica de la empresa.

- Evaluar y analizar los registros de logs y posibles eventos maliciosos identificados mediante las herramientas de monitoreo; ante alguna alarma o sospecha de ataque o vulneración de la seguridad, se debe hacer seguimiento inmediato para corregir las fallas detectadas y repetir los backup realizados.

- Construir una línea de tiempo para la reacción oportuna ante la notificación o identificación de posibles vulnerabilidades en la plataforma tecnológica de la empresa.

- Documentar todos los casos notificados o identificados como posibles eventos que afecten la seguridad de la información en la empresa, con el fin de tomar de forma oportuna, las acciones correctivas requeridas.

- Realizar un seguimiento periódico del proceso de gestión de riesgos y vulnerabilidades junto a una evaluación continua del mismo.

6.4.2 Sensibilización y capacitación en seguridad de la información. Esta actividad tiene por objetivo generar una cultura de la seguridad informática en el personal vinculado laboralmente a la empresa Nostradamus S.A.S y estará bajo la responsabilidad de la dirección de TI, sus tareas específicas son.

- Realización de talleres de sensibilización a través de actividades personalizadas con temáticas como la socialización de las políticas de seguridad de la empresa, las modalidades de ataques y delitos informáticos, la seguridad de la información, entre otros.

- Diseñar un material pedagógico digital que apoye el proceso de capacitación y sensibilización del personal que labora en la empresa, en materia de seguridad de la información.

- Incluir una temática introductoria de seguridad de la información en el proceso de inducción de nuevos empleados y contratistas.

6.4.3 Adquisición y desarrollo seguro de sistemas de información. Esta actividad tiene como objetivo controlar y promover el desarrollo seguro en Nostradamus S.A.S y estará a cargo de la dirección técnica de desarrollo, sus tareas específicas son.

- Implementar mecanismos y/o reglas de validación para los diferentes tipos de datos y conjuntos de valores válidos.

- Validación de campos en transacciones, validación contra tablas, validación de llaves únicas y llaves foráneas.

- Revisión periódica de la integridad de los datos contenidos y/o capturados a través de las herramientas tecnológicas y aplicativos vigentes.

- Implementación de procedimientos automatizados en cada una de las fuentes de ingreso para el procesamiento de los datos recibidos.

- Generación automática de reportes para la identificación de inconsistencias durante el procesamiento de los datos.

- Establecer procedimientos para el reporte y reprocesamiento de errores y transacciones fallidas durante la ejecución de los procesos.

- Las actualizaciones de las aplicaciones sólo deberán ser realizadas por personal autorizado de la dirección de TI.

- Todas las actualizaciones, nuevas versiones y liberaciones de software o cualquier herramienta técnologica, deben estar documentados y debidamente versionados.

- La dirección de TI, estará a cargo del almacenamiento de las antiguas versiones de software y su documentación debidamente aprobada.

- Se debe garantizar la independencia entre los ambientes de desarrollo y producción, evitando la transferencia de código fuente entre los mismos y la existencia de cuentas de usuarios activas, con acceso a ambos ambientes.

6.4.4 Seguridad de la red corporativa. El objetivo de esta actividad es prevenir y controlar cualquier tipo de intrusión no autorizada en la red corporativa de Nostradamus S.A.S y estará bajo la responsabilidad de la dirección técnica de infraestructura en cabeza de la dirección de TI, sus tareas específicas son.

- Implementación de mecanismos de defensa perimetral con varias capas, compuestos por la instalación de una zona desmilitarizada (DMZ) y varios firewalls en la red corporativa de Nostradamus S.A.S.

- Monitoreo, seguimiento y registro de los eventos de seguridad tanto en el perímetro como en el interior de la red corporativa.

- Utilizar herramientas de análisis de tráfico y monitoreo permanente de la red.

- Aplicar el filtrado por MAC y las políticas de filtrado de contenidos, desde el firewall principal de la red corporativa.

- Todos los equipos de cómputo de la empresa deben trabajar unidos al dominio corporativo.

- Realizar un escaneo periódico de vulnerabilidades en la red corporativa.

- Mantener actualizados los sistemas operativos con los últimos parches de seguridad e implementar las soluciones a nuevas vulnerabilidades publicadas en los boletines de seguridad reconocidos.

CONCLUSIONES

Durante los últimos años se ha hecho evidente un incremento considerable de incidentes de seguridad en diferentes sistemas informáticos de grandes compañías alrededor del mundo; razón que ha motivado la necesidad urgente de proteger la información por ser el activo de más impacto para cualquier organización tanto económicamente como por su imagen y credibilidad frente a sus clientes. El análisis de seguridad a las infraestructuras de TI y la gestión y tratamiento del riesgo permiten a las organizaciones la implementación de normas y procesos tendientes a conformar un sistema de gestión de seguridad de la información.

El análisis y gestión del riesgo mediante la metodología Magerit v.3, proporciona información confiable sobre las amenazas y debilidades presentes en un sistema informático como el de Nostradamus S.A.S, esto permite una eficiente toma de decisiones en materia de seguridad informática garantizando la mitigación exitosa de los riesgos identificados y un alto porcentaje de seguridad en cada uno de sus procesos.

Las pruebas de penetración permiten a las empresas y organizaciones identificar el nivel de seguridad de sus sistemas informáticos, identificando brechas de seguridad que eventualmente pueden convertirse en un posible medio de explotación para vulnerar el sistema; así mismo, una vez identificado el riesgo, posibilita la implementación de controles que mitiguen el mismo.

Las políticas, controles y procedimientos de seguridad implementados en Nostradamus S.A.S, conforman el conjunto de normas que la entidad debe cumplir para el aseguramiento de su plataforma tecnológica y por consiguiente su información. Este sistema de seguridad involucra todas las dependencias de la empresa como un conjunto de engranes trabajando por la protección de sus activos.

RECOMENDACIONES

El sistema de seguridad informático de Nostradamus S.A.S requiere una revisión periódica, si se tiene en cuenta que diariamente la evolución de las tecnologías es evidente y con ella el actuar de los cibercriminales también crece, por lo que se recomienda una evaluación periódica del sistema informático de la empresa, buscando mantener bajo control tanto los riesgos ya identificados como posibles nuevas amenazas.

La realización de campañas de información y sensibilización en materia de seguridad informática permitirá generar sentido de pertenencia y apropiación en todos los empleados de Nostradamus S.A.S a la vez que facilita la mitigación de riesgos originados por acciones humanas voluntarias o involuntarias; por lo tanto, se recomienda definir un plan de sensibilización y capacitación en materia de seguridad informática, con una periodicidad semestral mínima.

El desarrollo propio de aplicaciones y software en Nostradamus S.A.S facilita la oportuna atención de los requerimientos de clientes y usuarios, brindando soluciones efectivas a través de su plataforma tecnológica, por tal motivo es necesario que este desarrollo y adaptación de las herramientas tecnológicas a las necesidades del cliente se realice bajo las buenas prácticas de desarrollo de software implementando técnicas de seguridad.

Las pruebas de vulnerabilidad junto al análisis de riesgo aplicado a Nostradamus S.A.S muestra a los servidores de la empresa como los activos con más alto riesgo de ser atacados, evidenciando vulnerabilidades existentes y amenazas potenciales; dada esta situación se recomienda migrar los servidores físicos a la nube donde el nivel de seguridad que se puede implementar es mucho más avanzado, con tecnologías para el monitoreo de correos, WAF, NGFW, IDS y herramientas de mitigación de DDoS entre otras.

BIBLIOGRAFÍA

ALFARO, Ivan y VARGAS, Edwin. Diseño del plan de seguridad informática del sistema de información misional de la procuraduría general de la nación. Bogotá D.C., 2016. Trabajo de grado (especialista en seguridad informatica). Universidad Piloto de Colombia. Facultad de ingeniería.

ARDILA NAVARRETE, Julian. Diseño de un sistema de gestiòn de seguridad de la informaciòn (sgsi) basado en la norma iso/iec 27001 para positiva compañía de seguros s.a en la ciudad de Bogotá. Bogotá D.C., 2016. Trabajo de grado (especialista en seguridad informatica). Universidad Nacional Abierta y a Distancia. Escuela de ciencias basicas e ingenieria.

CALERO, Angie y PARDO, Maby. Propuesta de modelo de un sistema de gestión de la seguridad de la información aplicada a instituciones educativas. Bogotá D.C., 2017 Trabajo de grado (Ingeniero en telemática). Universidad Distrital Francisco Jose de Caldas. Facultad de ingeniería.

CEPEDA, Maria. Implementación de un estándar de calidad para la seguridad de la información en la empresa Insurcol Ltda. bajo la norma ISO 27001: 2013. Bucaramanga, 2016. Trabajo de grado (ingeniero industrial). Universidad Santo Tomas. Facultad de ingeniería industrial.

CHICANO TEJADA, Ester. Auditoría de seguridad informática. Andalucía : IC Editorial, 2014.

CLOUDFLARE, Inc. Cloudflare.com: DNS Flood DDoS Attack {En línea}. {19 de noviembre de 2020}. Disponible en: (https://www.cloudflare.com/learning/ddos/dns-flood-ddos-attack/).

CONGRESO DE COLOMBIA. Mintic.gov.co: Ley 1273 de 2009 - Ministerio de Tecnologías de La Información y las Comunicaciones, 04 de 01 de 2009. {En línea}. {23 de noviembre de 2020}. Disponible en:(https://www.mintic.gov.co/portal/inicio/3705:Ley-1273-de-2009).

DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA DE ESPAÑA. Magerit versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas

de Información - Libro I. Madrid : Ministerio de Hacienda y Administraciones Públicas, 2012.

DIRECCIÓN GENERAL DE MODERNIZACIÓN ADMINISTRATIVA DE ESPAÑA. Magerit versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información - Libro II. Madrid : Ministerio de Hacienda y Administraciones Públicas, 2012.

GAONA VASQUEZ, Karina. Aplicación de la medología Magerit para el analisis y gestión de riesgos de seguridad de la información aplicado a la empresa pesquera e industrial Bravito S.A. en la ciudad de Machala. Cuenca, 2013. Tesis de grado (ingeniero de sistemas). Universidad Politécnica Salesiana. Facultad de ingenierias.

GARAVITO ROBLES, Hina. Análisis y gestión del riesgo de la información en los sistemas de información misionales de una entidad del estado, enfocado en un sistema de seguridad de la información. Bogotá D.C., 2015. Trabajo de grado (especialista en seguridad informática). Universidad Nacional Abierta y a Distancia. Escuela de ciencias básicas tecnología e ingeniería.

GARCIA GUEVARA, Camilo. Establecimiento del sistema de seguridad de información en sfg bajo los estándares de la norma iso 27001: 2005. Bogotá D.C., 2012. Trabajo de grado (especialista en gerencia de tecnología). Universidad EAN. Facultad de postgrados.

GARCIA BALAGUERA, Vivian y ORTIZ GONZALEZ, Jhon. Análisis de riesgos según la norma iso 27001:2013 para las aulas virtuales de la universidad santo tomás modalidad presencial. Bogotá D.C. 2017. Trabajo de grado (especialista en seguridad informatica). Universidad Nacional Abierta y a Distancia. Escuela de ciencias basicas, tecnologias e ingenierias.

GARZÓN GARCIA, Daniel; RATKOVICH GÓMEZ, Juan y VERGARA TORRES, Alejandro. Metodología de análisis de vulnerabilidades para empresas de media y pequeña escala. Bogotá D.C., 2005. Trabajo de grado (ingeniero de sistemas) Pontificia Universidad Javeriana. Facultad de ingeniería.

GUEVARA CHUMAN, Javier. Aplicación de la metodología Magerit para el análisis y gestión de riesgos en los servidores de los sistemas de gestión académica de la Universidad Nacional Pedro Ruiz Gallo. Lambayequé, 2015. Tesis de grado (ingeniero en computación e informática). Universidad Nacional Pedro Ruiz Gallo.

Facultad de ciencias físicas y matematicas. Escuela profesional de ingeniería en computación e informática.

HACKPLAYERS. Hackplayers.com: Phishing for dummies {En línea}. {09 de diciembre de 2020}. Disponible en: (https://www.hackplayers.com/2017/05/phishing-for-dummies.html#more).

HARÁN, Juan Manuel. Welivesecurity.com: BlueKeep: la vulnerabilidad que tiene en vilo a gran parte de la industria de la seguridad. {En línea}. {10 de junio de 2021}. Disponible en: (https://www.welivesecurity.com/la-es/2019/06/10/bluekeep-vulnerabilidad-tiene-vilo-industria-seguridad/).

ICONTEC. Norma técnica colombiana NTC 1486 Presentación de tesis, trabajos de grado y otros trabajos de investigación. Bogotá D.C. , 2008.

ISO27000.ES. Iso27000.es: ¿Qué es un SGSI?. {En línea}. {28 de enero de 2021}. Disponible en: (https://www.iso27000.es/sgsi.html).

JIMENEZ, Javier. Redeszone.net: Este ataque informático permite robar datos de la caché de Windows y Linux por igual. {En línea}. {10 de febrero de 2021}. Disponible en: (https://www.redeszone.net/2019/01/10/ataque-datos-cache-windows-linux).

LAGOS FLOREZ, Eduardo. Análisis de vulnerabilidades y pruebas de penetración a la infraestructura tecnologica de empresas. Mexico, 2018. Trabajo de grado (ingeniero en computación). Universidad Nacional Autonoma de Mexico. Facultad de ingeniería.

MALDONADO MARIÑO, Diana y BAÑO NARANJO, Freddy. Gestión de riesgos informáticos para la protección de los sistemas de información en la cooperativa de ahorro y credito campesina coopac. Ambato, 2013. Informe final de tesis (maestria en informática empresarial). Universidad Regional Autonoma de los Andes. Facultad de sistemas mercantiles.

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. mintic.gov.co: Modelo de Seguridad y Privacidad de la Información. - 2016. - 2020. {En línea}. {23 de enero de 2021}. Disponible en: (https://www.mintic.gov.co/gestionti/615/articles-5482_Modelo_de_Seguridad_Privacidad.pdf).

MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES. mintic.gov.co: Plan de seguridad y privacidad de la información. - 2019. - 2020. {En línea}. {23 de enero de 2021}. Disponible en: (https://www.mintic.gov.co/portal/604/articles-100251_plan_seguridad_privacidad_informacion_2019.pdf).

OLMEDO, Javier. Hackapuntes: Explotación de vulnerabilidad CVE-2011-0762. {En línea}. {19 de diciembre de 2020}. Disponible en: (https://hackpuntes.com/explotacion-de-vulnerabilidad-cve-2011-0762-con-metasploit-en-vsftpd-v2-3-4/).

OSTEC. Ostec.blog: Primeros pasos para realizar un Análisis de Vulnerabilidad en redes corporativas {En línea}. {9 de diciembre de 2020}. Disponible en: (https://ostec.blog/es/generico/primeros-pasos-para-realizar-un-analisis-de-vulnerabilidad-en-redes-corporativas/#).

REYNA REYNA, Keynes. Plan de contingencia de los activos informáticos de la facultad de ingeniería de sistemas e informática de la universidad nacional de la amazonía peruana. Iquitos, 2014. Examén de suficiencia profesional (ingeniero de sistemas). Universidad Nacional de la Amazonia Peruana. Escuela formación profesional de ingeniería de sistemas e informática.

SANCHEZ ARDILA, Felix. Plan de implementación de la ISO/IEC 27001:2013 en la fundación universitaria San Mateo. Barcelona, 2018. Trabajo de grado (master universitario en seguridad de las tecnologías de la información y la comuicación). Universidad Abierta de Catalunya.

SECPRONET. secpronet.blogspot.com: Ataque Dos con Slowloris. {En línea}. {23 de enero de 2021}. Disponible en: (https://secpronet.blogspot.com/2019/02/slowloris-ataque-dos.html).

ANEXO A

IDENTIFICACION DE AMENAZAS

No.	Nombre del activo de información	Amenazas
1	[D_NOS_BACKUP] Copias de Seguridad de la información.	[E1] Errores de los usuarios
2	[D_NOS_BACKUP] Copias de Seguridad de la información.	[E2] Errores del administrador
3	[D_NOS_SOURCE] Codigo Fuente de las aplicaciones desarrolladas.	[E20] Vulnerabilidades de los programas (software)
4	[D_NOS_SOURCE] Codigo Fuente de las aplicaciones desarrolladas.	[E21] Errores de mantenimiento / actualización de programas (software)
5	[D_NOS_SOURCE] Codigo Fuente de las aplicaciones desarrolladas.	[A5] Suplantación de la identidad del usuario
6	[D_NOS_ACL] Datos de Acceso a Servidores.	[A4] Manipulación de la configuración
7	[D_NOS_ACL] Datos de Acceso a Servidores.	[A5] Suplantación de la identidad del usuario
8	[D_NOS_ACL] Datos de Acceso a Servidores.	[A11] Acceso no autorizado
9	[D_NOS_PASS] Datos de Acceso Usuarios del Sistema.	[A5] Suplantación de la identidad del usuario
10	[D_NOS_PASS] Datos de Acceso Usuarios del Sistema.	[A11] Acceso no autorizado
11	[S_NOS_RCE] Servicio Proyectos de Capacitación y Educación.	[I5] Avería de origen físico o lógico
12	[S_NOS_RCE] Servicio Proyectos de Capacitación y Educación.	[I6] Corte del suministro eléctrico
13	[S_NOS_RCE] Servicio Proyectos de Capacitación y Educación.	[E20] Vulnerabilidades de los programas (software)
14	[S_NOS_RCE] Servicio Proyectos de Capacitación y Educación.	[E21] Errores de mantenimiento / actualización de programas (software)
15	[S_NOS_RCE] Servicio Proyectos de Capacitación y Educación.	[E23] Errores de mantenimiento / actualización de equipos (hardware)
16	[S_NOS_RCE] Servicio Proyectos de Capacitación y Educación.	[E24] Caída del sistema por agotamiento de recursos
17	[S_NOS_RCE] Servicio Proyectos de Capacitación y Educación.	[A5] Suplantación de la identidad del usuario
18	[S_NOS_RCE] Servicio Proyectos de Capacitación y Educación.	[A6] Abuso de privilegios de acceso
19	[S_NOS_RCE] Servicio Proyectos de Capacitación y Educación.	[A11] Acceso no autorizado
20	[S_NOS_CAMPUS] Servicio de Aula virtual Institucional.	[I5] Avería de origen físico o lógico
21	[S_NOS_CAMPUS] Servicio de Aula virtual Institucional.	[E8] Difusión de software dañino
22	[S_NOS_CAMPUS] Servicio de Aula virtual Institucional.	[E20] Vulnerabilidades de los programas (software)
23	[S_NOS_CAMPUS] Servicio de Aula virtual Institucional.	[E21] Errores de mantenimiento / actualización de programas (software)
24	[S_NOS_CAMPUS] Servicio de Aula virtual Institucional.	[A5] Suplantación de la identidad del usuario
25	[S_NOS_CAMPUS] Servicio de Aula virtual Institucional.	[A24] Denegación de servicio
26	[S_NOS_EMAIL] Servicio de Correo Electronico Institucional.	[I8] Fallo de servicios de comunicaciones
27	[S_NOS_EMAIL] Servicio de Correo Electronico Institucional.	[E8] Difusión de software dañino
28	[S_NOS_EMAIL] Servicio de Correo Electronico Institucional.	[A5] Suplantación de la identidad del usuario
29	[S_NOS_EMAIL] Servicio de Correo Electronico Institucional.	[A30] Ingeniería social (picaresca)
30	[S_NOS_LIBRARY] Servicio de Biblioteca Virtual.	[I8] Fallo de servicios de comunicaciones
31	[S_NOS_LIBRARY] Servicio de Biblioteca Virtual.	[A11] Acceso no autorizado

No.	Nombre del activo de información	Amenazas
32	[SW_NOS_CONT] Sofware Contable Cloud.	[I5] Avería de origen físico o lógico
33	[SW_NOS_CONT] Sofware Contable Cloud.	[E15] Alteración accidental de la información
34	[SW_NOS_CONT] Sofware Contable Cloud.	[E21] Errores de mantenimiento / actualización de programas (software)
35	[SW_NOS_CONT] Sofware Contable Cloud.	[A5] Suplantación de la identidad del usuario
36	[SW_NOS_ARCA] Plataforma tecnologica Institucional	[I5] Avería de origen físico o lógico
37	[SW_NOS_ARCA] Plataforma tecnologica Institucional	[E1] Errores de los usuarios
38	[SW_NOS_ARCA] Plataforma tecnologica Institucional	[E21] Errores de mantenimiento / actualización de programas (software)
39	[SW_NOS_ARCA] Plataforma tecnologica Institucional	[A6] Abuso de privilegios de acceso
40	[SW_NOS_ARCA] Plataforma tecnologica Institucional	[A11] Acceso no autorizado
41	[SW_NOS_WEB] Portal Web Nostradamus.	[I5] Avería de origen físico o lógico
42	[SW_NOS_WEB] Portal Web Nostradamus.	[E20] Vulnerabilidades de los programas (software)
43	[SW_NOS_WEB] Portal Web Nostradamus.	[E21] Errores de mantenimiento / actualización de programas (software)
44	[SW_NOS_WEB] Portal Web Nostradamus.	[A5] Suplantación de la identidad del usuario
45	[SW_NOS_WEB] Portal Web Nostradamus.	[A24] Denegación de servicio
46	[SW_NOS_DEV] Paquete de Entorno de Desarrollo.	[E21] Errores de mantenimiento / actualización de programas (software)
47	[SW_NOS_OS] Sistemas Operativos.	[E1] Errores de los usuarios
48	[SW_NOS_OS] Sistemas Operativos.	[E8] Difusión de software dañino
49	[SW_NOS_OS] Sistemas Operativos.	[E20] Vulnerabilidades de los programas (software)
50	[SW_NOS_OS] Sistemas Operativos.	[E21] Errores de mantenimiento / actualización de programas (software)
51	[SW_NOS_OFFICE] Aplicaciones Ofiimatica.	[E1] Errores de los usuarios
52	[SW_NOS_OFFICE] Aplicaciones Ofiimatica.	[E20] Vulnerabilidades de los programas (software)
53	[SW_NOS_OFFICE] Aplicaciones Ofiimatica.	[E21] Errores de mantenimiento / actualización de programas (software)
54	[SW_NOS_SMAIL] Cliente de Correo Electronico.	[I8] Fallo de servicios de comunicaciones
55	[SW_NOS_SMAIL] Cliente de Correo Electronico.	[A5] Suplantación de la identidad del usuario
56	[SW_NOS_AV] Software Antivirus.	[E8] Difusión de software dañino
57	[SW_NOS_AV] Software Antivirus.	[E20] Vulnerabilidades de los programas (software)
58	[SW_NOS_AV] Software Antivirus.	[E21] Errores de mantenimiento / actualización de programas (software)
59	[HW_NOS_SRI] Dell Torre PowerEdge T440.	[I5] Avería de origen físico o lógico
60	[HW_NOS_SRI] Dell Torre PowerEdge T440.	[E2] Errores del administrador
61	[HW_NOS_SRI] Dell Torre PowerEdge T440.	[E21] Errores de mantenimiento / actualización de programas (software)
62	[HW_NOS_SRI] Dell Torre PowerEdge T440.	[I7] Condiciones inadecuadas de temperatura o humedad

No.	Nombre del activo de información	Amenazas
63	[HW_NOS_SRI] Dell Torre PowerEdge T440.	[A11] Acceso no autorizado
64	[HW_NOS_SRFTP] Dell Torre PowerEdge T130.	[I1] Fuego
65	[HW_NOS_SRFTP] Dell Torre PowerEdge T130.	[I8] Fallo de servicios de comunicaciones
66	[HW_NOS_SRFTP] Dell Torre PowerEdge T130.	[E8] Difusión de software dañino
67	[HW_NOS_SRFTP] Dell Torre PowerEdge T130.	[A4] Manipulación de la configuración
68	[HW_NOS_SRFTP] Dell Torre PowerEdge T130.	[A5] Suplantación de la identidad del usuario
69	[HW_NOS_SRCA] Dell Torre PowerEdge T440	[N1] Fuego
70	[HW_NOS_SRCA] Dell Torre PowerEdge T440	[N2] Daños por agua
71	[HW_NOS_SRCA] Dell Torre PowerEdge T440	[I*] Desastres industriales
72	[HW_NOS_SRCA] Dell Torre PowerEdge T440	[E2] Errores del administrador
73	[HW_NOS_SRCA] Dell Torre PowerEdge T440	[E21] Errores de mantenimiento / actualización de programas (software)
74	[HW_NOS_SRCA] Dell Torre PowerEdge T440	[I7] Condiciones inadecuadas de temperatura o humedad
75	[HW_NOS_SRCA] Dell Torre PowerEdge T440	[E24] Caída del sistema por agotamiento de recursos
76	[HW_NOS_SRCA] Dell Torre PowerEdge T440	[A6] Abuso de privilegios de acceso
77	[HW_NOS_SRCA] Dell Torre PowerEdge T440	[A11] Acceso no autorizado
78	[HW_NOS_SRDHCP] Dell Torre PowerEdge T440	[I5] Avería de origen físico o lógico
79	[HW_NOS_SRDHCP] Dell Torre PowerEdge T440	[E2] Errores del administrador
80	[HW_NOS_SRDHCP] Dell Torre PowerEdge T440	[E21] Errores de mantenimiento / actualización de programas (software)
81	[HW_NOS_SRDHCP] Dell Torre PowerEdge T440	[I7] Condiciones inadecuadas de temperatura o humedad
82	[HW_NOS_SRDHCP] Dell Torre PowerEdge T440	[A11] Acceso no autorizado
83	[HW_NOS_PC] Equipos de Computo.	[I1] Fuego
84	[HW_NOS_PC] Equipos de Computo.	[I2] Daños por agua
85	[HW_NOS_PC] Equipos de Computo.	[I*] Desastres industriales
86	[HW_NOS_PC] Equipos de Computo.	[I5] Avería de origen físico o lógico
87	[HW_NOS_PRINT1] Impresora HP LaserJet Enterprise serie 600	[I1] Fuego
88	[HW_NOS_PRINT1] Impresora HP LaserJet Enterprise serie 600	[I2] Daños por agua
89	[HW_NOS_PRINT1] Impresora HP LaserJet Enterprise serie 600	[I*] Desastres industriales
90	[HW_NOS_PRINT1] Impresora HP LaserJet Enterprise serie 600	[I5] Avería de origen físico o lógico
91	[HW_NOS_PRINT2] Impresora SMART MultiXpress M4370LX.	[I1] Fuego
92	[HW_NOS_PRINT2] Impresora SMART MultiXpress M4370LX.	[I2] Daños por agua
93	[HW_NOS_PRINT2] Impresora SMART MultiXpress M4370LX.	[I*] Desastres industriales

No.	Nombre del activo de información	Amenazas
94	[HW_NOS_PRINT2] Impresora SMART MultiXpress M4370LX.	[I5] Avería de origen físico o lógico
95	[HW_NOS_FIREWALL] Cortafuegos Cisco ASA 5505	[I1] Fuego
96	[HW_NOS_FIREWALL] Cortafuegos Cisco ASA 5505	[I2] Daños por agua
97	[HW_NOS_FIREWALL] Cortafuegos Cisco ASA 5505	[I*] Desastres industriales
98	[HW_NOS_FIREWALL] Cortafuegos Cisco ASA 5505	[I5] Avería de origen físico o lógico
99	[HW_NOS_FIREWALL] Cortafuegos Cisco ASA 5505	[E4] Errores de configuración
100	[HW_NOS_SWITCH] Switches Cisco Catalyst 2960	[I1] Fuego
101	[HW_NOS_SWITCH] Switches Cisco Catalyst 2960	[I2] Daños por agua
102	[HW_NOS_SWITCH] Switches Cisco Catalyst 2960	[I*] Desastres industriales
103	[HW_NOS_SWITCH] Switches Cisco Catalyst 2960	[I5] Avería de origen físico o lógico
104	[HW_NOS_SWITCH] Switches Cisco Catalyst 2960	[E4] Errores de configuración
105	[HW_NOS_SWITCH] Switches Cisco Catalyst 2960	[A4] Manipulación de la configuración
106	[HW_NOS_SWITCH] Switches Cisco Catalyst 2960	[A11] Acceso no autorizado
107	[HW_NOS_HUB] Puntos de acceso alámbricos	[I1] Fuego
108	[HW_NOS_HUB] Puntos de acceso alámbricos	[I2] Daños por agua
109	[HW_NOS_HUB] Puntos de acceso alámbricos	[I*] Desastres industriales
110	[HW_NOS_HUB] Puntos de acceso alámbricos	[I5] Avería de origen físico o lógico
111	[HW_NOS_HUB] Puntos de acceso alámbricos	[E4] Errores de configuración
112	[HW_NOS_WAP] Puntos de acceso inalámbricos.	[I1] Fuego
113	[HW_NOS_WAP] Puntos de acceso inalámbricos.	[I2] Daños por agua
114	[HW_NOS_WAP] Puntos de acceso inalámbricos.	[I*] Desastres industriales
115	[HW_NOS_WAP] Puntos de acceso inalámbricos.	[I5] Avería de origen físico o lógico
116	[HW_NOS_WAP] Puntos de acceso inalámbricos.	[E4] Errores de configuración
117	[HW_NOS_TELIP] Telefonos IP	[I1] Fuego
118	[HW_NOS_TELIP] Telefonos IP	[I2] Daños por agua
119	[HW_NOS_TELIP] Telefonos IP	[I*] Desastres industriales
120	[HW_NOS_TELIP] Telefonos IP	[I5] Avería de origen físico o lógico
121	[COM_NOS_INTERNET] Canal de Internet Dedicado.	[I8] Fallo de servicios de comunicaciones
122	[COM_NOS_LAN] Red Local Institucional.	[I1] Fuego
123	[COM_NOS_LAN] Red Local Institucional.	[I2] Daños por agua
124	[COM_NOS_LAN] Red Local Institucional.	[I8] Fallo de servicios de comunicaciones

No.	Nombre del activo de información	Amenazas
125	[COM_NOS_LAN] Red Local Institucional.	[A11] Acceso no autorizado
126	[COM_NOS_LAN] Red Local Institucional.	[A12] Análisis de tráfico
127	[COM_NOS_WLAN] Red Wifi Institucional.	[I5] Avería de origen físico o lógico
128	[COM_NOS_WLAN] Red Wifi Institucional.	[I8] Fallo de servicios de comunicaciones
129	[COM_NOS_WLAN] Red Wifi Institucional.	[E9] Errores de [re-]encaminamiento
130	[COM_NOS_WLAN] Red Wifi Institucional.	[A11] Acceso no autorizado
131	[COM_NOS_WLAN] Red Wifi Institucional.	[A12] Análisis de tráfico
132	[COM_NOS_TEL] Red Telefonica.	[I8] Fallo de servicios de comunicaciones
133	[COM_NOS_TEL] Red Telefonica.	[E9] Errores de [re-]encaminamiento
134	[COM_NOS_TEL] Red Telefonica.	[A14] Interceptación de información (escucha)
135	[AUX_NOS_POWER] Sistema Electrico.	[N*] Desastres naturales
136	[AUX_NOS_POWER] Sistema Electrico.	[I1] Fuego
137	[AUX_NOS_POWER] Sistema Electrico.	[I2] Daños por agua
138	[AUX_NOS_POWER] Sistema Electrico.	[I*] Desastres industriales
139	[AUX_NOS_POWER] Sistema Electrico.	[I4] Contaminación electromagnética
140	[AUX_NOS_CE] Cableado Estructurado.	[I1] Fuego
141	[AUX_NOS_CE] Cableado Estructurado.	[I2] Daños por agua
142	[AUX_NOS_CE] Cableado Estructurado.	[I*] Desastres industriales
143	[AUX_NOS_CE] Cableado Estructurado.	[I4] Contaminación electromagnética
144	[AUX_NOS_UPS] Sistema Alimentacion sin Interrupciones.	[I*] Desastres industriales
145	[AUX_NOS_UPS] Sistema Alimentacion sin Interrupciones.	[I4] Contaminación electromagnética
146	[L_NOS_DEP] Area de la Dirección de TI.	[N1] Fuego
147	[L_NOS_DEP] Area de la Dirección de TI.	[N2] Daños por agua
148	[L_NOS_DEP] Area de la Dirección de TI.	[N*] Desastres naturales
149	[L_NOS_DEP] Area de la Dirección de TI.	[I*] Desastres industriales
150	[L_NOS_DEP] Area de la Dirección de TI.	[A27] Ocupación enemiga
151	[P_NOS_TECM] Tecnicos de Mantenimiento a Equipos de Computo.	[E28] Indisponibilidad del personal
152	[P_NOS_TECM] Tecnicos de Mantenimiento a Equipos de Computo.	[A6] Abuso de privilegios de acceso
153	[P_NOS_TECM] Tecnicos de Mantenimiento a Equipos de Computo.	[A18] Destrucción de información
154	[P_NOS_TECM] Tecnicos de Mantenimiento a Equipos de Computo.	[A23] Manipulación de los equipos

ANEXO B

VALORACION DE AMENAZAS

No.	Nombre del activo de información	Amenazas Metodologia Magerit	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Probabilidad de vulneración
1	[D_NOS_BACKUP] Copias de Seguridad de la información.	[E1] Errores de los usuarios	B	B	MA	A	A	3
2	[D_NOS_BACKUP] Copias de Seguridad de la información.	[E2] Errores del administrador	B	B	MA	A	A	3
3	[D_NOS_SOURCE] Codigo Fuente de las aplicaciones desarrolladas.	[E20] Vulnerabilidades de los programas (software)	B	B	B	A	A	3
4	[D_NOS_SOURCE] Codigo Fuente de las aplicaciones desarrolladas.	[E21] Errores de mantenimiento / actualización de programas (software)	B	B	B	A	A	3
5	[D_NOS_SOURCE] Codigo Fuente de las aplicaciones desarrolladas.	[A5] Suplantación de la identidad del usuario	B	B	B	A	A	3
6	[D_NOS_ACL] Datos de Acceso a Servidores.	[A4] Manipulación de la configuración	A	B	A	A	A	4
7	[D_NOS_ACL] Datos de Acceso a Servidores.	[A5] Suplantación de la identidad del usuario	A	B	A	A	A	4
8	[D_NOS_ACL] Datos de Acceso a Servidores.	[A11] Acceso no autorizado	A	B	A	A	A	4
9	[D_NOS_PASS] Datos de Acceso Usuarios del Sistema.	[A5] Suplantación de la identidad del usuario	B	B	MA	A	A	4
10	[D_NOS_PASS] Datos de Acceso Usuarios del Sistema.	[A11] Acceso no autorizado	B	B	MA	A	A	4
11	[S_NOS_RCE] Servicio Proyectos de Capacitación y Educación.	[I5] Avería de origen físico o lógico	A	A	A	A	A	4
12	[S_NOS_RCE] Servicio Proyectos de Capacitación y Educación.	[I6] Corte del suministro eléctrico	A	A	A	A	A	4
14	[S_NOS_RCE] Servicio Proyectos de Capacitación y Educación.	[E21] Errores de mantenimiento / actualización de programas (software)	A	A	A	A	A	4
15	[S_NOS_RCE] Servicio Proyectos de Capacitación y Educación.	[E23] Errores de mantenimiento / actualización de equipos (hardware)	A	A	A	A	A	4
16	[S_NOS_RCE] Servicio Proyectos de Capacitación y Educación.	[E24] Caída del sistema por agotamiento de recursos	A	A	A	A	A	4
17	[S_NOS_RCE] Servicio Proyectos de Capacitación y Educación.	[A5] Suplantación de la identidad del usuario	A	A	A	A	A	4
18	[S_NOS_RCE] Servicio Proyectos de Capacitación y Educación.	[A6] Abuso de privilegios de acceso	A	A	A	A	A	3
19	[S_NOS_RCE] Servicio Proyectos de Capacitación y Educación.	[A11] Acceso no autorizado	A	A	A	A	A	3
20	[S_NOS_CAMPUS] Servicio de Aula virtual Institucional.	[I5] Avería de origen físico o lógico	A	A	A	A	A	3
21	[S_NOS_CAMPUS] Servicio de Aula virtual Institucional.	[E8] Difusión de software dañino	A	A	A	A	A	2
22	[S_NOS_CAMPUS] Servicio de Aula virtual Institucional.	[E20] Vulnerabilidades de los programas (software)	A	A	A	A	A	4
23	[S_NOS_CAMPUS] Servicio de Aula virtual Institucional.	[E21] Errores de mantenimiento / actualización de programas (software)	A	A	A	A	A	4
24	[S_NOS_CAMPUS] Servicio de Aula virtual Institucional.	[A5] Suplantación de la identidad del usuario	A	A	A	A	A	3
25	[S_NOS_CAMPUS] Servicio de Aula virtual Institucional.	[A24] Denegación de servicio	A	A	A	A	A	3
26	[S_NOS_EMAIL] Servicio de Correo Electronico Institucional.	[I8] Fallo de servicios de comunicaciones	A	A	A	A	A	3
27	[S_NOS_EMAIL] Servicio de Correo Electronico Institucional.	[E8] Difusión de software dañino	A	A	A	A	A	3
28	[S_NOS_EMAIL] Servicio de Correo Electronico Institucional.	[A5] Suplantación de la identidad del usuario	A	A	A	A	A	3
29	[S_NOS_EMAIL] Servicio de Correo Electronico Institucional.	[A30] Ingeniería social (picaresca)	A	A	A	A	A	3
32	[SW_NOS_CONT] Sofware Contable Cloud.	[I5] Avería de origen físico o lógico	A	A	A	A	A	4
33	[SW_NOS_CONT] Sofware Contable Cloud.	[E15] Alteración accidental de la información	A	A	A	A	A	4
34	[SW_NOS_CONT] Sofware Contable Cloud.	[E21] Errores de mantenimiento / actualización de programas (software)	A	A	A	A	A	4
35	[SW_NOS_CONT] Sofware Contable Cloud.	[A5] Suplantación de la identidad del usuario	A	A	A	A	A	4

No.	Nombre del activo de información	Amenazas Metodologia Magerit	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Probabilidad de vulneración
36	[SW_NOS_ARCA] Plataforma tecnologica Institucional	[I5] Avería de origen físico o lógico	A	A	A	A	A	4
37	[SW_NOS_ARCA] Plataforma tecnologica Institucional	[E1] Errores de los usuarios	A	A	A	A	A	3
38	[SW_NOS_ARCA] Plataforma tecnologica Institucional	[E21] Errores de mantenimiento / actualización de programas (software)	A	A	A	A	A	3
39	[SW_NOS_ARCA] Plataforma tecnologica Institucional	[A6] Abuso de privilegios de acceso	A	A	A	A	A	3
40	[SW_NOS_ARCA] Plataforma tecnologica Institucional	[A11] Acceso no autorizado	A	A	A	A	A	4
41	[SW_NOS_WEB] Portal Web Nostradamus.	[I5] Avería de origen físico o lógico	A	A	A	A	A	4
42	[SW_NOS_WEB] Portal Web Nostradamus.	[E20] Vulnerabilidades de los programas (software)	A	A	A	A	A	4
43	[SW_NOS_WEB] Portal Web Nostradamus.	[E21] Errores de mantenimiento / actualización de programas (software)	A	A	A	A	A	4
44	[SW_NOS_WEB] Portal Web Nostradamus.	[A5] Suplantación de la identidad del usuario	A	A	A	A	A	4
45	[SW_NOS_WEB] Portal Web Nostradamus.	[A24] Denegación de servicio	A	A	A	A	A	4
47	[SW_NOS_OS] Sistemas Operativos.	[E1] Errores de los usuarios	A	A	A	A	A	3
48	[SW_NOS_OS] Sistemas Operativos.	[E8] Difusión de software dañino	A	A	A	A	A	3
49	[SW_NOS_OS] Sistemas Operativos.	[E20] Vulnerabilidades de los programas (software)	A	A	A	A	A	3
50	[SW_NOS_OS] Sistemas Operativos.	[E21] Errores de mantenimiento / actualización de programas (software)	A	A	A	A	A	3
51	[SW_NOS_OFFICE] Aplicaciones Ofiimatica.	[E1] Errores de los usuarios	A	A	A	A	A	3
52	[SW_NOS_OFFICE] Aplicaciones Ofiimatica.	[E20] Vulnerabilidades de los programas (software)	A	A	A	A	A	3
53	[SW_NOS_OFFICE] Aplicaciones Ofiimatica.	[E21] Errores de mantenimiento / actualización de programas (software)	A	A	A	A	A	3
59	[HW_NOS_SRI] Dell Torre PowerEdge T440.	[I5] Avería de origen físico o lógico	M	M	M	M	M	4
60	[HW_NOS_SRI] Dell Torre PowerEdge T440.	[E2] Errores del administrador	M	M	M	M	M	3
61	[HW_NOS_SRI] Dell Torre PowerEdge T440.	[E21] Errores de mantenimiento / actualización de programas (software)	M	M	M	M	M	3
62	[HW_NOS_SRI] Dell Torre PowerEdge T440.	[I7] Condiciones inadecuadas de temperatura o humedad	M	M	M	M	M	3
63	[HW_NOS_SRI] Dell Torre PowerEdge T440.	[A11] Acceso no autorizado	M	M	M	M	M	4
64	[HW_NOS_SRFTP] Dell Torre PowerEdge T130.	[I1] Fuego	M	M	M	M	M	2
65	[HW_NOS_SRFTP] Dell Torre PowerEdge T130.	[I8] Fallo de servicios de comunicaciones	M	M	M	M	M	3
66	[HW_NOS_SRFTP] Dell Torre PowerEdge T130.	[E8] Difusión de software dañino	M	M	M	M	M	3
67	[HW_NOS_SRFTP] Dell Torre PowerEdge T130.	[A4] Manipulación de la configuración	M	M	M	M	M	3
68	[HW_NOS_SRFTP] Dell Torre PowerEdge T130.	[A5] Suplantación de la identidad del usuario	M	M	M	M	M	3
69	[HW_NOS_SRCA] Dell Torre PowerEdge T440	[N1] Fuego	A	B	A	A	A	3
70	[HW_NOS_SRCA] Dell Torre PowerEdge T440	[N2] Daños por agua	A	B	A	A	A	3
71	[HW_NOS_SRCA] Dell Torre PowerEdge T440	[I*] Desastres industriales	A	B	A	A	A	3
72	[HW_NOS_SRCA] Dell Torre PowerEdge T440	[E2] Errores del administrador	A	B	A	A	A	3
73	[HW_NOS_SRCA] Dell Torre PowerEdge T440	[E21] Errores de mantenimiento / actualización de programas (software)	A	B	A	A	A	3
74	[HW_NOS_SRCA] Dell Torre PowerEdge T440	[I7] Condiciones inadecuadas de temperatura o humedad	A	B	A	A	A	3
75	[HW_NOS_SRCA] Dell Torre PowerEdge T440	[E24] Caída del sistema por agotamiento de recursos	A	B	A	A	A	3
76	[HW_NOS_SRCA] Dell Torre PowerEdge T440	[A6] Abuso de privilegios de acceso	A	B	A	A	A	3
77	[HW_NOS_SRCA] Dell Torre PowerEdge T440	[A11] Acceso no autorizado	A	B	A	A	A	4
78	[HW_NOS_SRDHCP] Dell Torre PowerEdge T440	[I5] Avería de origen físico o lógico	A	A	A	A	A	3
79	[HW_NOS_SRDHCP] Dell Torre PowerEdge T440	[E2] Errores del administrador	A	A	A	A	A	3
80	[HW_NOS_SRDHCP] Dell Torre PowerEdge T440	[E21] Errores de mantenimiento / actualización de programas (software)	A	A	A	A	A	3
81	[HW_NOS_SRDHCP] Dell Torre PowerEdge T440	[I7] Condiciones inadecuadas de temperatura o humedad	A	A	A	A	A	3
82	[HW_NOS_SRDHCP] Dell Torre PowerEdge T440	[A11] Acceso no autorizado	A	A	A	A	A	4
86	[HW_NOS_PC] Equipos de Computo.	[I5] Avería de origen físico o lógico	A	B	A	A	A	3
98	[HW_NOS_FIREWALL] Cortafuegos Cisco ASA 5505	[I5] Avería de origen físico o lógico	A	B	A	A	A	3
99	[HW_NOS_FIREWALL] Cortafuegos Cisco ASA 5505	[E4] Errores de configuración	A	B	A	A	A	4

No.	Nombre del activo de información	Amenazas Metodologia Magerit	Autenticidad	Trazabilidad	Confidencialidad	Integridad	Disponibilidad	Probabilidad de vulneración
103	[HW_NOS_SWITCH] Switches Cisco Catalyst 2960	[I5] Avería de origen físico o lógico	M	M	M	M	M	3
106	[HW_NOS_SWITCH] Switches Cisco Catalyst 2960	[A11] Acceso no autorizado	M	M	M	M	M	4
110	[HW_NOS_HUB] Puntos de acceso alámbricos	[I5] Avería de origen físico o lógico	A	B	A	A	A	3
115	[HW_NOS_WAP] Puntos de acceso inalámbricos.	[I5] Avería de origen físico o lógico	M	M	M	M	M	3
116	[HW_NOS_WAP] Puntos de acceso inalámbricos.	[E4] Errores de configuración	M	M	M	M	M	3
121	[COM_NOS_INTERNET] Canal de Internet Dedicado.	[I8] Fallo de servicios de comunicaciones	M	M	M	M	M	4
124	[COM_NOS_LAN] Red Local Institucional.	[I8] Fallo de servicios de comunicaciones	M	M	M	M	M	4
125	[COM_NOS_LAN] Red Local Institucional.	[A11] Acceso no autorizado	M	M	M	M	M	4
126	[COM_NOS_LAN] Red Local Institucional.	[A12] Análisis de tráfico	M	M	M	M	M	2
127	[COM_NOS_WLAN] Red Wifi Institucional.	[I5] Avería de origen físico o lógico	M	M	M	M	M	3
128	[COM_NOS_WLAN] Red Wifi Institucional.	[I8] Fallo de servicios de comunicaciones	M	M	M	M	M	3
130	[COM_NOS_WLAN] Red Wifi Institucional.	[A11] Acceso no autorizado	M	M	M	M	M	4
132	[COM_NOS_TEL] Red Telefonica.	[I8] Fallo de servicios de comunicaciones	M	M	M	M	M	2
138	[AUX_NOS_POWER] Sistema Electrico.	[I*] Desastres industriales	M	M	M	MA	MA	1
139	[AUX_NOS_POWER] Sistema Electrico.	[I4] Contaminación electromagnética	M	M	M	MA	MA	1
151	[P_NOS_TECM] Tecnicos de Mantenimiento a Equipos de Computo.	[E28] Indisponibilidad del personal	A	A	A	A	A	4
152	[P_NOS_TECM] Tecnicos de Mantenimiento a Equipos de Computo.	[A6] Abuso de privilegios de acceso	A	A	A	A	A	3
154	[P_NOS_TECM] Tecnicos de Mantenimiento a Equipos de Computo.	[A23] Manipulación de los equipos	A	A	A	A	A	3

ANEXO C

MAPA DE CALOR DE LOS HALLAZGOS

APETITO POR EL RIESGO Y ZONAS DE ADMISIBILIDAD						
		IMPACTO				
		Insignificante	Menor	Moderado	Mayor	Catastrófico
IMPACTO	MUY ALTA		, R64, R21	, R154, R152, R128, R127, R116, R115, R110, R103, R98, R86, R81, R80, R79, R78, R76, R75, R74, R73, R72, R71, R70, R69, R68, R67, R66, R65, R62, R61, R60, R53, R52, R51, R50, R49, R48, R47, R39, R38, R37, R29, R28, R27, R26, R25, R24, R20, R19, R18, R5, R4, R3, R2, R1	, R151, R130, R125, R124, R121, R106, R99, R82, R77, R63, R59, R45, R44, R43, R42, R41, R40, R36, R35, R34, R33, R32, R23, R22, R17, R16, R15, R14, R13, R12, R11, R10, R9, R8, R7, R6	
	ALTA					
	MEDIA					
	BAJA					
	MUY BAJA					
RIESGO		MUY BAJA	BAJA	MEDIA	ALTA	MUY ALTA
		PROBABILIDAD				

ANEXO D

INFORME ESCANEO DE VULNERABILIDADES EN NOSTRADAMUS S.A.S

Vulnerabilities Total: 52

SEVERITY	CVSS	PLUGIN	NAME
MEDIUM	6.4	51192	SSL Certificate Cannot Be Trusted
MEDIUM	6.4	57582	SSL Self-Signed Certificate
MEDIUM	6.1	104743	TLS Version 1.0 Protocol Detection
MEDIUM	5.0	11213	HTTP TRACE / TRACK Methods Allowed
MEDIUM	5.0	140532	PHP 7.2.x / 7.3.x < 7.3.22 Memory Leak Vulnerability
MEDIUM	5.0	142591	PHP < 7.3.24 Multiple Vulnerabilities
MEDIUM	5.0	57608	SMB Signing not required
MEDIUM	5.0	15901	SSL Certificate Expiry
MEDIUM	5.0	35291	SSL Certificate Signed Using Weak Hashing Algorithm
MEDIUM	5.0	45411	SSL Certificate with Wrong Hostname
MEDIUM	5.0	42873	SSL Medium Strength Cipher Suites Supported (SWEET32)
MEDIUM	5.0	12218	mDNS Detection (Remote Network)
MEDIUM	4.3	144047	OpenSSL 1.1.1 < 1.1.1i Null Pointer Dereference Vulnerability
LOW	2.6	83875	SSL/TLS Diffie-Hellman Modulus <= 1024 Bits (Logjam)
INFO	N/A	48204	Apache HTTP Server Version
INFO	N/A	45590	Common Platform Enumeration (CPE)

INFO	N/A	10736	DCE Services Enumeration
INFO	N/A	54615	Device Type
INFO	N/A	35716	Ethernet Card Manufacturer Detection
INFO	N/A	86420	Ethernet MAC Addresses
INFO	N/A	84502	HSTS Missing From HTTPS Server
INFO	N/A	10107	HTTP Server Type and Version
INFO	N/A	24260	HyperText Transfer Protocol (HTTP) Information
INFO	N/A	117886	Local Checks Not Enabled (info)
INFO	N/A	11011	Microsoft Windows SMB Service Detection
INFO	N/A	100871	Microsoft Windows SMB Versions Supported (remote check)
INFO	N/A	106716	Microsoft Windows SMB2 and SMB3 Dialects Supported (remote check)
INFO	N/A	11219	Nessus SYN scanner
INFO	N/A	19506	Nessus Scan Information
INFO	N/A	43815	NetBIOS Multiple IP Address Enumeration
INFO	N/A	11936	OS Identification
INFO	N/A	50845	OpenSSL Detection
INFO	N/A	57323	OpenSSL Version Detection
INFO	N/A	48243	PHP Version Detection
INFO	N/A	66334	Patch Report
INFO	N/A	56984	SSL / TLS Versions Supported
INFO	N/A	45410	SSL Certificate 'commonName' Mismatch
INFO	N/A	10863	SSL Certificate Information
INFO	N/A	70544	SSL Cipher Block Chaining Cipher Suites Supported

INFO	N/A	136318	TLS Version 1.2 Protocol Detection
INFO	N/A	138330	TLS Version 1.3 Protocol Detection
INFO	N/A	110723	Target Credential Status by Authentication Protocol - No Credentials Provided
INFO	N/A	64814	Terminal Services Use SSL/TLS
INFO	N/A	10287	Traceroute Information
INFO	N/A	135860	WMI Not Available
INFO	N/A	10150	Windows NetBIOS / SMB Remote Host Information Disclosure
INFO	N/A	10940	Windows Terminal Services Enabled
INFO	N/A	21643	SSL Cipher Suites Supported
INFO	N/A	57041	SSL Perfect Forward Secrecy Cipher Suites Supported
INFO	N/A	22964	Service Detection
INFO	N/A	84821	TLS ALPN Supported Protocol Enumeration
INFO	N/A	121010	TLS Version 1.1 Protocol Detection

Descripción de las vulnerabilidades halladas con mayor relevancia.

51192 - No se puede confiar en el certificado SSL

MEDIO ID de complemento de Nessus 51192

Sinopsis

No se puede confiar en el certificado SSL para este servicio.

Descripción

No se puede confiar en el certificado X.509 del servidor. Esta situación puede ocurrir de tres formas diferentes, en las que se puede romper la cadena de confianza, como se indica a continuación:

- Primero, la parte superior de la cadena de certificados enviados por el servidor podría no ser descendiente de una autoridad de certificación pública conocida. Esto puede ocurrir cuando la parte superior de la cadena es un certificado autofirmado no reconocido, o cuando faltan certificados intermedios que conectarían la parte superior de la cadena de certificados con una autoridad de certificación pública conocida.
- En segundo lugar, la cadena de certificados puede contener un certificado que no es válido en el momento del escaneo. Esto puede ocurrir cuando el escaneo ocurre antes de una de las fechas 'notBefore' del certificado o después de una de las fechas 'notAfter' del certificado.
- En tercer lugar, la cadena de certificados puede contener una firma que no coincide con la información del certificado o que no se puede verificar. Las firmas incorrectas se pueden solucionar haciendo que el emisor vuelva a firmar el certificado con la firma incorrecta. Las firmas que no se pudieron verificar son el resultado de que el emisor del certificado utiliza un algoritmo de firma que Nessus no admite o no reconoce.
Si el host remoto es un host público en producción, cualquier ruptura en la cadena hace que sea más difícil para los usuarios verificar la autenticidad e identidad del servidor web. Esto podría facilitar la realización de ataques man-in-the-middle contra el host remoto.

Solución
Compre o genere un certificado SSL adecuado para este servicio.

Ver también
https://www.itu.int/rec/T-REC-X.509/en
https://en.wikipedia.org/wiki/X.509
Detalles del complemento
Severidad : media
ID : 51192
Nombre de archivo : ssl_signed_certificate.nasl
Versión : 1.19
Tipo : remoto
Familia : General
Publicado : 15/12/2010
Actualizado : 2020/04/27
Dependencias : 57571
Información de riesgo
Factor de riesgo : medio
CVSS v2.0
Puntuación base : 6,4
Vector : CVSS2 # AV: N / AC: L / Au: N / C: P / I: P / A: N
CVSS v3.0
Puntaje base : 6.5
Vector : CVSS: 3.0 / AV: N / AC: L / PR: N / UI: N / S: U / C: L / I: L / A: N
Información de vulnerabilidad
Elementos de KB obligatorios : SSL / BrokenCAChain

57582 - Certificado SSL autofirmado

MEDIO ID de complemento de Nessus 57582

Sinopsis

La cadena de certificados SSL para este servicio termina en un certificado autofirmado no reconocido.

Descripción

La cadena de certificados X.509 para este servicio no está firmada por una autoridad certificadora reconocida. Si el host remoto es un host público en producción, esto anula el uso de SSL, ya que cualquiera podría establecer un ataque man-in-the-middle contra el host remoto.

Tenga en cuenta que este complemento no comprueba las cadenas de certificados que terminan en un certificado que no está autofirmado, pero está firmado por una autoridad de certificación no reconocida.

Solución

Compre o genere un certificado SSL adecuado para este servicio.

Detalles del complemento

Severidad : media

ID : 57582

Nombre de archivo : ssl_self_signed_certificate.nasl

Versión : 1.5

Tipo : remoto

Familia : General

Publicado : 17/01/2012

Actualizado : 2020/04/27

Dependencias : 57571

Información de riesgo

Factor de riesgo : medio

CVSS v2.0

Puntuación base : 6,4

Vector : CVSS2 # AV: N / AC: L / Au: N / C: P / I: P / A: N

Información de vulnerabilidad

Elementos de KB obligatorios : SSL / Cadena / Autofirmado

104743 - Detección de protocolo TLS versión 1.0

MEDIO ID de complemento de Nessus 104743

Sinopsis

El servicio remoto cifra el tráfico con una versión anterior de TLS.

Descripción

El servicio remoto acepta conexiones cifradas mediante TLS 1.0. TLS 1.0 tiene una serie de 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 contra estos defectos y deben usarse siempre que sea posible.
A partir del 31 de marzo de 2020, los puntos finales que no estén habilitados para TLS 1.2 y superior ya no funcionarán correctamente con los principales navegadores web y los principales proveedores. PCI DSS v3.2 requiere que TLS 1.0 se desactive por completo antes del 30 de junio de 2018, excepto para los terminales POS POI (y los puntos de terminación SSL / TLS a los que se conectan) que pueden verificarse como no susceptibles a exploits conocidos.
Solución
Habilite la compatibilidad con TLS 1.2 y 1.3 y desactive la compatibilidad con TLS 1.0.
Ver también
https://tools.ietf.org/html/draft-ietf-tls-oldversions-deprecate-00
Detalles del complemento
Severidad : media
ID : 104743
Nombre de archivo : tls10_detection.nasl
Versión : 1.9
Tipo : remoto
Familia : detección de servicios
Publicado : 22/11/2017
Actualizado : 2020/03/31
Dependencias : 21643
Inventario de activos : verdadero
Información de riesgo
Factor de riesgo : medio
Fuente de puntuación CVSS : manual
Justificación del puntaje CVSS : puntaje de un análisis más profundo realizado por tenable
CVSS v2.0
Puntuación base : 6.1
Vector : CVSS2 # AV: N / AC: H / Au: N / C: C / I: P / A: N
CVSS v3.0
Puntaje base : 6.5
Vector : CVSS: 3.0 / AV: N / AC: H / PR: N / UI: N / S: U / C: H / I: L / A: N
Información de vulnerabilidad
Elementos de KB obligatorios : SSL / compatible

11213 - Métodos HTTP TRACE / TRACK permitidos

MEDIO ID de complemento de Nessus 11213

¡Nuevo! Clasificación de prioridad de vulnerabilidad (VPR)
Tenable calcula un VPR dinámico para cada vulnerabilidad. VPR combina información sobre vulnerabilidades con inteligencia de amenazas y algoritmos de aprendizaje automático para

predecir qué vulnerabilidades tienen más probabilidades de ser explotadas en ataques. Lea más sobre qué es VPR y en qué se diferencia de CVSS.

Puntuación VPR: 4.8

Sinopsis

Las funciones de depuración están habilitadas en el servidor web remoto.

Descripción

El servidor web remoto admite los métodos TRACE y / o TRACK. TRACE y TRACK son métodos HTTP que se utilizan para depurar conexiones de servidor web.

Solución

Desactive estos métodos HTTP. Consulte la salida del complemento para obtener más información.

Ver también

https://www.cgisecurity.com/whitehat-mirror/WH-WhitePaper_XST_ebook.pdf
http://www.apacheweek.com/issues/03-01-24
https://download.oracle.com/sunalerts/1000718.1.html

Detalles del complemento

Severidad : media
ID : 11213
Nombre de archivo : xst_http_trace.nasl
Versión : 1.73
Tipo : remoto
Familia : servidores web
Publicado : 2003/01/23
Actualizado : 2020/06/12
Dependencias : 10107

Información de riesgo

Factor de riesgo : medio
Puntuación VPR : 4.8
Puntaje CVSS Fuente : CVE-2004-2320
Puntuación CVSS Justificación : Tenable cree que la vulnerabilidad xst solo afecta la confidencialidad, no la integridad (reflejada en la puntuación de nvd para cve-2010-0386)

CVSS v2.0

Puntuación base : 5
Puntaje temporal : 3.7
Vector : CVSS2 # AV: N / AC: L / Au: N / C: P / I: N / A: N
Vector temporal : CVSS2 # E: U / RL: OF / RC: C

CVSS v3.0

Puntuación base : 5.3
Puntuación temporal : 4.6
Vector : CVSS: 3.0 / AV: N / AC: L / PR: N / UI: N / S: U / C: L / I: N / A: N
Vector temporal : CVSS: 3.0 / E: U / RL: O / RC: C

Información de vulnerabilidad

Explotación disponible : falso
Exploit Ease : no hay exploits conocidos disponibles
Fecha de publicación de la vulnerabilidad : 2003/01/20
Informacion de referencia
CVE : CVE-2003-1567 , CVE-2004-2320 , CVE-2010-0386
OFERTA : 9506 , 9561 , 11604 , 33374 , 37995
CERT : 288308 , 867593
CWE : 16 , 200

140532 - PHP 7.2.x / 7.3.x <7.3.22 Vulnerabilidad de pérdida de memoria

MEDIO ID de complemento de Nessus 140532

Sinopsis
La versión de PHP que se ejecuta en el servidor web remoto se ve afectada por una vulnerabilidad de pérdida de memoria.
Descripción
Según su número de versión autoinformado, la versión de PHP que se ejecuta en el servidor web remoto es 7.2.xo 7.3.x antes de 7.3.21. Por lo tanto, se ve afectado por una vulnerabilidad de pérdida de memoria en el componente LDAP. Un atacante remoto no autenticado podría aprovechar este problema para causar una condición de denegación de servicio.
Solución
Actualice a la versión 7.3.22 de PHP o posterior.
Ver también
https://www.php.net/ChangeLog-7.php#7.3.22
Detalles del complemento
Severidad : media
ID : 140532
Nombre de archivo : php_7_3_22.nasl
Versión : 1.2
Tipo : remoto
Familia : abusos CGI
Publicado : 11/09/2020
Actualizado : 2020/10/09
Dependencias : 48243
Información de riesgo
Factor de riesgo : medio
Fuente de puntuación CVSS : manual
Puntuación CVSS Justificación : Dos
CVSS v2.0

Puntuación base : 5
Vector : CVSS2 # AV: N / AC: L / Au: N / C: N / I: N / A: P
CVSS v3.0
Puntuación base : 7.5
Vector : CVSS: 3.0 / AV: N / AC: L / PR: N / UI: N / S: U / C: N / I: N / A: H
Información de vulnerabilidad
CPE : cpe: / a: php: php
Elementos de KB necesarios : www / PHP , installed_sw / PHP
Fecha de publicación del parche : 2020/09/03
Fecha de publicación de vulnerabilidad : 2020/09/03
Informacion de referencia
IAVA : 2020-A-0420-S

142591 - PHP <7.3.24 Varias vulnerabilidades

MEDIO ID de complemento de Nessus 142591

Sinopsis
La versión de PHP que se ejecuta en el servidor web remoto se ve afectada por múltiples vulnerabilidades.
Descripción
Según su número de versión autoinformado, la versión de PHP que se ejecuta en el servidor web remoto es anterior a la 7.3.24. Por lo tanto, se ve afectado por múltiples vulnerabilidades.
Solución
Actualice a la versión 7.3.24 de PHP o posterior.
Ver también
https://www.php.net/ChangeLog-7.php#7.3.24
Detalles del complemento
Severidad : media
ID : 142591
Nombre de archivo : php_7_3_24.nasl
Versión : 1.3
Tipo : remoto
Familia : abusos CGI
Publicado : 06/11/2020
Actualizado : 2020/11/06
Dependencias : 48243
Información de riesgo
Factor de riesgo : medio
Fuente de puntuación CVSS : manual
Puntuación CVSS Justificación : Dos
CVSS v2.0

Puntuación base : 5
Vector : CVSS2 # AV: N / AC: L / Au: N / C: N / I: N / A: P
CVSS v3.0
Puntuación base : 7.5
Vector : CVSS: 3.0 / AV: N / AC: L / PR: N / UI: N / S: U / C: N / I: N / A: H
Información de vulnerabilidad
CPE : cpe: / a: php: php
Elementos de KB necesarios : www / PHP , installed_sw / PHP
Fecha de publicación del parche : 2020/10/29
Fecha de publicación de vulnerabilidad : 2020/10/29
Informacion de referencia
IAVA : 2020-A-0510

57608 - No se requiere firma SMB

MEDIO ID de complemento de Nessus 57608

Sinopsis
No es necesario firmar en el servidor SMB remoto.
Descripción
No es necesario firmar en el servidor SMB remoto. Un atacante remoto no autenticado puede aprovechar esto para realizar ataques man-in-the-middle contra el servidor SMB.
Solución
Hacer cumplir la firma de mensajes en la configuración del host. En Windows, esto se encuentra en la configuración de política 'Servidor de red de Microsoft: firmar digitalmente las comunicaciones (siempre)'. En Samba, la configuración se llama 'firma del servidor'. Consulte los enlaces "ver también" para obtener más detalles.
Ver también
https://support.microsoft.com/en-us/help/887429/overview-of-server-message-block-signing
http://technet.microsoft.com/en-us/library/cc731957.aspx
http://www.nessus.org/u?74b80723
https://www.samba.org/samba/docs/current/man-html/smb.conf.5.html
http://www.nessus.org/u?a3cac4ea
Detalles del complemento
Severidad : media
ID : 57608
Nombre de archivo : smb_signing_disabled.nasl
Versión : 1.18
Tipo : remoto
Familia : Misc.
Publicado : 19/01/2012
Actualizado : 2018/11/15

Dependencias : 11153
Información de riesgo
Factor de riesgo : medio
CVSS v2.0
Puntuación base : 5
Puntaje temporal : 3.7
Vector : CVSS2 # AV: N / AC: L / Au: N / C: N / I: P / A: N
Vector temporal : CVSS2 # E: U / RL: OF / RC: C
CVSS v3.0
Puntuación base : 5.3
Puntuación temporal : 4.6
Vector : CVSS: 3.0 / AV: N / AC: L / PR: N / UI: N / S: U / C: N / I: L / A: N
Vector temporal : CVSS: 3.0 / E: U / RL: O / RC: C
Información de vulnerabilidad
CPE : cpe: / o: microsoft: windows , cpe: / a: samba: samba
Fecha de publicación de la vulnerabilidad : 2012/01/17

15901 - Caducidad del certificado SSL

MEDIO ID de complemento de Nessus 15901

Sinopsis
El certificado SSL del servidor remoto ya ha caducado.
Descripción
Este complemento verifica las fechas de vencimiento de los certificados asociados con los servicios habilitados para SSL en el destino e informa si alguno ya ha vencido.
Solución
Compre o genere un nuevo certificado SSL para reemplazar el existente.
Detalles del complemento
Severidad : media
ID : 15901
Nombre de archivo : ssl_cert_expiry.nasl
Versión : 1.48
Tipo : remoto
Familia : General
Publicado : 03/12/2004
Actualizado : 2020/06/12
Dependencias : 56984
Información de riesgo
Factor de riesgo : medio
Fuente de puntuación CVSS : manual
Puntuación CVSS Justificación : Los certificados caducados no se pueden validar.

CVSS v2.0
Puntuación base : 5
Vector : CVSS2 # AV: N / AC: L / Au: N / C: N / I: P / A: N
CVSS v3.0
Puntuación base : 5.3
Vector : CVSS: 3.0 / AV: N / AC: L / PR: N / UI: N / S: U / C: N / I: L / A: N
Información de vulnerabilidad
Elementos de KB obligatorios : SSL / compatible

35291 - Certificado SSL firmado mediante un algoritmo de hash débil

MEDIO ID de complemento de Nessus 35291

¡Nuevo! Clasificación de prioridad de vulnerabilidad (VPR)
Tenable calcula un VPR dinámico para cada vulnerabilidad. VPR combina información sobre vulnerabilidades con inteligencia de amenazas y algoritmos de aprendizaje automático para predecir qué vulnerabilidades tienen más probabilidades de ser explotadas en ataques. Lea más sobre qué es VPR y en qué se diferencia de CVSS.
Puntuación VPR: 4,4
Sinopsis
Se ha firmado un certificado SSL en la cadena de certificados utilizando un algoritmo hash débil.
Descripción
El servicio remoto utiliza una cadena de certificados SSL que se ha firmado mediante un algoritmo hash criptográficamente débil (por ejemplo, MD2, MD4, MD5 o SHA1). Se sabe que estos algoritmos de firma son vulnerables a los ataques de colisión. Un atacante puede aprovechar esto para generar otro certificado con la misma firma digital, permitiendo que un atacante se haga pasar por el servicio afectado.
Tenga en cuenta que este complemento informa todas las cadenas de certificados SSL firmadas con SHA-1 que caducan después del 1 de enero de 2017 como vulnerables. Esto está de acuerdo con la desaparición gradual de Google del algoritmo de hash criptográfico SHA-1. Tenga en cuenta que los certificados de la cadena que están contenidos en la base de datos de Nessus CA (known_CA.inc) se han ignorado.
Solución
Póngase en contacto con la autoridad de certificación para que se vuelva a emitir el certificado SSL.
Ver también
https://tools.ietf.org/html/rfc3279
http://www.nessus.org/u?9bb87bf2
http://www.nessus.org/u?e120eea1
http://www.nessus.org/u?5d894816
http://www.nessus.org/u?51db68aa

http://www.nessus.org/u?9dc7bfba
Detalles del complemento
Severidad : media
ID : 35291
Nombre de archivo : ssl_weak_hash.nasl
Versión : 1.31
Tipo : remoto
Familia : General
Publicado : 05/01/2009
Actualizado : 2020/04/27
Dependencias : 57571
Información de riesgo
Factor de riesgo : medio
Puntuación VPR : 4,4
Puntaje CVSS Fuente : CVE-2004-2761
CVSS v2.0
Puntuación base : 5
Puntuación temporal : 3.9
Vector : CVSS2 # AV: N / AC: L / Au: N / C: N / I: P / A: N
Vector temporal : CVSS2 # E: POC / RL: OF / RC: C
CVSS v3.0
Puntuación base : 7.5
Puntuación temporal : 6,7
Vector : CVSS: 3.0 / AV: N / AC: L / PR: N / UI: N / S: U / C: N / I: H / A: N
Vector temporal : CVSS: 3.0 / E: P / RL: O / RC: C
Información de vulnerabilidad
CPE : cpe: / a: ietf: md5 , cpe: / a: ietf: x.509_certificate
Elementos de KB obligatorios : SSL / Chain / WeakHash
Explotar disponible : verdadero
Exploit Ease : Exploits están disponibles
Fecha de publicación de la vulnerabilidad : 18/08/2004
Informacion de referencia
CVE : CVE-2004-2761
OFERTA : 11849 , 33065
CERT : 836068
CWE : 310

45411 - Certificado SSL con nombre de host incorrecto

MEDIO ID de complemento de Nessus 45411

Sinopsis
El certificado SSL para este servicio es para un host diferente.
Descripción
El atributo 'commonName' (CN) del certificado SSL presentado para este servicio es para una máquina diferente.
Solución
Compre o genere un certificado SSL adecuado para este servicio.
Detalles del complemento
Severidad : media
ID : 45411
Nombre de archivo : ssl_cert_wrong_host.nasl
Versión : 1.20
Tipo : remoto
Familia : General
Publicado : 03/04/2010
Actualizado : 2020/04/27
Dependencias : 24272 , 46180 , 56984 , 43815 , 45410 , 25202 , 25203
Información de riesgo
Factor de riesgo : medio
Fuente de puntuación CVSS : manual
Puntuación CVSS Justificación : El certificado SSL para este servicio es para un host diferente.
CVSS v2.0
Puntuación base : 5
Vector : CVSS2 # AV: N / AC: L / Au: N / C: N / I: P / A: N
CVSS v3.0
Puntuación base : 5.3
Vector : CVSS: 3.0 / AV: N / AC: L / PR: N / UI: N / S: U / C: N / I: L / A: N
Información de vulnerabilidad
Elementos de KB obligatorios : SSL / compatible

42873 - Se admiten conjuntos de cifrado de intensidad media SSL (SWEET32)

MEDIO ID de complemento de Nessus 42873

¡Nuevo! Clasificación de prioridad de vulnerabilidad (VPR)
Tenable calcula un VPR dinámico para cada vulnerabilidad. VPR combina información sobre vulnerabilidades con inteligencia de amenazas y algoritmos de aprendizaje automático para

predecir qué vulnerabilidades tienen más probabilidades de ser explotadas en ataques. Lea más sobre qué es VPR y en qué se diferencia de CVSS.

Puntuación VPR: 5.1

Sinopsis

El servicio remoto admite el uso de cifrados SSL de nivel medio.

Descripción

El host remoto admite el uso de cifrados SSL que ofrecen cifrado de nivel medio. Nessus considera que la potencia media es cualquier cifrado que utilice longitudes de clave de al menos 64 bits y menos de 112 bits, o que utilice el paquete de cifrado 3DES. Tenga en cuenta que es considerablemente más fácil eludir el cifrado de nivel medio si el atacante está en la misma red física.

Solución

Reconfigure la aplicación afectada si es posible para evitar el uso de cifrados de fuerza media.

Ver también

https://www.openssl.org/blog/blog/2016/08/24/sweet32/
https://sweet32.info

Detalles del complemento

Severidad : media
ID : 42873
Nombre de archivo : ssl_medium_supported_ciphers.nasl
Versión : 1.20
Tipo : remoto
Familia : General
Publicado : 23/11/2009
Actualizado : 2019/02/28
Dependencias : 21643

Información de riesgo

Factor de riesgo : medio
Puntuación VPR : 5.1
Puntaje CVSS Fuente : CVE-2016-2183
CVSS v2.0
Puntuación base : 5
Vector : CVSS2 # AV: N / AC: L / Au: N / C: P / I: N / A: N
CVSS v3.0
Puntuación base : 7.5
Vector : CVSS: 3.0 / AV: N / AC: L / PR: N / UI: N / S: U / C: H / I: N / A: N

Información de vulnerabilidad

Elementos de KB obligatorios : SSL / compatible
Fecha de publicación de la vulnerabilidad : 2016/08/24

Informacion de referencia

CVE : CVE-2016-2183

12218 - Detección mDNS (red remota)

MEDIO ID de complemento de Nessus 12218

Sinopsis

Es posible obtener información sobre el host remoto.

Descripción

El servicio remoto comprende el protocolo Bonjour (también conocido como ZeroConf o mDNS), que permite a cualquier persona descubrir información del host remoto, como el tipo de sistema operativo y la versión exacta, su nombre de host y la lista de servicios que está ejecutando. Este complemento intenta descubrir mDNS utilizado por hosts que no están en el segmento de red en el que reside Nessus.

Solución

Filtre el tráfico entrante al puerto UDP 5353, si lo desea.

Detalles del complemento

Severidad : media

ID : 12218

Nombre de archivo : mdns.nasl

Versión : Revisión: 1.26

Tipo : remoto

Familia : detección de servicios

Publicado : 28/04/2004

Actualizado : 2013/05/31

Información de riesgo

Factor de riesgo : medio

CVSS v2.0

Puntuación base : 5

Vector : CVSS2 # AV: N / AC: L / Au: N / C: P / I: N / A: N

144047 - OpenSSL 1.1.1 <1.1.1i Vulnerabilidad de desreferencia de puntero nulo

MEDIO ID de complemento de Nessus 144047

¡Nuevo! Clasificación de prioridad de vulnerabilidad (VPR)

Tenable calcula un VPR dinámico para cada vulnerabilidad. VPR combina información sobre vulnerabilidades con inteligencia de amenazas y algoritmos de aprendizaje automático para predecir qué vulnerabilidades tienen más probabilidades de ser explotadas en ataques. Lea más sobre qué es VPR y en qué se diferencia de CVSS.

Puntuación VPR: 5.1

Sinopsis

El servicio remoto se ve afectado por una vulnerabilidad de desreferencia de puntero nulo.

Descripción

La versión del producto probado instalado en el host remoto es anterior a la versión probada. Por lo tanto, está afectado por una vulnerabilidad como se menciona en el aviso 1.1.1i.

- El tipo X.509 GeneralName es un tipo genérico para representar diferentes tipos de nombres. Uno de esos tipos de nombres se conoce como EDIPartyName. OpenSSL proporciona una función GENERAL_NAME_cmp que compara diferentes instancias de GENERAL_NAME para ver si son iguales o no. Esta función se comporta incorrectamente cuando ambos GENERAL_NAME contienen un EDIPARTYNAME. Es posible que se produzca una desreferencia del puntero NULO y un bloqueo que conduzca a un posible ataque de denegación de servicio. El propio OpenSSL utiliza la función GENERAL_NAME_cmp para dos propósitos: 1) Comparación de nombres de puntos de distribución de CRL entre una CRL disponible y un punto de distribución de CRL incrustado en un certificado X509 2) Al verificar que un firmante de token de respuesta de marca de tiempo coincide con el nombre de autoridad de marca de tiempo (expuesto a través de las funciones de API TS_RESP_verify_response y TS_RESP_verify_token) Si un atacante controlar ambos elementos que se están comparando, entonces ese atacante podría provocar un bloqueo. Por ejemplo, si el atacante puede engañar a un cliente o servidor para que compruebe un certificado malicioso con una CRL maliciosa, esto puede ocurrir. Tenga en cuenta que algunas aplicaciones descargan automáticamente las CRL basadas en una URL incrustada en un certificado. Esta verificación ocurre antes de que se verifiquen las firmas en el certificado y la CRL. Por ejemplo, si el atacante puede engañar a un cliente o servidor para que compruebe un certificado malicioso con una CRL maliciosa, esto puede ocurrir. Tenga en cuenta que algunas aplicaciones descargan automáticamente las CRL basadas en una URL incrustada en un certificado. Esta verificación ocurre antes de que se verifiquen las firmas en el certificado y la CRL. Por ejemplo, si el atacante puede engañar a un cliente o servidor para que compruebe un certificado malicioso con una CRL maliciosa, esto puede ocurrir. Tenga en cuenta que algunas aplicaciones descargan automáticamente las CRL basadas en una URL incrustada en un certificado. Esta verificación ocurre antes de que se verifiquen las firmas en el certificado y la CRL.

Las herramientas s_server, s_client y verify de OpenSSL tienen soporte para la opción -crl_download que implementa la descarga automática de CRL y se ha demostrado que este ataque funciona contra esas herramientas. Tenga en cuenta que un error no relacionado significa que las versiones afectadas de OpenSSL no pueden analizar ni construir codificaciones correctas de EDIPARTYNAME. Sin embargo, es posible construir un EDIPARTYNAME con formato incorrecto que el analizador de OpenSSL aceptará y, por lo tanto, desencadenará este ataque. Todas las versiones de OpenSSL 1.1.1 y 1.0.2 se ven afectadas por este problema.
Otras versiones de OpenSSL no son compatibles y no se han comprobado. Corregido en OpenSSL 1.1.1i (Afectado 1.1.1-1.1.1h). Corregido en OpenSSL 1.0.2x (Afectado 1.0.2-1.0.2w). (CVE-2020-1971)

Tenga en cuenta que Nessus no ha probado este problema, sino que se ha basado únicamente en el número de versión autoinformado de la aplicación.

Solución

Actualice a OpenSSL versión 1.1.1i o posterior.
Ver también
http://www.nessus.org/u?dc9b62cf
https://www.openssl.org/news/secadv/20201208.txt
Detalles del complemento
Severidad : media
ID : 144047
Nombre de archivo : openssl_1_1_1i.nasl
Versión : 1.5
Tipo : remoto
Familia : servidores web
Publicado : 10/12/2020
Actualizado : 2020/12/16
Dependencias : 57323
Información de riesgo
Factor de riesgo : medio
Puntuación VPR : 5.1
Puntaje CVSS Fuente : CVE-2020-1971
CVSS v2.0
Puntuación base : 4,3
Puntaje temporal : 3.2
Vector : CVSS2 # AV: N / AC: M / Au: N / C: N / I: N / A: P
Vector temporal : CVSS2 # E: U / RL: OF / RC: C
CVSS v3.0
Puntuación base : 5.9
Puntuación temporal : 5.2
Vector : CVSS: 3.0 / AV: N / AC: H / PR: N / UI: N / S: U / C: N / I: N / A: H
Vector temporal : CVSS: 3.0 / E: U / RL: O / RC: C
Información de vulnerabilidad
CPE : cpe: / a: openssl: openssl
Elementos de KB necesarios : openssl / port
Exploit Ease : no hay exploits conocidos disponibles
Fecha de publicación del parche : 08/12/2020
Fecha de publicación de la vulnerabilidad : 08/12/2020
Informacion de referencia
CVE : CVE-2020-1971
IAVA : 2020-A-0566

ANEXO E

DECLARACION DE APLICABILIDAD

Codificacion	Titulo	Descripción	si	no	Justificación
A5.1.1	Políticas para la seguridad de la información	Control: Se debe definir un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los empleados y a las partes externas pertinentes.	x		Las politicas de seguridad de la información existentes en la institución deben ser reevaluadas de acuerdo a las necesidades actuales, aprobadas por la dirección y socializadas a todo el personal.
A5.1.2	Revisión de las políticas para la seguridad de la información.	Control: Las políticas para la seguridad de la información se deben revisar a intervalos planificados o si ocurren cambios significativos, para para asegurar su conveniencia, adecuación y eficacia continuas.	x		Las politicas de seguridad de la información existentes en la institución deben ser reevaluadas de acuerdo a las necesidades actuales, aprobadas por la dirección y socializadas a todo el personal.
A6.1.1	Roles y responsabilidades para la seguridad de la información	Control: Se deben definir y asignar todas las responsabilidades de la seguridad de la información.	x		Las politicas de seguridad de la información existentes en la institución deben ser reevaluadas de acuerdo a las necesidades actuales, aprobadas por la dirección y socializadas a todo el personal.
A6.1.2	Separación de deberes	Control: Los deberes y áreas de responsabilidad en conflicto se deben separar para reducir las posibilidades de modificación no autorizada o no intencional, o el uso indebido de los activos de la organización	x		Las actividades de seguridad de la información deben ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles laborales relevantes.
A6.1.5	Seguridad de la información en la gestión de proyectos.	Control: La seguridad de la información se debe tratar en la gestión de proyectos, independientemente del tipo de proyecto.	x		Los procesos de desarrollo vigentes tiene inicio y aprobación de cambios dado por la dirección del área.
A6.2.1	Política para dispositivos móviles	Control: Se deben adoptar una política y unas medidas de seguridad de soporte, para gestionar los riesgos introducidos por el uso de dispositivos móviles.	x		No existen politicas para el uso de dispositivos moviles en el centro.
A6.2.2	Teletrabajo	Control: Se deben implementar una política y unas medidas de seguridad de soporte, para proteger la información a la que se tiene acceso, que es procesada o almacenada en los lugares en los que se realiza teletrabajo.	x		Es necesario fortalecer las politicas y medidas tendientes a proteger la información de las sesiones virtuales de tutoria y/o videoconferencias.
A7.2.2	Toma de conciencia, educación y formación en la seguridad de la información.	Control: Todos los empleados de la organización, y en donde sea pertinente, los contratistas, deben recibir la educación y la formación en toma de conciencia apropiada, y actualizaciones regulares sobre las políticas y procedimientos de la organización pertinentes para su cargo.		x	Programación de capacitación a todo el personal en materia de seguridad de la información y politicas de seguridad del centro.
A8.1.1	Inventario de activos	Control: Se deben identificar los activos asociados con información e instalaciones de procesamiento de información, y se debe elaborar y mantener un inventario de estos activos.	x		Procedimientos para la actualización constante de los activos
A8.1.2	Propiedad de los activos	Control: Los activos mantenidos en el inventario deben tener un propietario.	x		Asociar cada activo a un responsable
A8.1.3	Uso aceptable de los activos	Control: Se deben identificar, documentar e implementar reglas para el uso aceptable de información y de activos asociados con información e instalaciones de procesamiento de información.	x		No existen politicas para el uso adecuado y responsable de los equipos en el centro.
A9.1.1	Política de control de acceso	Control: Se debe establecer, documentar y revisar una política de control de acceso con base en los requisitos del negocio y de la seguridad de la información.	x		Definir politicas y niveles de acceso a la información
A9.1.2	Acceso a redes y a servicios en red	Control: Solo se debe permitir acceso de los usuarios a la red y a los servicios de red para los que hayan sido autorizados específicamente.	x		Definir politicas y niveles de acceso a la información
A9.2.1	Registro y cancelación del registro de usuarios	Control: Se debe implementar un proceso formal de registro y de cancelación de registro de usuarios, para posibilitar la asignación de los derechos de acceso.	x		Verificar proceso para registro y cancelación de usuarios
A9.2.2	Suministro de acceso de usuarios	Control: Se debe implementar un proceso de suministro de acceso formal de usuarios para asignar o revocar los derechos de acceso para todo tipo de usuarios para todos los sistemas y servicios.		x	Definir politicas y niveles de acceso a la información
A9.2.3	Gestión de derechos de acceso privilegiado	Control: Se debe restringir y controlar la asignación y uso de derechos de acceso privilegiado	x		Definir politicas y niveles de acceso a la información
A9.2.4	Gestión de información de autenticación secreta de usuarios	Control: La asignación de información de autenticación secreta se debe controlar por medio de un proceso de gestión formal.	x		Definir politicas y niveles de acceso a la información
A9.2.5	Revisión de los derechos de acceso de usuarios	Control: Los propietarios de los activos deben revisar los derechos de acceso de los usuarios, a intervalos regulares.	x		Definir politicas y niveles de acceso a la información
A9.4.1	Restricción de acceso a la información	Control: El acceso a la información y a las funciones de los sistemas de las aplicaciones se debe restringir de acuerdo con la política de control de acceso.	x		Definir politicas y niveles de acceso a la información
A9.4.2	Procedimiento de ingreso seguro	Control: Cuando lo requiere la política de control de acceso, el acceso a sistemas y aplicaciones se debe controlar mediante un proceso de ingreso seguro.	x		Definir pedagogia para el ingreso de usuarios y visitantes acorde a las politicas de seguridad.
A9.4.3	Sistema de gestión de contraseñas	Control: Los sistemas de gestión de contraseñas deben ser interactivos y deben asegurar la calidad de las contraseñas.	x		Verificar el proceso de generación de contraseñas y el nivel de seguridad de las mismas.
A9.4.5	Control de acceso a códigos fuente de programas	Control: Se debe restringir el acceso a los códigos fuente de los programas.	x		Documentar todo el proceso de desarrollo
A11.1.1	Perímetro de seguridad física	Control: Se deben definir y usar perímetros de seguridad, y usarlos para proteger áreas que contengan información confidencial o critica, e instalaciones de manejo de información.	x		Determinar las areas con manejo de información critica y establecer medidas de seguridad y acceso de personal.

Codificacion	Titulo	Descripción	sí	no	Justificación
A11.1.2	Controles de acceso físicos	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	X		Determinar las areas con manejo de información critica y establecer medidas de seguridad y acceso de personal.
A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones..	X		Determinar las areas con manejo de información critica y establecer medidas de seguridad y acceso de personal.
A11.1.4	Protección contra amenazas externas y ambientales.	Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	X		Revisar los procedimientos y sistemas de emergencias, asi como el plan de contingencia del centro.
A11.2.4	Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	X		Definir los procedimientos para el soporte técnico y mantnimiento de equipos.
A12.1.2	Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	X		Diseñar plan de revisión y evaluación del sistema de seguridad de la información.
A12.1.3	Gestión de capacidad	Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	X		Definir plan de proyección de crecimiento y modernización del centro.
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	X		Verificar que los ambientes de desarrollo, pruebas y producción se encuentren definidos.
A12.2.1	Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	X		Reevaluar los controles de detección de intrusos exitentes
A12.3.1	Respaldo de la información	Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	X		Evaluar el procedimiento para copias de seguridad del centro.
A12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	X		Diseñar procedimientos para el registro de eventos.
A12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	X		No existen politicas para el uso adecuado y responsable de los equipos en el centro.
A12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	X		Revisión de los procedimientos de soporte técnico y mantenimiento de equipos.
A12.6.2	Restricciones sobre la instalación de software	Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	X		No existen politicas para el uso adecuado y responsable de los equipos en el centro.
A12.7.1	Controles de auditorías de sistemas de información	Control: Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	X		No existen lineamientos para los procesos de audoría en el centro.
A13.1.1	Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	X		Evaluar los controles existentes en la red, filtrado de contenidos, segmentación, acceso a la red, etc.
A13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	X		Evaluar los controles existentes en la red, filtrado de contenidos, segmentación, acceso a la red, etc.
A13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	X		Evaluar los controles existentes en la red, filtrado de contenidos, segmentación, acceso a la red, etc.
A13.2.3	Mensajería Electronica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	X		Programación de capacitación a todo el personal en materia de seguridad de la información y politicas de seguridad del centro.
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	X		Las politicas de seguridad de la información existentes en la institución deben ser reevaluadas de acuerdo a las necesidades actuales, aprobadas por la dirección y socializadas a todo el personal.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Control: La informacion involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	X		Evaluar los controles existentes en la red, filtrado de contenidos, segmentación, acceso a la red, etc.
A.14.1.3	Protección de transaccciones de los servicios de las aplicaciones.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	X		Las politicas de seguridad de la información existentes en la institución deben ser reevaluadas de acuerdo a las necesidades actuales, aprobadas por la dirección y socializadas a todo el personal.

Codificacion	Titulo	Descripción	si	no	Justificación
A11.1.2	Controles de acceso físicos	Control: Las áreas seguras deben estar protegidas con controles de acceso apropiados para asegurar que sólo se permite el acceso a personal autorizado.	X		Determinar las areas con manejo de información critica y establecer medidas de seguridad y acceso de personal.
A11.1.3	Seguridad de oficinas, recintos e instalaciones.	Control: Se debe diseñar y aplicar la seguridad física para oficinas, recintos e instalaciones..	X		Determinar las areas con manejo de información critica y establecer medidas de seguridad y acceso de personal.
A11.1.4	Protección contra amenazas externas y ambientales.	Control: Se deben diseñar y aplicar protección física contra desastres naturales, ataques maliciosos o accidentes.	X		Revisar los procedimientos y sistemas de emergencias, asi como el plan de contingencia del centro.
A11.2.4	Mantenimiento de los equipos.	Control: Los equipos se deben mantener correctamente para asegurar su disponibilidad e integridad continuas.	X		Definir los procedimientos para el soporte técnico y mantnimiento de equipos.
A12.1.2	Gestión de cambios	Control: Se deben controlar los cambios en la organización, en los procesos de negocio, en las instalaciones y en los sistemas de procesamiento de información que afectan la seguridad de la información.	X		Diseñar plan de revisión y evaluación del sistema de seguridad de la información.
A12.1.3	Gestión de capacidad	Control: Se debe hacer seguimiento al uso de recursos, hacer los ajustes, y hacer proyecciones de los requisitos de capacidad futura, para asegurar el desempeño requerido del sistema.	X		Definir plan de proyección de crecimiento y modernización del centro.
A12.1.4	Separación de los ambientes de desarrollo, pruebas y operación	Control: Se deben separar los ambientes de desarrollo, pruebas y operación, para reducir los riesgos de acceso o cambios no autorizados al ambiente de operación.	X		Verificar que los ambientes de desarrollo, pruebas y producción se encuentren definidos.
A12.2.1	Controles contra códigos maliciosos	Control: Se deben implementar controles de detección, de prevención y de recuperación, combinados con la toma de conciencia apropiada de los usuarios, para proteger contra códigos maliciosos.	X		Reevaluar los controles de detección de intrusos exitentes
A12.3.1	Respaldo de la información	Control: Se deben hacer copias de respaldo de la información, software e imágenes de los sistemas, y ponerlas a prueba regularmente de acuerdo con una política de copias de respaldo acordadas.	X		Evaluar el procedimiento para copias de seguridad del centro.
A12.4.1	Registro de eventos	Control: Se deben elaborar, conservar y revisar regularmente los registros acerca de actividades del usuario, excepciones, fallas y eventos de seguridad de la información.	X		Diseñar procedimientos para el registro de eventos.
A12.5.1	Instalación de software en sistemas operativos	Control: Se deben implementar procedimientos para controlar la instalación de software en sistemas operativos.	X		No existen politicas para el uso adecuado y responsable de los equipos en el centro.
A12.6.1	Gestión de las vulnerabilidades técnicas	Control: Se debe obtener oportunamente información acerca de las vulnerabilidades técnicas de los sistemas de información que se usen; evaluar la exposición de la organización a estas vulnerabilidades, y tomar las medidas apropiadas para tratar el riesgo asociado.	X		Revisión de los procedimientos de soporte técnico y mantenimiento de equipos.
A12.6.2	Restricciones sobre la instalación de software	Control: Se deben establecer e implementar las reglas para la instalación de software por parte de los usuarios.	X		No existen politicas para el uso adecuado y responsable de los equipos en el centro.
A12.7.1	Controles de auditorías de sistemas de información	Control: Los requisitos y actividades de auditoria que involucran la verificación de los sistemas operativos se deben planificar y acordar cuidadosamente para minimizar las interrupciones en los procesos del negocio.	X		No existen lineamientos para los procesos de audoría en el centro.
A13.1.1	Controles de redes	Control: Las redes se deben gestionar y controlar para proteger la información en sistemas y aplicaciones.	X		Evaluar los controles existentes en la red, filtrado de contenidos, segmentación, acceso a la red, etc.
A13.1.2	Seguridad de los servicios de red	Control: Se deben identificar los mecanismos de seguridad, los niveles de servicio y los requisitos de gestión de todos los servicios de red, e incluirlos en los acuerdos de servicio de red, ya sea que los servicios se presten internamente o se contraten externamente.	X		Evaluar los controles existentes en la red, filtrado de contenidos, segmentación, acceso a la red, etc.
A13.1.3	Separación en las redes	Control: Los grupos de servicios de información, usuarios y sistemas de información se deben separar en las redes.	X		Evaluar los controles existentes en la red, filtrado de contenidos, segmentación, acceso a la red, etc.
A13.2.3	Mensajería Electronica	Control: Se debe proteger adecuadamente la información incluida en la mensajería electrónica.	X		Programación de capacitación a todo el personal en materia de seguridad de la información y politicas de seguridad del centro.
A.14.1.1	Análisis y especificación de requisitos de seguridad de la información	Control: Los requisitos relacionados con seguridad de la información se deben incluir en los requisitos para nuevos sistemas de información o para mejoras a los sistemas de información existentes.	X		Las politicas de seguridad de la información existentes en la institución deben ser reevaluadas de acuerdo a las necesidades actuales, aprobadas por la dirección y socializadas a todo el personal.
A.14.1.2	Seguridad de servicios de las aplicaciones en redes públicas	Control: La informacion involucrada en los servicios de las aplicaciones que pasan sobre redes públicas se debe proteger de actividades fraudulentas, disputas contractuales y divulgación y modificación no autorizadas.	X		Evaluar los controles existentes en la red, filtrado de contenidos, segmentación, acceso a la red, etc.
A.14.1.3	Protección de transaccciones de los servicios de las aplicaciones.	Control: La información involucrada en las transacciones de los servicios de las aplicaciones se deben proteger para evitar la transmisión incompleta, el enrutamiento errado, la alteración no autorizada de mensajes, la divulgación no autorizada, y la duplicación o reproducción de mensajes no autorizada.	X		Las politicas de seguridad de la información existentes en la institución deben ser reevaluadas de acuerdo a las necesidades actuales, aprobadas por la dirección y socializadas a todo el personal.