CASO DE ESTUDIO PARA EL ANÁLISIS DE VULNERABILIDAD Y PROPUESTA DE ASEGURAMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA EMPRESA NOSTRADAMUS S.A.S

ALEJANDRO MEJÍA ESCOBAR

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ

2020

CASO DE ESTUDIO PARA EL ANÁLISIS DE VULNERABILIDAD Y PROPUESTA DE ASEGURAMIENTO DE LA SEGURIDAD DE LA INFORMACIÓN EN LA INFRAESTRUCTURA TECNOLÓGICA DE LA EMPRESA NOSTRADAMUS S.A.S

ALEJANDRO MEJÍA ESCOBAR

Anteproyecto para optar por el título de

ESPECIALISTA EN SEGURIDAD INFORMÁTICA

Asesor Metodológico

EDGAR ROBERTO DULCE

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA - UNAD

ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA – ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ

2020

Nota de aceptación:

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

Bogotá, 13 de marzo de 2020

DEDICATORIA

A mis padres, mi esposa y mis hijas, por todo el apoyo y la paciencia.

AGRADECIMIENTOS

A los asesores por su apoyo y orientación, así como a mi familia por la paciencia y el acompañamiento en este periodo de fortalecimiento profesional.

RESUMEN

En este proyecto aplicado se trabajará sobre el caso de estudio NOSTRADAMUS S.A.S, empresa que ha sufrido de una serie de ataques informáticos, los cuales serán replicados para identificar las vulnerabilidades del sistema: ingeniería social, elevación de privilegios, denegación de servicio, ransomware e inyección de SQL. A partir de los hallazgos encontrados y la evaluación de los activos informáticos de NOSTRADAMUS S.A.S, se propondrá una serie de documentos base para la posterior implementación de un Sistema de Gestión de la Seguridad Informática, teniendo presente la norma ISO 27001, con el fin de reforzar el aseguramiento de la información en la infraestructura tecnológica de NOSTRADAMUS S.A.S.

PALABRAS CLAVES

Seguridad informática, seguridad de la información, vulnerabilidades, ingeniería social, elevación de privilegios, lazange, ransomware, SQL inyection, plan de mitigación, ISO 27001, pentesting, sistema de gestión de la información, MAGERIT.

ABSTRACT

In this applied project, we will work on the case study NOSTRADAMUS SAS, a company that has suffered a series of computer attacks, which will be replicated to identify system vulnerabilities: social engineering, privilege problems, denial of service, ransomware and injection of SQL. Based on the findings found and the evaluation of the IT assets of NOSTRADAMUS SAS, a series of base documents will be proposed for the subsequent implementation of a Computer Security Management System, taking into account ISO 27001, with the end of infrastructure the assurance of information in the technological infrastructure of said NOSTRADAMUS S.A.S.

KEYWORDS

Computer security, information security, vulnerabilities, social engineering, elevation of privileges, lazange, ransomware, SQL injection, mitigation plan, ISO 27001, pentesting.

TABLA DE CONTENIDO

LISTA DE TABLAS

LISTA DE FIGURAS

LISTA DE ANEXOS

GLOSARIO

CRACKER: Término que proviene de la palabra inglesa crack, que significa romper. Se asigna a personas que se dedican a violar la seguridad de un sistema de manera ilegal y con el fin de sacar provecho monetario del acto delictivo, o simplemente con el fin de producir daño a su víctima[1]. Son ciberdelincuentes, no debe confundirse con los Hacker.

DENEGACIÓN DE SERVICIO: También conocido con DoS, es un ataque que tiene como objetivo disminuir e incluso detener la disponibilidad de un servicio mediante un ataque, bien sea a la fuente de la información, al canal de transmisión o ambos[2]. Una variante son los ataques Distribuidos de Denegación de Servicio (DDoS), en el cual el atacante ha logrado infectar un gran número de máquinas para que todas a la vez envíen paquetes de datos inútiles al servidor víctima y así logren o bien saturar el ancho de banda del servidor para dejarlo inaccesible, o bien agotando directamente los recursos de la máquina host[3].

ELEVACIÓN DE PRIVILEGIOS: Se dice que hay elevación de privilegios cuando un usuario que no es el administrador de un sistema logra tener acceso a las

---

[1] Hector Jara y Federico G Pacheco, *Ethical Hacking 2.0* (Usershop, 2012), https://books.google.com.co/books?hl=es&lr=lang_es&id=PkDCIzakkB4C&oi=fnd&pg=PA4&dq=riesgo+de+ethical+hacking&ots=B4x48Tz38q&sig=LtD_o7zAxvXnRrsMzFPMkvrOHRY&redir_esc=y#v=onepage&q=riesgo%20de%20ethical%20hacking&f=false.

[2] Gabriel Macía Fernández, «Ataques de denegación de servicio a baja tasa contra servidores», 2007, http://digibug.ugr.es/bitstream/handle/10481/1543/16714763.pdf?sequence=1.

[3] Monsalve Mendez y Jaime Yesid, «Ciberseguridad: Principales Amenazas En Colombia (Ingeniería Social, Phishing y Dos)», 21 de noviembre de 2018, http://repository.unipiloto.edu.co/handle/20.500.12277/4663.

funciones de administrador y modificar el sistema a su antojo[4]. Normalmente cuando se habla de elevación de privilegios se refiere al sistema operativo.

EXPLOIT: Pequeña aplicación o fragmento de código que se utiliza con el fin de aprovechar una vulnerabilidad conocida de un software, producto de un fallo en su programación, generalmente en la etapa de implementación[5].

HACKER: Término que se utiliza para referirse a alguien que es experto en un campo especifico, no sólo técnico o informático, sino de cualquier área del conocimiento humano[6]. El concepto de hacker ha sufrido de mala fama por la prensa y la opinión pública, sin embargo, no debe confundirse con los crackers. Son grandes los aportes que el hacking ha contribuido a la evolución de tecnologías emergentes, especialmente en internet, gracias a ellos existen los foros, los detectores de intrusos, los antimalware y un sinfín de aportes más[7].

INGENIERÍA SOCIAL: Técnica que se utiliza para extraer información de otras personas utilizando como base la interacción social, donde la víctima no se da cuenta que está revelando información personal sensible que después puede ser utilizada por el atacante para inducir a la víctima a un escenario vulnerable, suplantar su identidad o realizar extorsión[8]. Existen dos principales formas de ataque en la ingeniería social, el primero es basado en el uso de tecnologías, en el

---

[4] Monterroza Barrios y Rafael Enrique, «Análisis, explotación y definición de estrategias de mitigación de vulnerabilidades en un sistema GNU/Linux», 7 de enero de 2019, http://openaccess.uoc.edu/webapps/o2/handle/10609/91846.

[5] Guillén Zafra y José Luis, «Introducción al pentesting», 20 de julio de 2017, http://diposit.ub.edu/dspace/bitstream/2445/124085/2/memoria.pdf.

[6] Jara y Pacheco, *Ethical Hacking 2.0*.

[7] Federico Iván Gacharná Gacharná, «El estigma Hacker, entre lo bueno y lo malo», *INVENTUM* 6, n.º 10 (1 de febrero de 2011): 24-27, https://doi.org/10.26620/uniminuto.inventum.6.10.2011.24-27.

[8] Lady Johana Cañon Parada, «Ataques informáticos, Ethical Hacking y conciencia de seguridad informática en niños» (Universidad Piloto de Colombia, 2015), http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2870/00002427.pdf?sequence=1, http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2870/00002427.pdf?sequence=1.

cual el atacante logra engañar a la víctima haciéndole creer que está interactuando con un sitio de confianza o legitimo; el segundo es basado en el engaño humano, en el que el atacante logra congraciar con la víctima para extraer información[9].

INYECCIÓN DE SQL: Ataque cuyo principal objetivo son los aplicativos web, buscando acceder a las bases de datos donde se almacena la información privada de los usuarios; los crackers se enfocan especialmente en páginas web de comercio donde podrían extraer grandes cantidades de información sensible[10].

KALI LINUX: Herramienta para la auditoria y seguridad informática. Creada y mantenida por Offesive Security Ltd., donde Devon Kearns y Mati Aharoni la desarrollaron basándose en la re escrituración de BackTrack. Cada paquete de Kali está firmado por el desarrollador, el compilado y el publicador de la actualización. Así mismo, los encargados de mantener los repositorios de Kali firman los paquetes utilizando GNU Privacy Guard[11].

PENTESTING: Prueba de penetración, en ingles pentesting, es un ataque voluntario a una infraestructura tecnológica con la intención de identificar las vulnerabilidades existentes en los sistemas que la compongan y así hallar puntos de acceso no permitidos a datos y funcionalidades. Gracias a estas pruebas se

[9] Alejandro Méndez Carvajal, «Estudio de metodologías de ingeniería social», diciembre de 2018, http://openaccess.uoc.edu/webapps/o2/handle/10609/90305.
[10] Cañon Parada, «Ataques informáticos, Ethical Hacking y conciencia de seguridad informática en niños».
[11] Esquerra Blanco y Liliana de la Caridad, «Pruebas de penetración con la herramienta Kali Linux en la Universidad Central Marta Abreu de las Villas» (Thesis, Universidad Central «Marta Abreu» de Las Villas, 2014), http://dspace.uclv.edu.cu/bitstream/handle/123456789/1350/Liliana%20de%20la%20Caridad%20Esquerra%20Blanco.pdf?sequence=1&isAllowed=y.

puede reforzar la seguridad informática de una empresa, evaluando el impacto potencial y tomando medidas para la reducción del riesgo[12].

RANSOMWARE: Software malicioso, o malware, que toma el control de un sistema o sus datos, comúnmente cifrando los archivos con una clave que solo el atacante conoce, con el fin de exigirle un pago de rescate para su liberación[13].

UTM: Gestión Unificada de Amenazas, UTM, por sus siglas en inglés (Unified Threat management) es un software o hardware del tipo firewall diseñado para unificar diversas funciones de seguridad como proxy, filtro de paquetes, sistema de detección y prevención de intrusos, protección anti malware, regular el tráfico de redes, entre otros[14].

VULNERABILIDAD: Debilidad en un componente que compromete potencialmente la confidencialidad, integridad, disponibilidad, control de acceso y consistencia del activo informático en el que se encuentre. Puede estar presente en un equipo físico, un software o incluso en procedimientos, ofreciendo al atacante una fuente de acceso no permitido[15].

---

[12] Edson Denis Zanabria Ticona y Edwin Cayo Mamani, «Seguridad informática en dispositivos móviles con Sistemas Operativos Android mediante Pentesting», *Universidad Nacional del Altiplano*, 13 de abril de 2018, http://repositorio.unap.edu.pe/handle/UNAP/7047.

[13] Santiago Trigo et al., «Ransomware: seguridad, investigación y tareas forenses», 2017, http://hdl.handle.net/10915/65216.

[14] Pichucho Bombón y Jorge Aníbal, «ELABORACIÓN DE UN MÓDULO PARA PRÁCTICAS DE LABORATORIO DE GESTIÓN UNIFICADA DE AMENAZAS EN LA UNIVERSIDAD ISRAEL», 2017, https://repositorio.uisrael.edu.ec/handle/47000/1401.

[15] Francisco Nicolás Solarte Solarte, Edgar Rodrigo Enriquez Rosero, y Mirian del Carmen Benavides, «Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001», *Revista Tecnológica - ESPOL* 28, n.º 5 (31 de diciembre de 2015), http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456.

INTRODUCCIÓN

El ser humano ha tenido siempre la necesidad de registrar sus progresos, sus fallas, y de llevar un control contable de las cosas que posee; en la medida que ha evolucionado la humanidad han evolucionado las técnicas y herramientas que utiliza para este fin, pasando por el ábaco, la máquina calculadora de latón, la Pascalina, la máquina analítica de Babbage, la ABC (Atanasoff Berry Computer), la EDVAC (Electronic Discrete Variable Automatic Computer)[16], hasta llegar a la computación moderna. Sin embargo, nada ha impulsado con tanta fuerza el desarrollo de la computación, ni ha cambiado tanto la forma en la que las personas resguardan y comparten la información, como con la aparición en 1990 del *World Wide Web*, diseñado por Tim Berners-Lee y Roger Cailliau[17].

Con cada paso que da la tecnología más se adhiere a nuestra vida diaria y a la de las organizaciones bien sean públicas o privadas, más relevancia cobra la información que allí se almacena, y más riesgos surgen a nivel computacional. Robos de información confidencial de empresas o personas, robos de claves, compras y movimientos monetarios sin la autorización de los dueños, pérdidas millonarias y extorciones.

Es así como se han venido identificando casos que ponen en riesgo esta tendencia tecnológica, como son los casos vistos en el 2014 cuando se registró uno de los ataques cibernéticos más grandes de la historia, en el cual se robaron más de 500 millones de cuentas en las que se incluían datos de nombres,

[16] R Martínez y A García-Beltrán, «BREVE HISTORIA DE LA INFORMÁTICA», s. f., 20.
[17] Martínez y García-Beltrán.

direcciones, preguntas de seguridad y teléfonos[18]. Pero no sólo son las grandes compañías, de países del "primer mundo" las víctimas de los ataques cibernéticos. En el año 2009, en Colombia, se registró el robo de identidades bancarias y transacciones ilegales que llegaron hasta los 50 millones de pesos[19]. Según la empresa Symantec destaca que, en Venezuela, durante el 2013, el 23% de las computadoras analizadas estaban infectados por malware[20].

Afortunadamente las organizaciones y los gobiernos son cada vez más conscientes de los riesgos a los que está expuesta la información y los servicios que almacenan en los sistemas de información, así que buscan personas especializadas en seguridad informática. Estos individuos o empresas enfocadas en la seguridad informática se encargan de identificar, proponer y aplicar controles sobre las vulnerabilidades que potencialmente permitan ataques a la infraestructura tecnológica de la organización con el fin de extraer de manera ilegal información clasificada o de anular o afectar los servicios ofrecidos.

Hoy en día es imposible que una empresa mediana o grande pueda existir sin el uso de las tecnologías de la información, bien sea a nivel administrativo o comunicacional. Por esto es que es importante que cada organización cuente con personas especializadas en el manejo de dichas tecnologías y sepa administrar y capacitar sobre la administración de los activos informáticos que la organización vaya generando, alimentando o desechando, teniendo en cuenta los riesgos latentes en cada una de estas acciones. Si bien ningún sistema puede ser 100%

[18] Jorge Izaguirre Olmedo y Fernando León Gavilánez, «Análisis de los Ciberataques realizados en América Latina.», *INNOVA Research Journal* 3, n.º 9 (2018): 180-89.

[19] Riveros Cardenas y Fredy Orlando, «Administración del riesgo cibernetico un enfoque desde la alta gerencia empresarial en Colombia», *observatorio de la ciberseguridad para america latina y el caribe. (10 de enero de 2016). observatorio de ciberseguridad. organizacion de estados americanos: banco interamericano de desarrollo. Obtenido de observatorio de ciberseguridad .*, 31 de enero de 2017, http://repository.unimilitar.edu.co/handle/10654/15837.

[20] Juan Antonio Rodríguez, Jesús Oduber, y Endira Mora, «Actividades rutinarias y cibervictimización en Venezuela», *URVIO: Revista Latinoamericana de Estudios de Seguridad*, n.º 20 (2017): 63-79.

seguro, es importante minimizar al máximo el impacto si alguno de los sistemas informáticos se ve afectado, es más, un enfoque bastante acertado es el propuesto por Cano (2004)[21] en el que, complementario al análisis en seguridad informática de causas y efectos sobre los riesgos latentes en los activos informáticos, se propone un análisis de la inseguridad informática de la infraestructura tecnológica de la organización, pensando como lo haría un cracker y dificultar al máximo su objetivo de ingresar al sistema de manera ilegal y de vulnerar los mecanismos de protección.

Por medio del caso de estudio de la Empresa NOSTRADAMUS S.A.S., se realizará una exploración práctica para identificar y evaluar algunos de los ataques cibernéticos más comunes: la ingeniería social, la elevación de privilegios, la denegación de servicio, los ransomware y la inyección SQL en aplicativos web.

[21] Jeimy J. Cano, «Inseguridad informática: un concepto dual en seguridad informática.», *Revista de Ingeniería* 0, n.º 19 (2004): 40-44-44, https://doi.org/10.16924/riua.v0i19.437.

1 PROBLEMA DE INVESTIGACIÓN

1.1 ANTECEDENTES DEL PROBLEMA

Durante el 2017 el ransomware denominado “WannaCry” afectó a nivel mundial más de 15 millones de equipos, y se estima que podría haber provocado una perdida aproximada de 200 millones de euros[22].

Durante el año 2013 en Colombia 6 millones de personas fueron víctimas de alguna modalidad de crimen digital y en total se acumularon hasta 874 mil millones de pesos en pérdidas[23]. El crimen más relevante en dicho año fue el robo de identidades digitales y datos bancarios, incluyendo en esta lista de víctimas las cuentas de correo electrónico del presidente Santos[24]. En el 2014 se reportaron más de 801 ataques a páginas web, entre portales comerciales, sitios web educativos y sitios web de entidades[25]. Según Symantec, en el 2017 Colombia ocupó el sexto país con mayor número de ciberataques de América Latina[26].

Las organizaciones están propensas a sufrir fallos en los sistemas informáticos, bien sea ocasionados por fallas naturales, ataques externos o deterioro en los sistemas o equipos. Esto puede generar como consecuencia la parálisis parcial o completa de los servicios o la perdida, suplantación o afectación de información

[22] Ferrando Guillem y Anna Lourdes, «La ciberseguridad como reto internacional: la protección frente a las ciberamenazas», diciembre de 2018, http://openaccess.uoc.edu/webapps/o2/handle/10609/88685.
[23] Hoyos Buiron y Victor Antonio, «¿Que tal esta Colombia en cuestion de ciberseguridad?», 28 de enero de 2016, http://repository.unimilitar.edu.co/handle/10654/7794.
[24] Buiron y Antonio.
[25] Rodrigo Cortés Borrero, «Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia», *instname:Universidad Santo Tomás*, 2015, http://repository.usta.edu.co/handle/11634/14032.
[26] El Colombiano, «Colombia, el sexto país con más ciberataques en 2017», www.elcolombiano.com, accedido 18 de abril de 2019, https://www.elcolombiano.com/colombia/ciberataques-en-colombia-sexto-pais-mas-vulnerable-en-la-region-AB8535174.

importante para la organización o para los usuarios, internos y externos de esta. Cuando una organización no está preparada intelectual y físicamente para asumir estos sucesos adversos, es porque no tiene planteado un buen sistema de gestión de la seguridad de la información.

1.2 PLANTEAMIENTO DEL PROBLEMA

En el caso de estudio, la empresa NOSTRADAMUS S.A.S. ha sido víctima de una serie de ataques a sus sistemas, entre los que se destacan la elevación de privilegios, la presencia de ransomware y la inyección de SQL en el aplicativo web de la entidad. Esto evidencia debilidades en la seguridad informática de la empresa, ítem que debe asumirse de manera planificada y racional para que los mecanismos de protección sean eficaces.

A partir de los hallazgos en la exploración práctica de las vulnerabilidades y la identificación de los activos de información de NOSTRADAMUS S.A.S., se propondrá una serie de documentos base para la posterior implementación de un Sistema de Gestión de la Seguridad Informática.

1.3 FORMULACIÓN DEL PROBLEMA

¿Cómo el aseguramiento a la seguridad informática permite disminuir los riesgos presentados en la infraestructura tecnológica del caso de estudio Empresa NOSTRADAMUS S.A.S y como podría ser un sistema de seguridad de la información adecuado para dicha empresa?

2 JUSTIFICACIÓN

En la actualidad existen cada vez más individuos especializados en aprovechar las herramientas disponibles en internet para introducirse de manera no autorizada en los sistemas de otras personas u organizaciones. Algunos lo hacen como un reto personal o con un fin educativo, sin embargo, la gran mayoría lo hacen con la intención de sacar un provecho económico o el deseo de perjudicar a una persona u organización, de allí la diferencia entre hackers y crackers[27].

El caso de estudio de NOSTRADAMUS S.A.S permite identificar las vulnerabilidades que facilitan algunos de los principales ataques a la seguridad informática, como la elevación de privilegio, la denegación de servicios, los ransomware y la inyección SQL en aplicativos web. Basado en este insumo, se explorarán las mejores alternativas para el aseguramiento de la infraestructura tecnológica de la empresa a través de la definición de un sistema de seguridad para la información. Teniendo este insumo y la evaluación de los activos de información se resalta la importancia que tiene la implementación de un sistema de gestión de la información (SGSI) en cualquier empresa, sin importar su naturaleza o tamaño.

[27] David Dittrich y Kenneth E. Himma, «Hackers, crackers, and computer criminals», *Handbook of Information Security. Bakersfield, CA: California State University*, 2006, 154-72.

3 OBJETIVOS

3.1 OBJETIVO GENERAL

Analizar desde un enfoque técnico los ataques a los sistemas de información registrados en el caso de estudio NOSTRADAMUS S.A.S, con el fin de plantear, desde un enfoque administrativo, un proyecto de diseño para la posterior implementación de un sistema de gestión para la seguridad de la información, basado en la norma ISO 27001, para dicha empresa.

3.2 OBJETIVOS ESPECÍFICOS

- Implementar un laboratorio con máquinas virtuales que permita ejecutar ataques y defensas cibernéticas (pentesting) con el fin de replicar los ataques registrados en el caso de estudio NOSTRADAMUS S.A.S

- Establecer, a partir de los resultados obtenidos en el laboratorio de pentesting, una propuesta estratégica para la mitigación del riesgo de futuros ataques, en el que se incluyan monitoreo de red y análisis de un UTM.

- Plantear un diseño de proyecto para la posterior implementación de un SGSI, basado en la norma ISO 27001, en el que se incluyan los objetivos de la seguridad de la información, la metodología que se propone utilizar y el alcance del sistema.

- Realizar un análisis de gestión de riesgos a todos los procesos involucrados de NOSTRADAMUS S.A.S. y establecer un control interno de seguridad de la información.

4 MARCO DE REFERENCIA

4.1 MARCO TEÓRICO

Hoy día la información es uno de los bienes más preciados y de mayor importancia para las organizaciones y la forma más efectiva de almacenarla es por medio de las tecnologías de la información. Sin embargo, esto conlleva una serie de riesgos informáticos de los que las organizaciones deben estar conscientes para poder coexistir con ellos de manera controlada. Por ello es que la seguridad de la información ha tomado un papel relevante al interior de las organizaciones, sin importar el tamaño de esta.

La seguridad informática es *"un conjunto de medidas de prevención, detección y corrección, orientadas a proteger la confidencialidad, integridad y disponibilidad de los activos de información"*[28]. Un sistema se considere seguro cuando puede garantizar estos tres principios.

En este trabajo se exploran dos enfoques a través de los cuales se busca evaluar y fortalecer tanto la seguridad informática como la seguridad de la información de la empresa de estudio NOSTRADAMUS S.A.S. La primera es un enfoque técnico en el que se montará un laboratorio de pentesting para identificar las vulnerabilidades que permitan poner en riesgo la infraestructura tecnológica de NOSTRADAMUS; el segundo enfoque es administrativo y consta de evaluar y proponer un proyecto de diseño para la posterior implementación de un Sistema de gestión de la seguridad de la información de dicha empresa.

[28] Jara y Pacheco, *Ethical Hacking 2.0*.

En el enfoque técnico se aplica un procedimiento ordenado que permite la simulación de los ataques registrados en el caso de estudio NOSTRADAMUS S.AS., para ellos se utilizan herramientas y procedimientos de hacking en un entorno controlado. Sobre las pruebas de pentesting Florentino (2016) indica que[29]:

> *Las pruebas de penetración no se consideran ni auditorías informáticas, ni análisis de riesgos, pues no se evalúa la alineación de la seguridad a determinados estándares y tampoco se evalúa el nivel de impacto que ciertas amenazas pueden causar a los activos (datos) de una organización. Las pruebas de penetración emulan un ataque real a un sistema informático, estos ataques se realizan utilizando una serie de técnicas, herramientas y una metodología dividida en fases de: reconocimiento, escaneo, enumeración, acceso y la generación de reportes.*

Sin embargo, la evaluación de vulnerabilidades a través de pentesting es una práctica muy útil para entender las técnicas de los crackers y así reducir al mínimo el número de vulnerabilidades y aumentar al máximo la dificultad de lograr un ataque exitoso. Son varios los trabajos enfocados en la implementación de laboratorios de pentesting. En el laboratorio de Florentino (2016)[30], se utilizaron una serie de máquinas virtuales montadas en Virtual Box y, como centro de monitoreo y pentesting, una máquina instalada con Kali Linux. Se realizaron siete tipos de ataques a varias aplicaciones y servicios de red: un ataque de fuerza bruta, un ataque al servidor Samba, una inserción XSS (Cross Site Scripting), un

[29] Florentino Mendez Gijon et al., «Técnicas de Hacking Ético en un Laboratorio de Pentesting Virtualizado», 2011, https://www.researchgate.net/profile/Armando_Ronquillo/publication/308312418_Tecnicas_de_Hacking_Etico_en_un_Laboratorio_de_Pentesting_Virtualizado/links/57e04ed608aece48e9e1f4b4/Tecnicas-de-Hacking-Etico-en-un-Laboratorio-de-Pentesting-Virtualizado.pdf.
[30] Gijon et al.

ataque tipo Man in the Middle (MITM), una inserción de SQL y una denegación de servicio por puerto 80.

Otro trabajo destacable de pentesting fue el elaborado por Caridad (2014)[31], en el que, teniendo como objetivo los sistemas informativos de la Universidad Central Marta Abreu de las Villas, realizó una serie de pruebas sistemáticas de penetración, entre las que se incluía el análisis de vulnerabilidad de los sitios web, especialmente los montados sobre los administradores de contenidos Wordpress y Joomla, los ataques de ingeniería social, ataques de MITM, SSL strip (ataques a nivel de servidor) y ataques de denegación de servicios.

Desde el enfoque administrativo de este trabajo, se aborda el caso de estudio NOSTRADAMUS S.A.S. con el desarrollo de un proyecto de diseño para la posterior implementación de un Sistema de gestión de la seguridad de la información (SGSI). Existen muchos escritos sobre la implementación del SGSI en diferentes empresas, todas de tamaños, fines y nacionalidades diferentes[32]

El propósito del SGSI es establecer mecanismos de gestión para proteger la confidencialidad, integridad y disponibilidad de la información según estándares para evaluar la seguridad, como la ISO 27001.

[31] Blanco y Caridad, «Pruebas de penetración con la herramienta Kali Linux en la Universidad Central Marta Abreu de las Villas».

[32] Villacís Espinosa y Miguel Leopoldo, «Diseño de un sistema de gestión de la seguridad de la información (SGSI) basado en la norma ISO 27001:2013 para la red corporativa de la empresa Ecuatronix.», febrero de 2016, http://dspace.ups.edu.ec/handle/123456789/12406; Aliaga Flores y Luis Carlos, «Diseño de un sistema de gestión de seguridad de información para un instituto educativo», *Pontificia Universidad Católica del Perú*, 2 de septiembre de 2013, http://tesis.pucp.edu.pe/repositorio//handle/20.500.12404/4721; Arlenys Carolina Nieves, «Diseño de un sistema de gestión de la seguridad de la información (SGSI) basados en la norma Iso/iec 27001:2013», 4 de agosto de 2017, http://alejandria.poligran.edu.co/handle/10823/994.

Se deben comprender los principios básicos de la seguridad informática[33]. La integridad es la característica que indica que un dato, o conjunto de datos, no ha sufrido alteración o ha sido destruido sin autorización del propietario; la confidencialidad es cuando un dato es de conocimiento solo de las personas, entidades o mecanismos autorizados, de la manera autorizada y en el momento autorizado. La disponibilidad es la capacidad del sistema de información para acceder a un dato en un momento, lugar y forma en que lo requiere el usuario autorizado.

Con el fin de mantener estas características de la información, el SGSI se enfoca en identificar los activos y personas que infieren en los sistemas informáticos mediante la gestión de riesgos asociados a los procesos. Así mismo, se enfoca en verificar los controles de seguridad que permitan mitigar los riesgos encontrados.

Existen cuatro formas tradicionales de asumir los riesgos: establecer controles para mitigarlos, aceptar el riesgo ya que es imposible mitigarlo, eliminar el riesgo quitando los procesos del negocio que lo generan, o trasladarlo a un tercero, como una aseguradora[34]. Todas estas decisiones pueden impactar los recursos o incluso el quehacer mismo de la organización. Es por ello que el gobierno de TI dentro de la compañía se convierte en una pieza fundamental para asegurar el éxito y la pertinencia de las estrategias que se definan. Una organización que no le dé la relevancia suficiente a la mitigación de riesgos tecnológicos se está exponiendo a situaciones en las que no solo los sistemas, sino todas las áreas de la compañía pueden verse afectadas. Para tal fin, se han creado en el transcurso de los años estándares para el análisis y la gestión de los riesgos, también conocidos como Marcos de trabajo o Frameworks.

---

[33] Ciro Antonio Dussán Clavijo, «Políticas de seguridad informática», *Entramado* 2, n.º 1 (1 de junio de 2006): 86-92.

[34] Ricardo Gómez et al., «Metodología y gobierno de la gestión de riesgos de tecnologías de la información», *Revista de Ingeniería* 0, n.º 31 (23 de agosto de 2010): 109-118-118, https://doi.org/10.16924/riua.v0i31.217.

Algunos de los marcos de trabajo más conocidos son NIST, Octave, Magerit, EBIOS, CRAMM, Mehari, ISO entre otros. El objetivo de estos es el de establecer de manera sistemática y ordenada buenas prácticas mundialmente aceptadas, orientadas al análisis de riesgos y a la implementación de sistemas de gestión de riesgos.

NIST SP 800:30SP 800:30: Estándar desarrollado el NIST (Instituto Nacional de Estándares y Tecnología), especialmente diseñado para la evaluación de riesgos de seguridad de la información en sistemas TI. Cuenta con nueve fases: la caracterización del sistema, la identificación de las amenazas, la identificación de vulnerabilidades, el análisis de controles, la determinación de probabilidades, el análisis del impacto, la evaluación del riesgo y la documentación del resultado[35].

OCTAVE Allegro: Metodología desarrollada por SEI (Software Engineering Institute) que busca equilibrar los riesgos operativos, las prácticas de seguridad y la tecnología para que las organizaciones puedan tomar decisiones enfocadas a la seguridad informática. Se proponen 8 pasos para el análisis de riesgos: primero establecer criterios de medición del riesgo, a continuación, desarrollar un perfil de activos de información, identificar contenedores de activos de información, identificar áreas de preocupación, identificar escenarios de amenaza, identificar riesgos (Riesgo = Amenaza (condición) + Impacto (consecuencia)), analizar riesgos y, por último, seleccionar un enfoque de mitigación[36].

MAGERIT: Metodología elaborada por el Consejo Superior de Administración Electrónica con el fin de garantizar la autenticidad, confidencialidad, disponibilidad,

[35] «Análisis de riesgos en seguridad de la información | Ciencia, Innovación y Tecnología», accedido 19 de abril de 2019, https://www.jdc.edu.co/revistas/index.php/rciyt/article/view/121.
[36] Gómez et al., «Metodología y gobierno de la gestión de riesgos de tecnologías de la información».

trazabilidad e integridad de los activos informáticos de la organización. Define en 3 libros el proceso para el análisis de riesgos, en el primero describe la estructura adecuada para un modelo de gestión de riesgos, en el segundo establece una serie de enfoques para el análisis de riesgos y en el último presenta guías de trabajo para tal fin. MAGERIT se enfoca especialmente en conocer el estado de seguridad de los sistemas de información para implementar medidas de seguridad, buscando que no queden elementos por fuera para mitigar vulnerabilidades. Esta es una de las metodologías más utilizadas en las organizaciones[37].

EBIOS: Creada por la DCSSI (Dirección Central de Seguridad de los sistemas de información de Francia), esta es una metodología enfocada en la gestión del riesgo y en la comunicación entre clientes externos e internos para facilitar el reconocimiento de activos informáticos, actividades de seguridad y necesidades de seguridad, gracias a la identificación preventiva de vulnerabilidades y amenazas. Es una metodología enfocada en establecer buenas prácticas, apoyándose en los estándares internacionales definidos por la ISO[38].

4.2 MARCO CONCEPTUAL

Seguridad informática

Metodologías, procesos y procedimientos establecidos para proteger la información y los datos confidenciales de una organización dentro de sistemas informáticos, estableciendo para dicho fin procesos definidos por estándares, normas y protocolos enfocados en la infraestructura tecnológica. En otras palabras, es el conjunto de medidas que se deben tomar para prevenir, detectar y

[37] «Análisis de riesgos en seguridad de la información | Ciencia, Innovación y Tecnología».
[38] «Análisis de riesgos en seguridad de la información | Ciencia, Innovación y Tecnología».

corregir posibles problemas que puedan afectar la integridad, confidencialidad y disponibilidad de los recursos informáticos[39].

Seguridad de la información

Son las medidas preventivas establecidas para proteger la información, su confidencialidad, disponibilidad e integridad. Ya que la información puede almacenarse en distintos formatos, tanto físicos, como electrónicos, las organizaciones deben hacer uso de metodologías especializadas tanto para proteger los archivos y registros, como para mantenerlos en funcionamiento. La seguridad de la información también busca definir una infraestructura tecnológica idónea para custodiar y proteger la información[40]. No se trata sólo de un tema técnico, la seguridad de la información involucra procesos del negocio y políticas de la organización que aseguren la continua gestión de los riesgos y el aseguramiento de los niveles de seguridad requeridos por la organización.

Estándares ISO/IEC 27001

Estas son normas específicas para la gestión de la seguridad de la información y pueden ser aplicadas a cualquier organización, sin importar su actividad o tamaño. Establecen cuales son los requerimientos que debe cumplir un SGSI para ser implementado, desarrollado, monitoreado y mejorado. La ISO 27001 también define los requerimientos que deben cumplir los controles de seguridad de una organización, bien sea en un proceso especifico, un servicio, o cualquiera sea el alcance definido en el SGSI. Al ser de carácter internacional ofrece una

[39] Víctor Daniel Gil Vera y Juan Carlos Gil Vera, «Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas», *Scientia Et Technica* 22, n.º 2 (2017), http://www.redalyc.org/resumen.oa?id=84953103011.

[40] Zanabria Ticona y Cayo Mamani, «Seguridad informática en dispositivos móviles con Sistemas Operativos Android mediante Pentesting».

certificación para aquellas organizaciones que cumplan con los lineamientos establecidos, la cual es válida en muchos países[41].

El estándar ISO/IEC 27001 se puede dividir en dos secciones[42]: La primera especifica cinco cláusulas enfocadas en la metodología del SGSI (4. SGSI, 5. Responsabilidad de la dirección, 6. Auditorías Internas, 7. Revisión de la Dirección y 8. Mejora continua del SGSI) que son de obligatorio cumplimiento si la organización quiere aspirar a la certificación de su sistema.

En la segunda se definen los controles para la gestión de la seguridad de la información, asociados al Anexo A de la norma ISO/IEC 27001. Estos son:

Tabla 1. Cuadro de dominios, objetivos y controles de la ISO/IEC 27002:2013

Dominios	Objetivos	Controles
5. POLÍTICAS DE SEGURIDAD	5.1 Directrices de la Dirección en seguridad de la información.	5.1.1 Conjunto de políticas para la seguridad de la información. 5.1.2 Revisión de las políticas para la seguridad de la información
6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMACIÓN	6.1 Organización interna	6.1.1 Asignación de responsabilidades para la segur. de la información. 6.1.2 Segregación de tareas. 6.1.3 Contacto con las autoridades. 6.1.4 Contacto con grupos de interés especial. 6.1.5 Seguridad de la información en la gestión de proyectos

[41] Solarte, Rosero, y Benavides, «Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001».
[42] Solarte, Rosero, y Benavides.

Tabla 2. Cuadro de dominios, objetivos y controles (continuación)

Dominios	Objetivos	Controles
	6.2 Dispositivos para movilidad y teletrabajo.	6.2.1 Política de uso de dispositivos para movilidad. 6.2.2 Teletrabajo.
7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.	7.1 Antes de la contratación.	7.1.1 Investigación de antecedentes. 7.1.2 Términos y condiciones de contratación.
	7.2 Durante la contratación.	7.2.1 Responsabilidades de gestión. 7.2.2 Concienciación, educación y capacitación en seguridad de la información 7.2.3 Proceso disciplinario.
	7.3 Cese o cambio de puesto de trabajo	7.3.1 Cese o cambio de puesto de trabajo.
8. GESTIÓN DE ACTIVOS	8.1 Responsabilidad sobre los activos.	8.1.1 Inventario de activos. 8.1.2 Propiedad de los activos. 8.1.3 Uso aceptable de los activos. 8.1.4 Devolución de activos.
	8.2 Clasificación de la información	8.2.1 Directrices de clasificación. 8.2.2 Etiquetado y manipulado de la información. 8.2.3 Manipulación de activos.
	8.3 Manejo de los soportes de almacenamiento.	8.3.1 Gestión de soportes extraíbles.

		8.3.2 Eliminación de soportes. 8.3.3 Soportes físicos en tránsito.

Tabla 3. Cuadro de dominios, objetivos y controles (continuación)

Dominios	Objetivos	Controles
9. CONTROL DE ACCESOS.	9.1 Requisitos de negocio para el control de accesos	9.1.1 Política de control de accesos. 9.1.2 Control de acceso a las redes y servicios asociados
	9.2 Gestión de acceso de usuario	9.2.1 Gestión de altas/bajas en el registro de usuarios. 9.2.2 Gestión de los derechos de acceso asignados a usuarios. 9.2.3 Gestión de los derechos de acceso con privilegios especiales. 9.2.4 Gestión de información confidencial de autenticación de usuarios. 9.2.5 Revisión de los derechos de acceso de los usuarios. 9.2.6 Retirada o adaptación de los derechos de acceso
	9.3 Responsabilidades del usuario.	9.3.1 Uso de información confidencial para la autenticación

Tabla 4. Cuadro de dominios, objetivos y controles (continuación)

Dominios	Objetivos	Controles
	9.4 Control de acceso a sistemas y aplicaciones.	9.4.1 Restricción del acceso a la información. 9.4.2 Procedimientos seguros de inicio de sesión. 9.4.3 Gestión de contraseñas de usuario. 9.4.4 Uso de herramientas de administración de sistemas. 9.4.5 Control de acceso al código fuente de los programas.
10. CIFRADO	10.1 Controles criptográficos	10.1.1 Política de uso de los controles criptográficos. 10.1.2 Gestión de claves
11. SEGURIDAD FÍSICA Y AMBIENTAL	11.1 Áreas seguras	11.1.1 Perímetro de seguridad física. 11.1.2 Controles físicos de entrada. 11.1.3 Seguridad de oficinas, despachos y recursos. 11.1.4 Protección contra las amenazas externas y ambientales. 11.1.5 El trabajo en áreas seguras. 11.1.6 Áreas de acceso público, carga y descarga

Tabla 5. Cuadro de dominios, objetivos y controles (continuación)

Dominios	Objetivos	Controles
	11.2 Seguridad de los equipos	11.2.1 Emplazamiento y protección de equipos. 11.2.2 Instalaciones de suministro. 11.2.3 Seguridad del cableado. 11.2.4 Mantenimiento de los equipos. 11.2.5 Salida de activos fuera de las dependencias de la empresa. 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones. 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento. 11.2.8 Equipo informático de usuario desatendido. 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla
12. SEGURIDAD EN LA OPERATIVA	12.1 Responsabilidades y procedimientos de operación	12.1.1 Documentación de procedimientos de operación. 12.1.2 Gestión de cambios. 12.1.3 Gestión de capacidades. 12.1.4 Separación de entornos de desarrollo, prueba y producción.
	12.2 Protección contra código malicioso.	12.2.1 Controles contra el código malicioso.
	12.3 Copias de seguridad.	12.3.1 Copias de seguridad de la información.

Tabla 6. Cuadro de dominios, objetivos y controles (continuación)

Dominios	Objetivos	Controles
	12.4 Registro de actividad y supervisión	12.4.1 Registro y gestión de eventos de actividad. 12.4.2 Protección de los registros de información. 12.4.3 Registros de actividad del administrador y operador del sistema. 12.4.4 Sincronización de relojes
	12.5 Control del software en explotación	12.5.1 Instalación del software en sistemas en producción.
	12.6 Gestión de la vulnerabilidad técnica.	12.6.1 Gestión de las vulnerabilidades técnicas. 12.6.2 Restricciones en la instalación de software
	12.7 Consideraciones de las auditorías de los sistemas de información.	12.7.1 Controles de auditoría de los sistemas de información.
13. SEGURIDAD EN LAS TELECOMUNICACIONES	13.1 Gestión de la seguridad en las redes.	13.1.1 Controles de red. 13.1.2 Mecanismos de seguridad asociados a servicios en red. 13.1.3 Segregación de redes
	13.2 Intercambio de información con partes externas.	13.2.1 Políticas y procedimientos de intercambio de información. 13.2.2 Acuerdos de intercambio. 13.2.3 Mensajería electrónica. 13.2.4 Acuerdos de confidencialidad y secreto.

Tabla 7. Cuadro de dominios, objetivos y controles (continuación)

Dominios	Objetivos	Controles
14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS	14.1 Requisitos de seguridad de los sistemas de información	14.1.1 Análisis y especificación de los requisitos de seguridad. 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas. 14.1.3 Protección de las transacciones por redes telemáticas.
	14.2 Seguridad en los procesos de desarrollo y soporte.	14.2.1 Política de desarrollo seguro de software. 14.2.2 Procedimientos de control de cambios en los sistemas. 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo. 14.2.4 Restricciones a los cambios en los paquetes de software. 14.2.5 Uso de principios de ingeniería en protección de sistemas. 14.2.6 Seguridad en entornos de desarrollo. 14.2.7 Externalización del desarrollo de software. 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas. 14.2.9 Pruebas de aceptación.

	14.3 Datos de prueba.	14.3.1 Protección de los datos utilizados en pruebas.

Tabla 8. Cuadro de dominios, objetivos y controles (continuación)

Dominios	Objetivos	Controles
15. RELACIONES CON SUMINISTRADORES	15.1 Seguridad de la información en las relaciones con suministradores.	15.1.1 Política de seguridad de la información para suministradores. 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores. 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
	15.2 Gestión de la prestación del servicio por suministradores	15.2.1 Supervisión y revisión de los servicios prestados por terceros. 15.2.2 Gestión de cambios en los servicios prestados por terceros
16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.	16.1 Gestión de incidentes de seguridad de la información y mejoras.	16.1.1 Responsabilidades y procedimientos. 16.1.2 Notificación de los eventos de seguridad de la información. 16.1.3 Notificación de puntos débiles de la seguridad. 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones. 16.1.5 Respuesta a los incidentes de seguridad. 16.1.6 Aprendizaje de los incidentes de seguridad de la información.

		16.1.7 Recopilación de evidencias.

Tabla 9. Cuadro de dominios, objetivos y controles (continuación)

Dominios	Objetivos	Controles
17. ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.	17.1 Continuidad de la seguridad de la información.	17.1.1 Planificación de la continuidad de la seguridad de la información. 17.1.2 Implantación de la continuidad de la seguridad de la información. 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
	17.2 Redundancias.	17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.
18. CUMPLIMIENTO	18.1 Cumplimiento de los requisitos legales y contractuales.	18.1.1 Identificación de la legislación aplicable. 18.1.2 Derechos de propiedad intelectual (DPI). 18.1.3 Protección de los registros de la organización. 18.1.4 Protección de datos y privacidad de la información personal. 18.1.5 Regulación de los controles criptográficos.
	18.2 Revisiones de la seguridad de la	18.2.1 Revisión independiente de la

	información.	seguridad de la información. 18.2.2 Cumplimiento de las políticas y normas de seguridad. 18.2.3 Comprobación del cumplimiento

Fuente: Anexo A de la norma ISO/IEC 27001

Para que se dé cumplimiento a la normativa, es vital que exista apoyo por parte de la dirección de la empresa, alineación entre los objetivos de seguridad y los objetivos de la organización, compatibilidad entre los controles y la cultura de la organización, participación activa de todos los involucrados, una correcta administración de los riesgos, canales de comunicación efectivos con los empleados, disposición de las políticas y procedimientos de seguridad y mecanismos de medición que permitan monitorear la efectividad del programa de seguridad de la información, así como de los controles y planes de tratamiento[43].

Pentesting

Un test de penetración, también conocido como pentesting, es una evaluación de seguridad informática ejecutada a una infraestructura tecnológica por medio de la simulación de un ataque. Para esto, se utilizan una serie de técnicas y softwares diseñados para poner a prueba la seguridad del sistema y así medir que tan bien reacciona ante dichos intentos de penetración. A este proceso también se le conoce como “hacking ético”[44]. Los pentesting permiten detectar tanto los niveles de seguridad interno y externo del sistema de información y medir el grado de acceso que tendría un cracker.

[43] Solarte, Rosero, y Benavides.
[44] Jara y Pacheco, *Ethical Hacking 2.0*.

Los servicios de pentesting permiten[45]:

- Evaluar e identificar vulnerabilidades que puedan ser explotadas
- Analizar y categorizar las debilidades explotables según su impacto y posibilidad de ocurrencia
- Proveer recomendaciones para la mitigación y eliminación de las debilidades.

Algunas de las metodologías de pentesting más populares son OSSTMM, OWASP e ISSAF.

4.3 MARCO LEGAL

Ha medida que las tecnologías aumentan su rango de cobertura e influencia en la vida cotidiana, también aumentan las herramientas y técnicas para usar las tecnologías de la información con fines delictivos. Esto es una preocupación a nivel mundial ya que afectan tanto la información privada de los individuos como la información confidencial de los estados e incluso el funcionamiento de los sistemas automatizados.

En el 2007 Estonia sufrió un grave ataque cibernético que afectó a la presidencia, la mayoría de los parlamentos de dicho país y dos grandes bancos. A partir de esto, la OTAN implementó el Centro de Excelencia para la Cooperación de Ciberdefensa (CCD), con el fin de proteger a los miembros de esta de dicho ataque. Sin embargo, se registraron dos grandes ataques que afectaron, en el 2009 a la Casa Blanca y el Departamento de Defensa de Estados Unidos, y otro en el 2010 que afectó la Guardia Civil española[46].

---

[45] Blanco y Caridad, «Pruebas de penetración con la herramienta Kali Linux en la Universidad Central Marta Abreu de las Villas».

[46] Jorge Eliécer Ojeda-Pérez et al., «Delitos informáticos y entorno jurídico vigente en Colombia», *Cuadernos de Contabilidad* 11, n.º 28 (1 de junio de 2010), https://revistas.javeriana.edu.co/index.php/cuacont/article/view/3176.

En Colombia la legislación para regular los delitos cibernéticos ha tenido la siguiente evolución cronológica[47].

Tabla 10. Leyes, resoluciones y circulares de Colombia

Ley / resolución circular	Tema
Ley 527 de 1999 - Comercio electrónico	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación y se dictan otras disposiciones"
Ley 599 de 2000	Por la cual se expide el Código Penal. En esta se mantuvo la estructura del tipo penal de "violación ilícita de comunicaciones", se creó el bien jurídico de los derechos de autor y se incorporaron algunas conductas relacionadas indirectamente con el delito informático, tales como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas. Se tipificó el "Acceso abusivo a un sistema informático", así: "Art. 195. El que abusivamente se introduzca en un sistema informático protegido con medida de seguridad o se mantenga contra la voluntad de quien tiene derecho a excluirlo, incurrirá en multa."
Ley 962 de 2005	Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos. Prevé el incentivo del uso de medios tecnológicos integrados para disminuir los tiempos y costos de realización de los trámites por parte de los administrados.
Ley 1150 de 2007	Por medio de la cual se introducen medidas para la

[47] Pedro Antonio Fula Perilla, «Lineamientos de política para ciberseguridad y ciberdefensa, documento CONPES 3701», 2016, http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2723/00003294.pdf?sequence=1.

	eficiencia y la transparencia en la Ley 80 de 1993 y se dictan otras disposiciones generales sobre la contratación con Recursos Públicos. Específicamente, se establece la posibilidad de que la administración pública expida actos administrativos y documentos y haga notificaciones por medios electrónicos, para lo cual prevé el desarrollo del Sistema Electrónico para la Contratación Pública, Secop.

Tabla 11. Leyes, resoluciones y circulares de Colombia (continuación)

Ley / resolución circular	Tema
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1341 de 2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la Información y las Comunicaciones – TIC, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.
Resolución de la Comisión de Regulación de Comunicaciones 2258 de 2009	Sobre seguridad de las redes de los proveedores de redes y servicios de telecomunicaciones. Esta resolución modifica los artículos 22 y 23 de la Resolución CRT 1732 de 2007 y los artículos 1,8 y 2,4 de la Resolución CRT 1740 de 2007. Esta regulación establece la obligación para los proveedores de redes y/o servicios de telecomunicaciones que ofrezcan acceso a Internet de implementar modelos de seguridad, de acuerdo con las características y necesidades propias de su red, que contribuyan a mejorar la seguridad de sus redes de acceso, de acuerdo con los marcos de seguridad definidos por la UIT, cumpliendo los principios de confidencialidad de datos, integridad de datos y disponibilidad de los elementos de red, la información, los servicios y las aplicaciones, así como medidas para autenticación, acceso y no repudio. Así mismo, establece

	obligaciones a cumplir por parte de los proveedores de redes y servicios de telecomunicaciones relacionadas con la inviolabilidad de las comunicaciones y la seguridad de la información

Tabla 12. Leyes, resoluciones y circulares de Colombia (continuación)

Ley / resolución circular	Tema
Circular 052 de 2007 (Superintendencia Financiera de Colombia	Fija los requerimientos mínimos de seguridad y calidad en el manejo de información a través de medios y canales de distribución de productos y servicios para clientes y usuarios.

Fuente: Pedro Antonio Fula Perilla, «Lineamientos de política para ciberseguridad y ciberdefensa, documento CONPES 3701», 2016, http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2723/00003294.pdf?sequence=1.

5 DISEÑO METODOLÓGICO

5.1 TIPO DE INVESTIGACIÓN

Proyecto aplicado

5.2 MÉTODO DE INVESTIGACIÓN

La metodología utilizada es de tipo investigación aplicada, ya que es el tipo de metodología que más se ajusta a este trabajo. Este tipo de investigación se considera una consulta no sistemática, enfocada en encontrar una solución a un problema inmediato al que se enfrenta una sociedad u organización, y por lo general la inicia una empresa, agencia o individuo con intereses particulares en la resolución del problema[48].

Si bien, en términos generales este trabajo se desarrolla a través del proceso de Recolectar información, Planificar, Ejecutar y Analizar[49], dichos pasos se ejecutan de manera especial para cada uno de los enfoques (el técnico y el administrativo) en los que se trabaja la seguridad informática y la seguridad de la información del caso de estudio NOSTRADAMUS S.A.S.

---

[48] Cesar Leonardo Almeida Coloma y Jasson Alfredo Pincay Párraga, «Implementación de un laboratorio de seguridad de informática para la realización de técnicas de ataque y defensa (Pentesting) en un ambiente real controlado, utilizando una distribución de Kali Linux dentro de la empresa industrial siderúrgica Andec S.A.» (Thesis, Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería En Networking y Telecomunicaciones, 2018), http://repositorio.ug.edu.ec/handle/redug/35450.

[49] Viver Ramirez y Aydee Mercedes, «Identificación de vulnerabilidades de la red LAN del Buque Oceanográfico de la autoridad Colombiana a través de las herramientas de pruebas de Pentesting.», 14 de junio de 2017, https://repository.unad.edu.co/bitstream/10596/12425/1/46646702.pdf.

5.2.1 Para el enfoque técnico

Paso 1 - Reconocimiento: Se debe estudiar el ambiente del objetivo y los rasgos generales del mismo antes del lanzar un ataque. Entre más información se consiga, más efectiva y rápida será la ruta para lograr un ataque exitoso[50]. Las *black boxtesting* (pruebas de caja negra) requieren más reconocimiento que las *white boxtesting* (pruebas de caja blanca) y los *gray boxtesting* (pruebas de caja gris, las cuales son una combinación de ambos), ya que se desconoce la información del sistema en el caso de las cajas negras, contrario a lo que pasa en los otros dos casos. Como objetivo del reconocimiento es el conocer datos importantes del destino del pentesting, como puertos de comunicación, dónde se encuentra alojado, que tipo de servicios ofrece a sus clientes, entre otros. Kali Linux ofrece todo un grupo de herramientas denominadas Gatheringthat que sirven para el proceso de reconocimiento[51].

Paso 2 - Evaluación del objetivo: Una vez realizado el reconocimiento, se pasa identificar las posibles vulnerabilidades o debilidades del objetivo. En este punto también se buscan los controles de seguridad existentes y la mejor manera de evadirlos. En Kali Linux existe una categoría de herramientas denominada Análisis de Vulnerabilidades[52].

Paso 3 - Explotación: Teniendo en cuenta las vulnerabilidades encontradas, se verifica si estas son o no reales y que tanto pueden aprovecharse. En esta fase se utilizan los exploits específicos para cada vulnerabilidad. Una buena práctica es identificar un grupo de vulnerabilidades y desarrollar una estrategia de ataque en

[50] Blanco y Caridad, «Pruebas de penetración con la herramienta Kali Linux en la Universidad Central Marta Abreu de las Villas».
[51] Blanco y Caridad.
[52] Blanco y Caridad.

torno a estos. Kali Linux cuenta con un catálogo de herramientas llamado Explotación Toolsfor[53].

Paso 4 - Análisis: Como resultado de las fases anteriores, se procederá a realizar un análisis de los resultados obtenidos para así realizar una propuesta de aseguramiento de la infraestructura tecnológica de NOSTRADAMUS S.A.S., con el fin de evitar futuros ataques como los evaluados.

5.2.2 Para el enfoque administrativo

Para el diseño de un Sistema de Gestión de la Seguridad de la Información (SGSI), la norma ISO 27001 adopta como metodología el ciclo de Deming, también conocido como ciclo de vida PHVA (Planear, Hacer, Verificar, Actuar) o, por sus siglas en ingles ciclo PDCA (Plan, Do, Check, Act). El concepto de PHVA nació a finales de los 70's por Edwards Deming, quien es considerado como el precursor del control de calidad moderno, y quien se basó en el método científico: hipótesis, experimentación y evaluación[54]. Además de ser una metodología ideal para este tipo de proyectos, es la recomendada por ISO.

En este proyecto se abarcará la fase del "Plan" del ciclo PHVA de acuerdo a 3 etapas:

Etapa 1 - Determinación de vulnerabilidades, amenazas y riesgos: Teniendo en cuenta el inventario de activos de información con el que cuenta la organización se estudian las vulnerabilidades, amenazas y riesgos que puedan

[53] Blanco y Caridad.
[54] Flores y Carlos, «Diseño de un sistema de gestión de seguridad de información para un instituto educativo».

presentarse a los procesos y sistemas implementados[55]. Es importante no confundir esta identificación de vulnerabilidades con el de la etapa técnica ya que en el proceso de elaboración del SGSI se tienen en cuenta además de los sistemas, la infraestructura física, el personal humano y los procesos relacionados al sistema de información de la empresa. Para recolectar información se aplican técnicas de observación directa mediante visitas programadas y entrevistas al personal encargado del área informática[56], sin embargo, dado que este es un caso de estudio, la evaluación de los activos se hará sobre el documento de descripción del caso.

Una vez levantada la información se describen las vulnerabilidades o debilidades encontradas, las amenazas por parte del personal interno o externo y los riesgos naturales y no naturales a los que está expuesta NOSTRADAMUS S.A.S. Adicionalmente se seleccionan los dominios y objetivos de control de la norma ISO/IEC 27001, que es la norma que se utilizará para la evaluación de la seguridad de la información.

Etapa 2 - Análisis de riesgos y diagnóstico de la seguridad de la información: En esta fase se realiza el análisis y evaluación de riesgos teniendo como referencia el estándar MAGERIT, el cual permite valorar los riesgos identificando posibles causas que los originan y que posteriormente permiten definir el sistema de control de seguridad más adecuado, con el fin de reducir la posibilidad de que vuelvan a ocurrir y mitigar el impacto en el caso que suceda.

[55] Solarte, Rosero, y Benavides, «Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001».
[56] Solarte, Rosero, y Benavides.

El análisis de riesgos propuesto por MAGERIT permite determinar los riesgos siguiendo los siguientes pasos[57]:

- Determinar los activos relevantes para la empresa
- Determinar las amenazas a las que están expuestos aquellos activos
- Estimar el impacto, definido como el daño sobre el activo, si se llega a concretar la amenaza
- Valorar dichos activos en función del coste que supondría para la empresa recuperarse ante un problema de disponibilidad, integridad o confidencialidad de información
- Valorar las amenazas potenciales
- Estimar el riesgo

Etapa 3 - Definición de controles para el diseño del SGSI que incluya políticas y procedimientos para mitigar los riesgos: En esta fase se definen los controles apropiados de acuerdo a la norma ISO/IEC 27001, se establece el tratamiento más apropiado para mitigar los riesgos y se diseñan las políticas y procedimientos que irán en el SGSI, el cual deberá estar ligado e implementado junto a los procesos de la organización.

5.3 FUENTES Y TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

5.3.1 Fuentes primarias

La primera fuente de información es la descripción del caso de estudio NOSTRADAMUS S.A.S. en la que se describe tanto el panorama de vulnerabilidades que deben ser revisadas en la infraestructura tecnológica de la organización, como el panorama administrativo de la información de dicha

[57] Carlos Ampuero Chang, «Diseño de un Sistema de Gestión de Seguridad de Información para una compañía de Seguros», 2011, https://core.ac.uk/download/pdf/71403748.pdf.

empresa, en el que se describen los activos de información y el estado general de su seguridad informática.

5.3.2 Fuentes secundarias

Se utilizarán resúmenes, compilaciones o listados de referencia sobre herramientas de pentesting para el análisis de vulnerabilidades y diseño de SGSI con el objetivo de mejorar la seguridad informática de NOSTRADAMUS S.A.S.

Así mismo, en especial para la etapa técnica de pentesting, se utilizarán referencias audiovisuales compartidas en Youtube, canal en el que se explorarán y seleccionarán técnicas de pentesting apropiadas para cumplir los objetivos de este trabajo.

5.4 DELIMITACIÓN Y ALCANCE

Con respecto al enfoque técnico, enfocado en la seguridad informática, el alcance del pentesting se define por medio de una reunión de alcance denominada Scoping Meeting, que tiene como objetivo definir claramente que será probado con el cliente y deja por fuera de dicho alcance (normalmente documentado en un contrato o documento de alcance) cualquier solicitud extra[58]. Sin embargo, al tratarse este trabajo de un caso de estudio, se establece únicamente dentro del alcance del pentest los ataques registrados en la solicitud de estudio:

- Ataque a sistemas operativos Windows 7 a través de navegadores web haciendo uso de técnicas de ingeniería social con metasploit

[58] Zafra y Luis, «Introducción al pentesting».

- Acceso indebido, Ataque de elevación de privilegios y robo de información a sistemas operativos Windows, dejando huella del uso de un .exe denominado lazange

- Denegación de servicio a la intranet de la empresa, alojada en un servidor con sistema operativo Windows (Se solicita simular a partir sistema operativo metasploitable)

- Ataque de Ransomware (Secuestro de información) utilizando la vulnerabilidad denominada eternalblue, la cual será explicada al detalle más adelante, al sistema operativo Windows que no contaban con el parche de seguridad MS17-010

- El Sitio web de NOSTRADAMUS S.A.S fue vulnerado posiblemente con un ataque de inyección de SQL. Para esta simulación se determinará cuál es el usuario y contraseña que se usó para realizar una posible elevación de privilegios. La dirección del sitio es: http://104.236.31.57/Test_SQLInj, facilitada por la Universidad Nacional Abierta y a Distancia para simular el portal web de NOSTRADAMUS S.A.S.

Con respecto al enfoque administrativo, enfocado en la seguridad de la información, se buscará establecer un proyecto de diseño para la posterior implementación de un SGSI, donde se incluyan algunos puntos esenciales, más no la elaboración e implementación del SGSI como tal. Dentro de los puntos tratados se resolverán las siguientes necesidades:

- Definir los objetivos de la seguridad de la información, planteando la planificación del proyecto y plasmando un registro de los posibles riesgos inherentes al proyecto.

- Determinar la metodología que va a tomar para la implementación del SGSI.

- Identificar y definir el alcance del sistema, considerando todos los activos de información de la organización.

- Identificar las necesidades básicas de seguridad del caso de estudio NOSTRADAMUS S.A.S.

- Realizar un análisis de gestión de riesgos a todos los procesos involucrados en el proyecto a partir de la metodología elegida, estableciendo el marco para la evaluación de riesgos.

- Establecer un control interno de seguridad de la información para el caso de estudio NOSTRADAMUS S.A.S., a partir del análisis de riesgos realizado.

6 DESARROLLO DE LA PROPUESTA

6.1 DESARROLLO OBJETIVO ESPECÍFICO 1- PENTESTING

A partir del punto 6.1.3, hasta el punto 6.1.7, se realizaron y documentaron los ataques comprendidos dentro de este pentesting. En este documento se mencionarán los principales hallazgos y la información complementaria que sea relevante para comprender la vulnerabilidad evidenciada; para ver el desarrollo del ataque a mayor detalle, remitirse al Anexo – Video Pentesting[59]. En cada uno de los numerales mencionados, se indicará el minuto y segundo (mm:ss) del video en el que se puede hallar cada uno de los ataques.

6.1.1 Montaje del laboratorio de pentesting

El objetivo de la configuración del ambiente de pruebas es proveer el hardware y software necesarios para realizar la ejecución de las pruebas de las aplicaciones en escenarios que cumplan con los requisitos necesarios para su funcionamiento normal con el fin de obtener resultados acertados[60].

A continuación, se describirán las características de la máquina anfitrión sobre las que se instalarán las dos máquinas virtuales que componen el laboratorio de pentesting:

- PC Intel Core 3.9 GHz
- Windows 7 Ultimate de 64 bytes
- 8 GB de RAM

---

[59] *Proyecto de grado - Alejandro Mejia Escobar*, accedido 14 de octubre de 2019, https://www.youtube.com/watch?v=6at_3GJ8Tvg&feature=youtu.be.

[60] Cadavid Romero y Diego Fernando, «Hallazgos de vulnerabilidades en los sistemas operativos y base de datos de la empresa ALDIM Acciones Logísticas en Distribución de Mercancías S.A.S.», 16 de marzo de 2018, http://repository.unad.edu.co/handle/10596/17412.

- Disco duro de 1 Terabyte

Las dos máquinas virtuales fueron instaladas en el software libre Oracle Virtual Box, tal como se evidencia en las figuras 1 y 2, con las siguientes características:

Figura 1. Máquina atacante - Kali Linux

Fuente: Autor

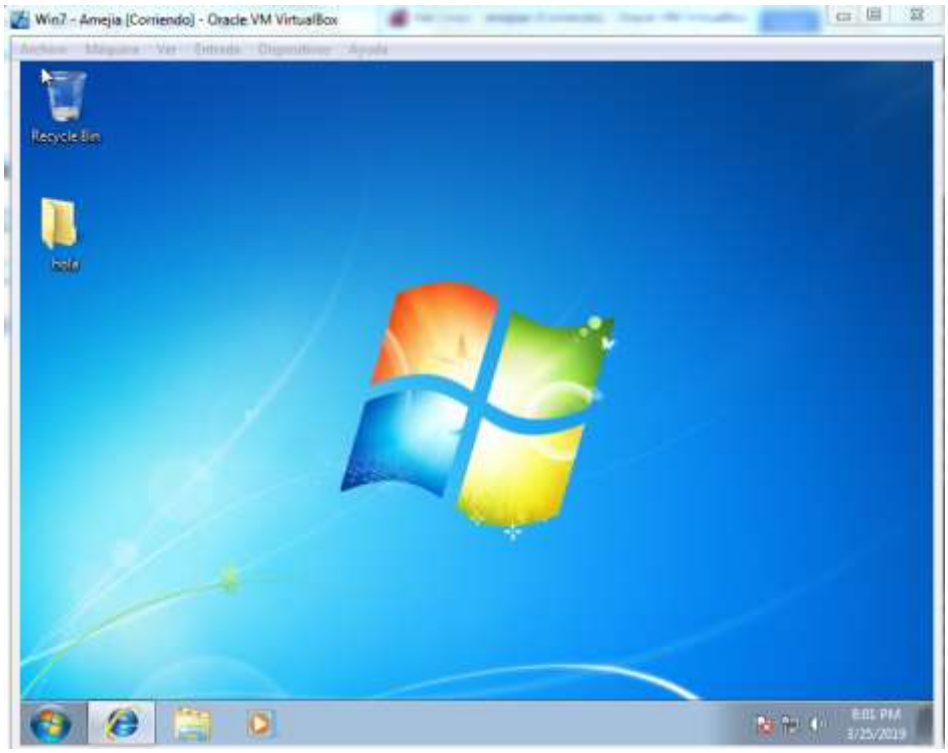
Máquina atacante:

- Linux
- Sistema operativo Debian - Kali Linux de 64 bytes
- 2 GB de RAM
- Disco duro tipo SATA de 80 Gigabytes

Luego de instalado el sistema Kali se actualiza la última versión de los paquetes mediante el comando `apt-get update && apt-get upgrade && apt-get`

`dist-upgrade`. De esta manera se garantiza que las herramientas de Kali Linux cuentan con las últimas actualizaciones para analizar vulnerabilidades y/o realizar ataques[61].

Figura 2. Máquina víctima - Windows 7



Fuente: Autor

Máquina víctima:

- Windows
- Windows 7 de 64 bytes
- 2 GB de RAM
- Disco duro tipo SATA de 32 Gigabytes

[61] Barrios y Enrique, «Análisis, explotación y definición de estrategias de mitigación de vulnerabilidades en un sistema GNU/Linux».

Ya que esta es la máquina víctima es importante evitar actualizaciones del sistema que puedan corregir vulnerabilidades explotables en el ejercicio de penetración.

6.1.2 Reconocimiento del sistema

Lo primero que debe hacerse es una evaluación del estado de la máquina víctima, los puertos que tiene abiertos y la demás información que se pueda conseguir de manera “externa”. Con este fin se utiliza la herramienta Nmap, usando el comando `nmap -sV`, lo cual permitirá obtener la información de los puertos abiertos en la máquina y la versión del sistema. A continuación, se presenta el resultado del escaneo con Nmap.

Figura 3. Resultado de Nmap

Fuente: Autor

6.1.3 Ataque por navegador web con ingeniería social[62]

Este ataque tiene dos partes, la ingeniería social y el exploit por navegador. La ingeniería social no se muestra en el video, pero basta con que se diseñe un mensaje llamativo en un email que invite a la víctima a ingresar a una URL que parece legitima para que el exploit pueda hacer lo suyo. En las siguientes imágenes se pueden apreciar dos ejemplos de mensaje llamativo fraudulento que pueden utilizarse para este tipo de ataque; el primero (figura 4) es de tipo económico, el segundo (figura 5) es de tipo legal.

Figura 4. Email promocional

Fuente: Google, criterio de búsqueda: Promociones Falabella

Figura 5. Email promocional

[62] Ver Anexo A – Video Pentesting, minuto 00:00.

FISCALÍA GENERAL DE LA NACIÓN

Bogota 31 de julio del 2018

estimado ciudadano:

Le enviamos esta notificación con el único objetivo de esclarecer los hechos que lo señalan por su presunta participación en las pasadas elecc
realizadas el ida **domingo 17 de junio de 2018**. en el cual usted es señalado por participar en las compras de votos y jurados elect

de esta manera es de carácter urgente su presentación recuerde que la no presentación a este llamado detonara una orden de captura en su c

adjunto los detalles donde deberá presentarse.

BOLETA DE CITACION
Nº 0008-2014

Sírvase comparecer ante la sede de esta Fiscalía Vigésima a Nivel Nacional con Competencia Plena, ubicada en la avenida Urdaneta, esquinas de animas a platanal, sede Ministerio Publico, piso 8, el día **Lunes 16 de Junio de 2014, a las 09:00 horas de la mañana,** en calidad de Testigo, en la causa penal identificada MP-127367-2014, por la presunta comisión de uno de los delitos establecidos en el Libro Segundo, Titulo I, Capitulo I del Código Penal, contra la independencia y seguridad de la nación, y uno de los delitos previstos en la Ley contra la Delincuencia Organizada y Financiamiento al Terrorismo (Asociación para Delinquir), donde fungen como investigados **PERSONAS POR IDENTIFICAR**.

La Fiscal,

KATHERINE NAYARITH HARINGHTON PADRON
FISCAL PROVISORIO VIGESIMA DEL MINISTERIO PÚBLICO
A NIVEL NACIONAL CON COMPETENCIA PLENA

KNHP/kh
F20NN-0005-2014/ MP-127367-14

RECIBIDO POR: Laura S de Acosta DIA: 4/06/14 HORA: 9:00PM
CI: 3981551

Dirección: Fiscalía Vigésima a Nivel Nacional con competencia plena , Caracas, Distrito Capital, Urbanización La Candelaria, Av. Urdaneta, esquinas de animas a platanal, edificio sede Ministerio Publico Piso 8
Teléfono-Fax: (58) (212) 408.6846 / 4086853

Asistente Legislativa de la Diputada Maria Corina Machad

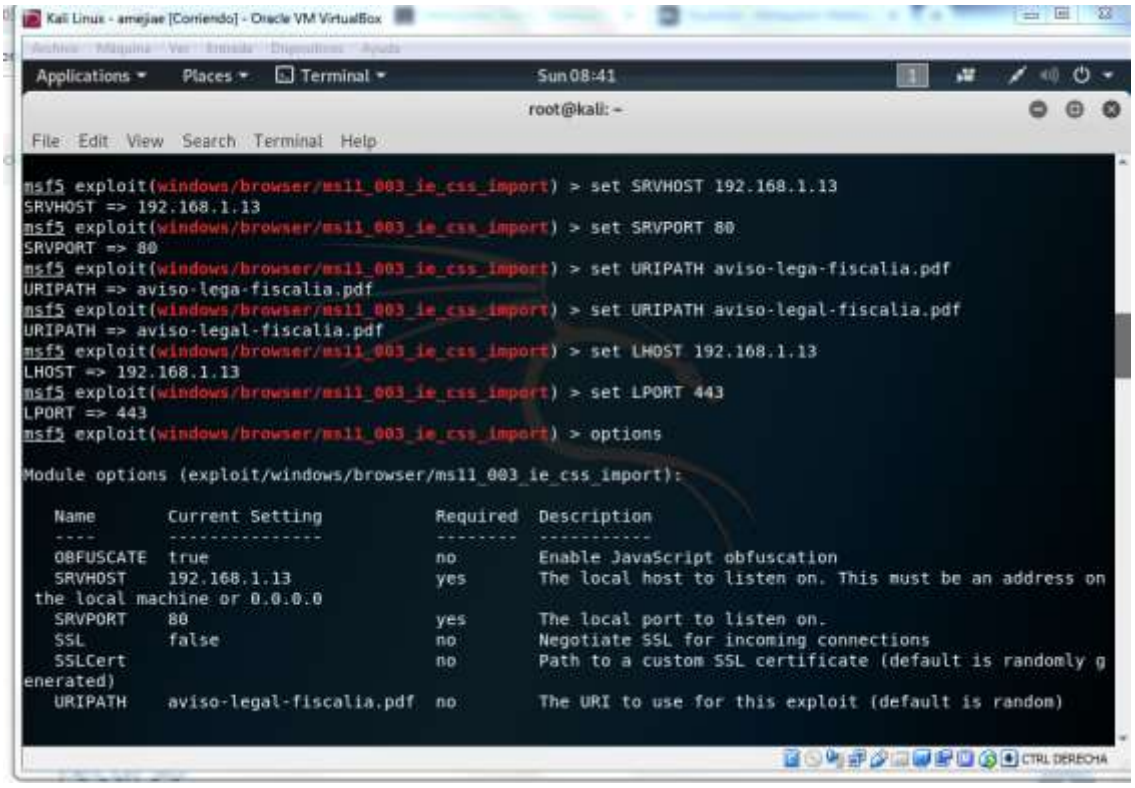
Fuente: Google, criterio de búsqueda: Avisos de la fiscalía

La segunda parte utiliza la herramienta Metasploit para preparar el exploit *ms11_003_ie_css_import*[63]. Este exploit aprovecha una vulnerabilidad de corrupción de memoria incluida en el motor HTML de Microsoft (mshtml). Ocurre cuando se mapea, o recorre una página web que realiza importaciones recursivas de CSS, donde un objeto en C++ es eliminado y posteriormente utilizado, lo que lleva a una referencia de puntero nulo. Este exploit funciona cuando la máquina objetivo tiene instalado .NET 2.0.50727 y las versiones del IE 6, 7 y 8 son vulnerables[64].

El ataque exitoso genera una sesión remota que permite la exploración completa del sistema e incluso su alteración, gracias al inicio de sesión en la máquina víctima con Meterpreter[65]. La figura a continuación refleja la configuración del exploit para ejecutar el ataque.

[63] Cyber Shield, *Exploit Internet Explorer 8 on win 7*, accedido 20 de abril de 2019, https://www.youtube.com/watch?v=h8xOnfQlxDE.
[64] «Exploiting MS11_003 Internet Explorer Vulnerability Using Metasploit Framework», accedido 28 de abril de 2019, https://www.hacking-tutorial.com/hacking-tutorial/exploiting-ms11_003-internet-explorer-vulnerability-using-metasploit-framework/#sthash.rIdwMmbq.dpbs.
[65] «Meterpreter Basic Commands», accedido 28 de abril de 2019, https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/.

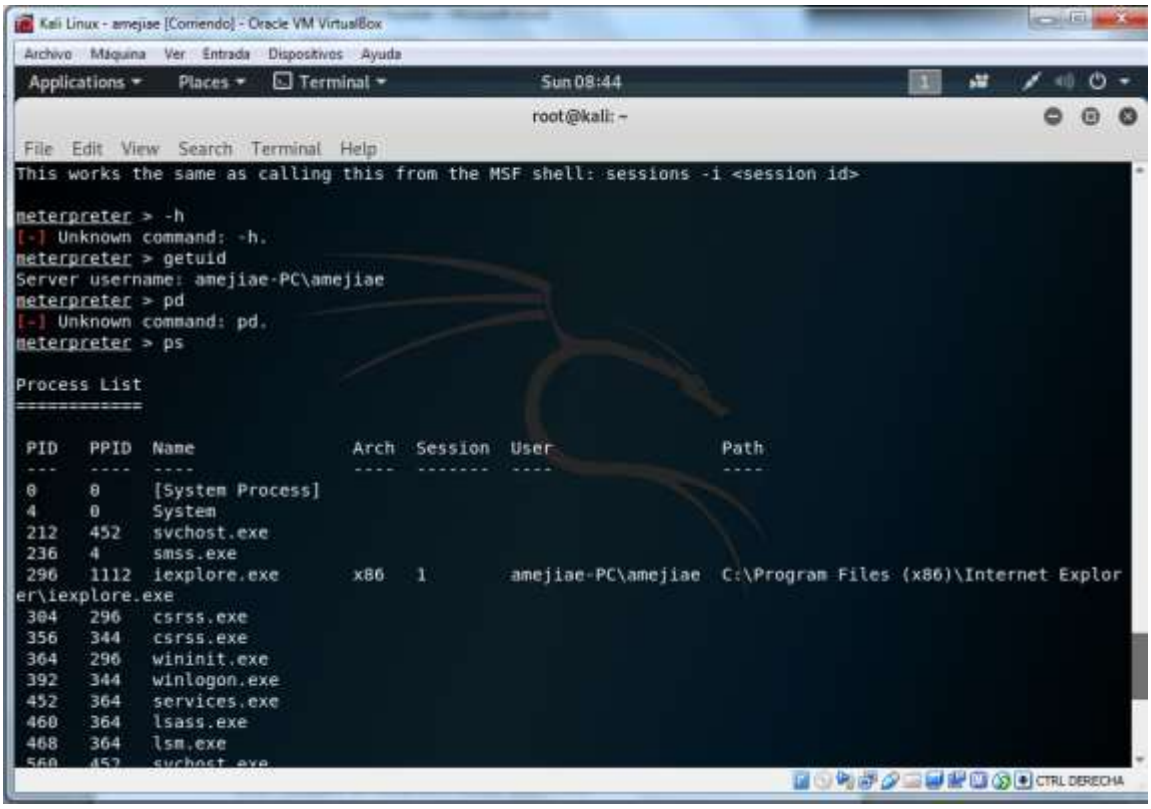
Figura 6. Configuración del exploit



Fuente: Autor

La figura a continuación es la sesión iniciada del Meterpreter, logrando así inicio de sesión remota y la extracción de información del sistema víctima.

Figura 7. Acceso exitoso a la máquina víctima



Fuente: Autor

6.1.4 Elevación de privilegios y acceso a contraseñas con lazange[66]

LaZagne es un programa en Phyton desarrollado con el objetivo de ayudar a los usuarios a recuperar contraseñas que hayan quedado almacenadas en los sistemas operativos Windows y Linux; especialmente permite descifrar claves almacenadas en GNOME y KDE, algo que sucede en Windows, cuando las contraseñas son almacenadas por el módulo LSA[67].

[66] Ver Anexo A – Video Pentesting, minuto 06:10.

[67] Adrián Crespo, «LaZagne, una utilidad que permite recuperar contraseñas de Windows y Linux», RedesZone, 28 de mayo de 2015, https://www.redeszone.net/2015/05/28/lazagne-una-utilidad-que-permite-recuperar-contrasenas-de-windows-y-linux/.

La manera en la que se puede utilizar LaZagne de manera remota[68] es aprovechando el acceso remoto logrado con la vulnerabilidad anterior (ver 6.1.3) y el exploit bypassuac[69], el cual logra emular el UAC (por sus siglas en inglés, User Access Control), el cual controla que sólo un usuario o programa autenticado como administrador pueda realizar ciertos cambios en el sistema operativo, como obtener hashes y contraseñas[70]. Una vez se inicia la sesión System, se podrá enviar a la máquina víctima el ejecutable LaZagne.exe, previamente descargado en la máquina Kali Linux. La imagen a continuación refleja el inicio exitoso del ataque LaZagne.

Figura 8. Claves reveladas por LaZagne

Fuente: Autor

[68] Vect0r, *LaZagne Get all Passwords on a Computer (Windows and Linux)*, accedido 28 de abril de 2019, https://www.youtube.com/watch?v=tyXFUBUeUDo.
[69] Raj Ch y el, «Múltiples formas de omitir UAC utilizando Metasploit», 16 de septiembre de 2018, //www.hackingarticles.in/multiple-ways-to-bypass-uac-using-metasploit/.
[70] «Escalar Privilegios en Windows Evadiendo UAC | Alonso Caballero / ReYDeS», accedido 28 de abril de 2019, http://www.reydes.com/d/?q=Escalar_Privilegios_en_Windows_Evadiendo_UAC.

Actualmente el sistema víctima no tiene configuradas ningunas claves, pero de tenerlas, LaZagne podría revelar las claves de chats, mails, SVN, database, entre otras (ver Figura 9)

Figura 9. Opciones de LaZagne

Fuente: Autor

6.1.5 Ataque de denegación de servicios a la intranet[71]

Como primer paso, se descarga e instala Xampp en la máquina de Windows, con el objetivo de configurar un servidor local para servicios web, también conocido como localhost, que sirva como intranet.

[71] Ver Anexo A – Video Pentesting, minuto 11:55.

Figura 10. Sitio disponible en máquina víctima

Fuente: Autor

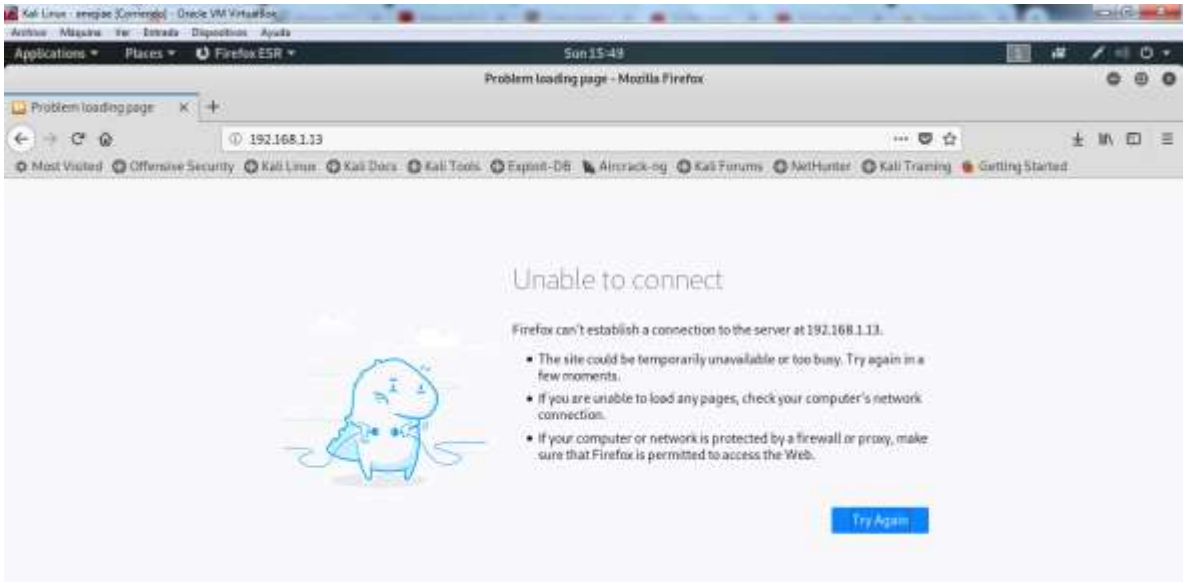
Una vez está disponible el sitio en Windows, y se verifica que existe conexión con él desde el servidor Kali Linux, se inicia el proceso para la denegación de servicios (DoS).

Para este ataque[72] se usará el Slow loris[73], el cual funciona realizando un ataque a la capa de aplicación mediante la utilización de solicitudes HTTP parciales. El ataque abre conexiones a un servidor web específico y mantiene estas conexiones abiertas todo el tiempo que pueda. Este programa no viene por defecto en Kali Linux, así que debe clonarse por consola desde su GitHub oficial y ejecutarse.

[72] «(1) Kali Linux - Slowloris - DOS Attacking Tool - YouTube», accedido 5 de mayo de 2019, https://www.youtube.com/watch?v=7LFKff42qEQ.
[73] «Slowloris DDoS Attack | Cloudflare», accedido 5 de mayo de 2019, https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/.

El resultado del ataque de DoS es la indisponibilidad de la intranet, como puede verse en la imagen a continuación en la que, a diferencia de la figura 10, la página arroja error de disponibilidad:

Figura 11. Página después de ser atacada con Slowloris



Fuente: Autor

6.1.6 Ataque ransomware / ms17-010[74]

MS17-010 es la actualización que resuelve una vulnerabilidad identificada en marzo de 2017 que podría permitir la ejecución remota de código si un atacante envía mensajes especialmente diseñados a un servidor de Microsoft Server Message Block 1.0 (SMBv1)[75]. Fue gracias a esta vulnerabilidad que en mayo se difundió el ransomware WannaCry[76].

---

[74] Ver Anexo A – Video Pentesting, minuto 15:35.

[75] BetaFred, «Microsoft Security Bulletin MS17-010 - Critical», accedido 28 de abril de 2019, https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010.

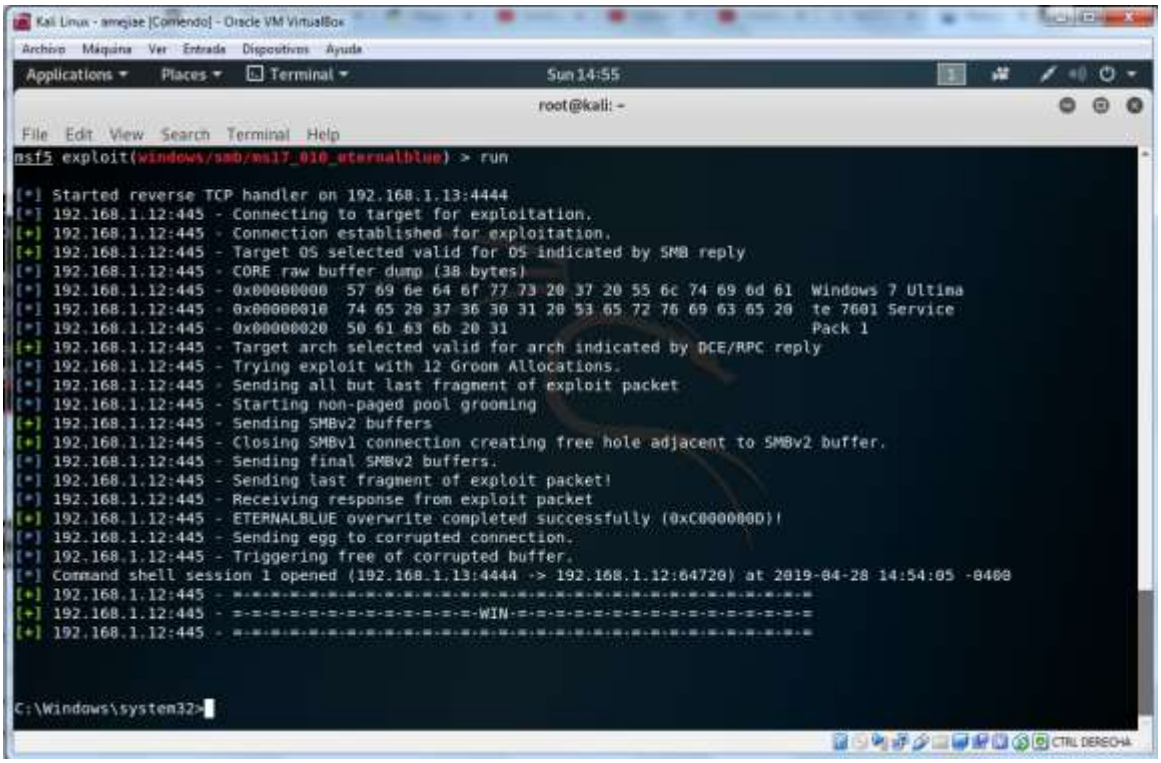
[76] Víctor Gabriel Reyes Macedo y Moisés Salinas-Rosales, «WannaCry: Análisis del movimiento de recursos financieros en el blockchain de bitcoin.», *Research in Computing Science* 137 (2017): 147-55.

La explotación de MS17-010, también conocida como eternalblue, conduce al acceso a nivel del SISTEMA a través de la ejecución remota de código (RCE) que permite el acceso a la consola de la víctima desde la máquina del atacante. El método más común para explotar MS17-010 es mediante el uso del módulo *Windows/smb/ms17_010_eternablue* de Metasploit[77]. Los equipos vulnerables se pueden encontrar utilizando varios métodos, incluidos los escáneres de vulnerabilidades como el motor de scripts Nmap (con el comando `nmap --script smb-vuln-ms17-010 -p445 targetip`) y el módulo de Metasploit *auxiliary/scanner/smb/smb_ms17_010*[78].

La figura a continuación refleja el sistema vulnerado después del ataque, permitiéndole al atacante acceder al sistema víctima:

[77] antony daubuoi, *exploit ms17-010 with metasploit in kali-linux*, accedido 28 de abril de 2019, https://www.youtube.com/watch?v=wpvWFEmqR-s.
[78] Korey McKinley, «Manually Exploiting MS17-010», *LMG Security* (blog), 20 de febrero de 2018, 17-010, https://lmgsecurity.com/manually-exploiting-ms17-010/.

Figura 12. Acceso a Windows con ms17_010_eternablue



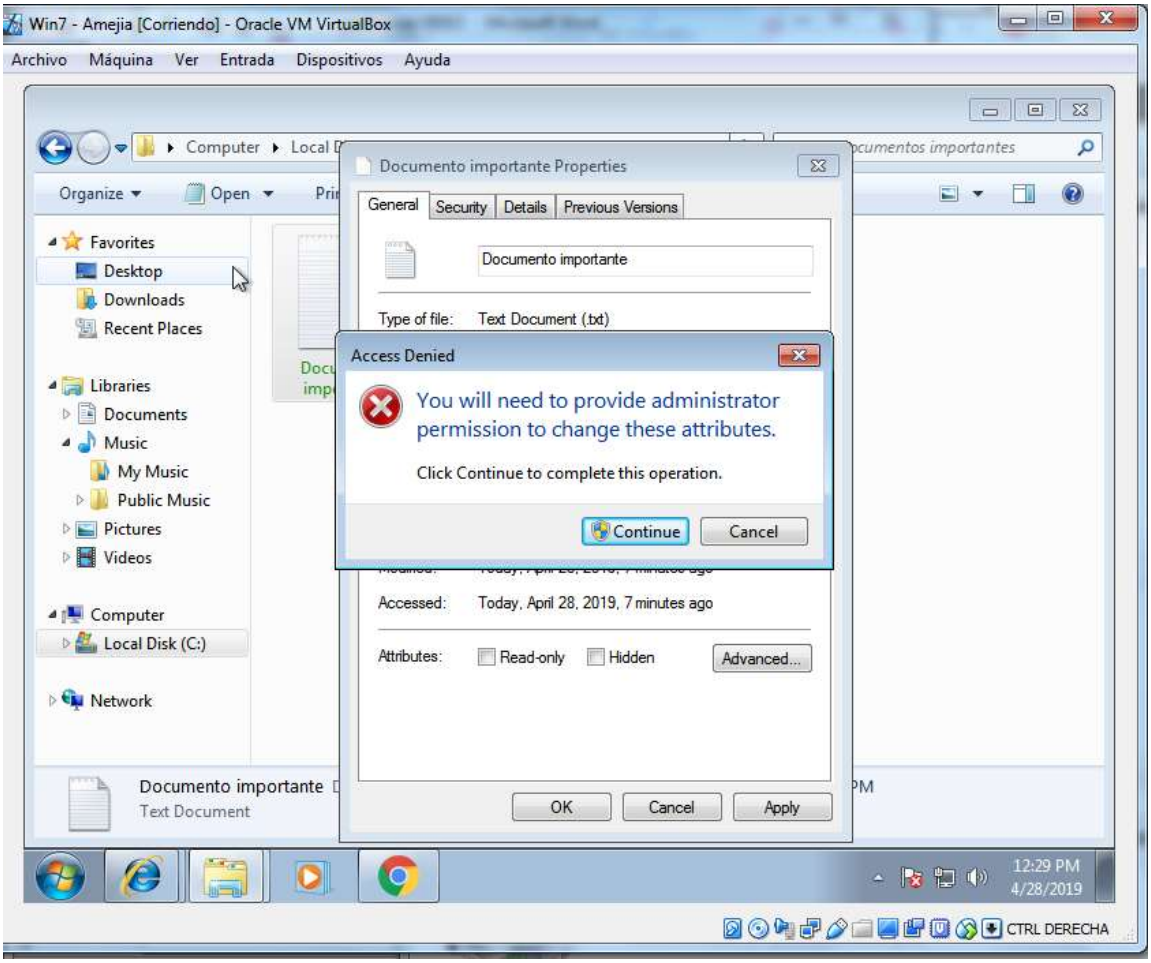
Fuente: Autor

Una vez adentro del sistema, el ataque ransomware se puede aplicar de diferentes maneras y a diferentes escalas, desde solo algunos archivos claves hasta los archivos de arranque del sistema. En este ejercicio se bloquean algunos archivos encriptándolos con una función del propio Windows `CIPHER`[79]. Este comando cifra los archivos de la carpeta donde esté. Ya que el usuario que realiza el bloqueo es el usuario de Sistema con el que se ha ingresado gracias al exploit, un usuario común no podrá acceder a los archivos y tampoco podrá desencriptarlos.

A continuación, se muestra el error que le genera el sistema a la víctima cuando intenta acceder al archivo encriptado.

[79] coreyp-at-msft, «Cipher», accedido 28 de abril de 2019, https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/cipher.

Figura 13. Archivos encriptados

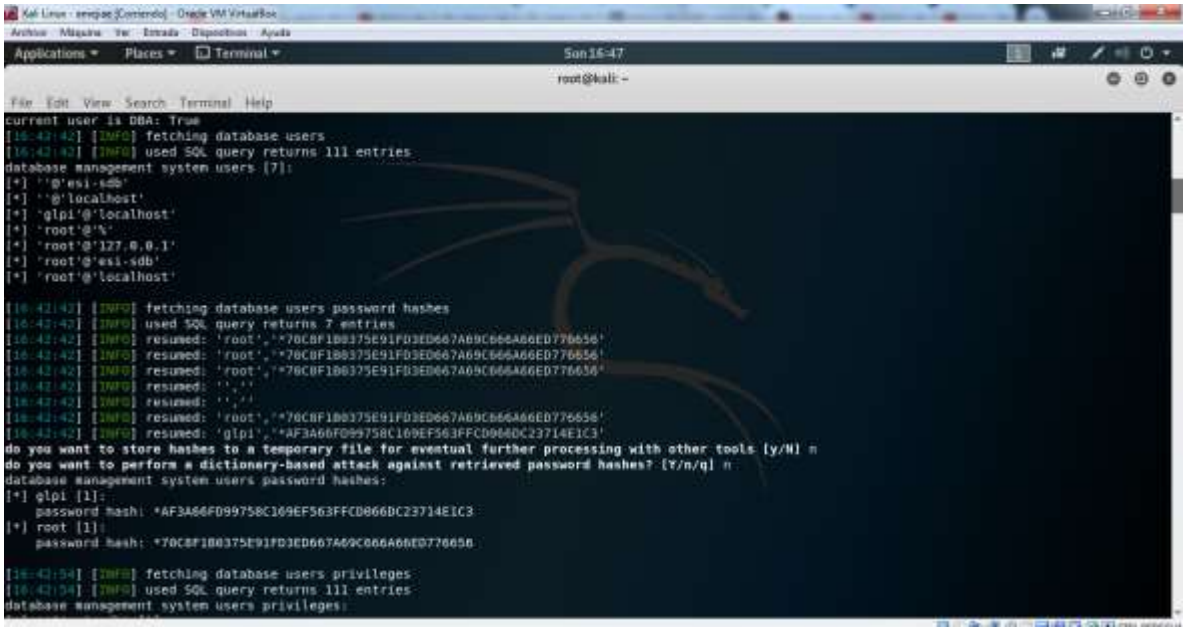


Fuente: Autor

6.1.7 Ataque sql inyection[80]

Gracias a la insegura configuración del aplicativo web de NOSTRADAMUS S.A.S. (http://104.236.31.57/Test_SQLInj/index.php), en la cual se permiten ataques de SQL Injection, es posible utilizar la herramienta de Kali Linux SQLMap, con la cual se puede mapear toda la base de datos del aplicativo y sacar información como el tipo de procesador de Bases de datos en el que está montado e información confidencial como la lista de usuarios administradores y sus claves en hash, las cuales podrían llegar a ser también crackeadas. A continuación, se presenta el resultado del análisis de información con SQLMap, permitiendo así el acceso a información sensible.

Figura 14. Mapeo con SQL Map



Fuente: Autor

[80] Ver Anexo A – Video Pentesting, minuto 20:35.

6.2 DESARROLLO OBJETIVO ESPECÍFICO 2

6.2.1 Propuesta de mitigación

Como resultado de las pruebas de penetración, o pentesting realizadas en el numeral 6.1, en este numeral se hablará de las principales estrategias de mitigación del riesgo, de tal manera que se combatan las vulnerabilidades encontradas en la infraestructura tecnológica de NOSTRADAMUS S.A.S.

Mantener actualizado el Navegador

Muchas empresas mantienen una versión antigua de sus navegadores, especialmente de Internet Explorer (IE), para poder tener aplicativos desarrollados a la medida que requieren ser desplegados en versiones antiguas de este navegador. Sin embargo, como cualquier aplicativo, los navegadores deberían mantenerse actualizados con el fin de lograr una mejor funcionalidad y rendimiento. Y no sólo esto, como se puede ver en la el ataque por navegador con ingeniería social (6.1.3), los navegadores antiguos tienen muchas vulnerabilidades que pueden ser fácilmente explotables para permitir el acceso a otras partes del sistema

Mantener actualizado el SO

Más aún que el navegador, el Sistema Operativo (SO) debe mantenerse actualizado, con sus parches de seguridad al día. Incluso, a veces no es suficiente con la actualización automática. Está por ejemplo el caso del Eternalblue[81], en el que se hace evidente tras los ataques ransomware, tipo WannaCry, que es necesario que se actualicen los equipos con Windows 7 con la instalación del MS17-010 para el acceso remoto, la elevación de privilegios y los ransomware.

[81] «Explotando Vulnerabilidad MS17-010 o WannaCry», *Juan Oliva* (blog), 1 de junio de 2017, https://jroliva.net/2017/06/01/explotando-vulnerabilidad-wannacry-o-ms17-010/.

Antivirus y Firewall

Un buen antivirus y un firewall robusto son las principales armas de defensa de un sistema operativo; como siempre, no son infalibles, pero si suman dificultad a la hora de realizar un ataque exitoso. Un antivirus es capaz de detectar una gran cantidad de virus bien sea por búsqueda heurística, vigilancia continua o CRC (Ciclyc Redundant Check)[82]. Estos evitan la proliferación de los malware o el envío de archivos que permitan el bypass UAC (ver (6.1.4)

Mitigar las inyecciones de código en los aplicativos web

Las inyecciones son uno de los ataques más comunes en los aplicativos web, por ello se han desarrollado varias técnicas de mitigación, entre las que se destacan evitar la generación de consultas dinámicas por GET, implementar parámetros de seguridad adicional y validaciones de caracteres especiales[83]. Es muy útil también realizar pruebas de vulnerabilidad en nuevos aplicativos o actualizaciones funcionales a los mismos, como las que se han desarrollado en este escrito, para identificar posibles vulnerabilidades y puntos de fuga.

Instalación de un WAF para el aplicativo web

Una vez asegurado el aplicativo web lo mejor posible, principalmente aplicando las mejores prácticas de desarrollo[84] es momento de proteger el canal de comunicación con un firewall de aplicaciones web, o WAF por sus siglas en inglés Web Application Firewall, es un elemento flexible que puede configurarse según las características de la aplicación que está protegiendo. Principalmente su función es aplicar una política de bloque o continuación al tráfico HTTP según los

---

[82] «Análisis comparativo de los principales sistemas antivirus», accedido 5 de mayo de 2019, http://scielo.sld.cu/scielo.php?pid=S1024-94352003000500005&script=sci_arttext&tlng=en.

[83] «Técnicas de mitigación para principales vulnerabilidades de seguridad en aplicaciones web - ProQuest», accedido 5 de mayo de 2019, https://search.proquest.com/openview/ef48269d2b309b464f6d0070f79eee7b/1?pq-origsite=gscholar&cbl=1006393.

[84] Cesar R. Cuenca Díaz, «Desarrollo Seguro: Principios y Buenas Prácticas», s. f., 23.

parámetros que se definan. Estas políticas y patrones de bloqueo serán aplicadas a cada trama de HTTP que se dirija o salga de la aplicación[85].

Los WAF fueron desarrollados a principios de la década de los 90 por Gene Spafford, Bill Cheswick y Marcus Ranum. Aunque sus primeras implementaciones estaban más enfocadas a ser un firewall de red, podía manejar el flujo de algunas aplicaciones como FTP (*File Transfer Portocol*, protocolo estándar para la transferencia de archivos que utiliza por defecto el puerto 21 para solicitar conexiones de control del cliente servidor y el puntero 20 para el envío de datos en modo activo)[86].

6.2.2 Propuesta de UTM

El término gestor unificado de amenazas (UTM, por sus siglas en inglés *Unified Threat Management*) fue utilizado por primera vez en 2004 por Charle Kologgy, vicepresidente de Investigación de Productos de Seguridad del *International Data Corporation*[87]. Se trata de la consolidación de distintas soluciones de seguridad de redes en una única solución que incluye servicios como firewall, antivirus de puerta de enlace, filtrado de contenido web, prevención y detección de intrusiones y accesos remotos a través de VPN, además permite el balanceo de carga de enlaces para asegurar la continuidad de la disponibilidad. Todo esto desde un administrador centralizado de red desde el que puede controlar las distintas soluciones que proporciona el proveedor.

---

[85] «idUS - Implementación y medida del rendimiento de un firewall para aplicaciones web (WAF) en un balanceador de carga», accedido 5 de mayo de 2019, https://idus.us.es/xmlui/handle/11441/85834.

[86] «RUA: Práctica 3. Protocolos de transporte TCP y UDP», accedido 13 de octubre de 2019, http://rua.ua.es/dspace/handle/10045/11606.

[87] «Repositorio Universidad de Guayaquil: Implementación de un gestor unificado de amenazas de seguridad para la red administrativa de la carrera de Ingeniería de Sistemas Computacionales, basado en el análisis de su infraestructura de red interna y de perímetro.», accedido 5 de mayo de 2019, http://repositorio.ug.edu.ec/handle/redug/6672.

A continuación, se presenta un cuadro comparativo con las principales características de dos de los UTM más conocidos en el mercado[88].

Tabla 13. Tabla comparativa de UTM

Dispositivo del mercado	Características	Fortalezas	Debilidades
SOPHOS (ASTARO)	Con sede en Massachusetts, Alemania, ofrece dispositivos UTM desde 2001. Astaro fue adquirida por Sophos endpoitns, proveedores de seguridad en el 2011. Tiene un rendimiento de 575 Mbps en general. Está disponible en el mercado versiones de hardware y software que soportan Firewall, IPS, VPN y otras funciones. También está disponible como dispositivo virtual el cual ejecuta WNWARE, CITRIX, KVM, Hiper-V, junto con Amzaon Machine.	Ofrece diferentes tipos de paquetes a empresas industriales donde se realiza venta al por menor, capacitaciones y atención permanente Se caracteriza por la facilidad de instalación y de uso Debido a la adquisición de Astaro por la empresa Sophos se nota un mayor incremento financiero lo cual promueve nuevos productos	No es elegido por los clientes, según Gartner y no es catalogado como producto fuerte por la competencia Los usuarios esperan que genere mejora en los productos ofrecidos Sophos debe evitar que los nuevos productos UTM que se ponen en el mercado dependan solo de las soluciones propias

[88] Salinas Salinas y Wilson Enrique, «Comparación de los sistemas de gestión unificado y dispositivos de propósito específico que ayudan a prevenir las amenazas informáticas a que están expuestas las Pymes», 2013, http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2591/00000789.pdf?sequence=1.

Tabla 14. Tabla comparativa de UTM (continuación)

Dispositivo del mercado	Características	Fortalezas	Debilidades
FORTINET	Con sede en California, se ha centrado en el desarrollo de circuitos integrados para redes de procesamiento e inspección de contenidos para lograr altos niveles de rendimiento. Ofrecen firewall con rendimiento de 20 Mbps a 1 Gbs y ofrecen puntos de acceso WLAN	Tiene la mayor credibilidad ante los clientes de UTM según Gartner, es la empresa más mencionada por los competidores La línea de productos tiene un alto precio dada su alto desempeño e incremento en la velocidad de red La línea de soporte MSSP es muy fuerte FortiGuard Labs es una poderosa fuente de información sobre amenazas y vulnerabilidades	Si bien la interfaz de usuario ha mejorado, sigue teniendo una calificación inferior a la de sus competidores Los usuarios les gusta ver más registros de filtrado y una interfaz más sencilla

Fuente: Autor

A continuación, se presenta otra tabla comparativa con los servicios ofrecidos por ambas empresas[89].

[89] «Repositorio Universidad de Guayaquil: Implementación de un gestor unificado de amenazas de seguridad para la red administrativa de la carrera de Ingeniería de Sistemas Computacionales, basado en el análisis de su infraestructura de red interna y de perímetro.»

Tabla 15. Segunda tabla comparativa UTM

Características	Sophos UTM	Fortinet
Firewall	SI	SI
IPS	SI	SI
VPN	SI	SI
Filtrado de Navegación	SI	SI
QoS (Calidad de servicio)	SI	SI
Protección Antivirus doble	SI	NO
WAF	SI	NO
Portal de usuario	SI	NO
Reporteria completa	SI	CONDICIONADO
Factor de doble autenticación integrado	SI	NO
Protección de amenazas avanzadas	SI	NO
Control de aplicaciones	SI	SI
Versión de software	SI	NO
Versión libre	SI	NO

Fuente: «Repositorio Universidad de Guayaquil: Implementación de un gestor unificado de amenazas de seguridad para la red administrativa de la carrera de Ingeniería de Sistemas Computacionales, basado en el análisis de su infraestructura de red interna y de perímetro.»

Por las razones expuestas en los cuadros comparativos, se recomienda Sophos que, a pesar de no tener aún el reconocimiento de Gartner, se proyecta a tener un mayor rango de soporte, además de incluir una versión gratuita para poder iniciar poco a poco la adaptación de la seguridad de NOSTRADAMUS S.A.S

6.3 DESARROLLO OBJETIVO ESPECÍFICO 3 Y 4 - PLAN PARA LA POSTERIOR IMPLEMENTACIÓN DE UN SGSI Y ANÁLISIS DE GESTIÓN DE RIESGOS

Dentro del enfoque administrativo de este proyecto práctico, se define la necesidad de establecer las bases para la implementación de un SGSI, basados en la norma ISO/IEC 27001, para el caso de estudio NOSTRADAMUS S.A.S.,

teniendo como base de información de la organización brindada por la Universidad Nacional Abierta y a Distancia.

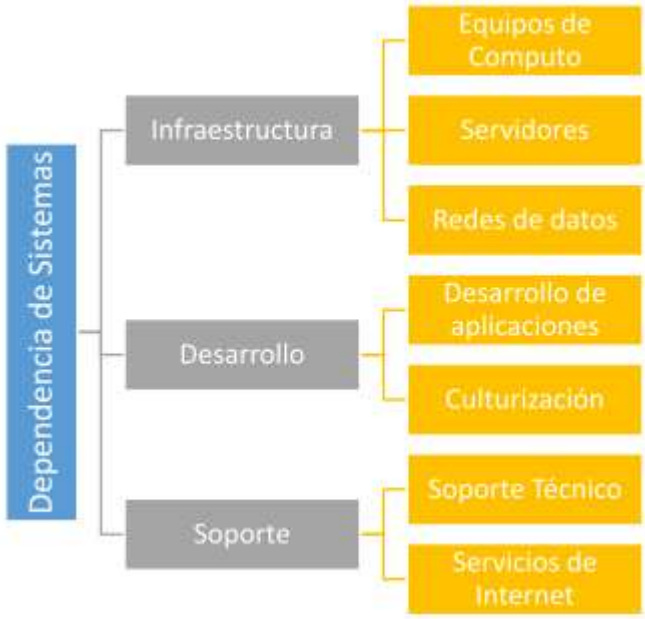
6.3.1 Situación actual de NOSTRADAMUS S.A.S. [90]

NOSTRADAMUS S.A.S. es una empresa del sector tecnológico que busca el desarrollo tecnológico en comunidades colombianas a través del uso de Tecnologías de Información. Actualmente cuenta con 120 colaboradores entre directivos, administrativos y operativos quienes hacen uso de forma regular de los medios de información para consulta de datos.

Cuenta con una dependencia de sistemas que brinda soporte a la infraestructura tecnológica 24/7

[90] Toda la información de este numeral fue tomada y adaptada del documento PROPUESTA PARA EL DESARROLLO DE LA ALTERNATIVA DE GRADO COMO PROYECTO APLICADO – ESCENARIO DOS (ENFOQUE DIRECTIVO – ADMINISTRATIVO), brindado por la Universidad Nacional Abierta y a Distancia.

Figura 15. Organigrama – Dependencia de sistemas NOSTRADAMUS S.A.S.



Fuente: Propuesta para el desarrollo de la alternativa de grado como proyecto aplicado – Escenario dos (enfoque directivo – administrativo)

Las funciones de las áreas son:

- **Área de infraestructura:** Soporte al acceso a la red interna y a internet. Revisión de diseños de cableado estructurado.
- **Área de desarrollo:** Apoyo técnico a las dependencias de la organización del centro en desarrollo de medios eficientes para lograr actividades basadas en usos de tecnologías de la informática y las telecomunicaciones.
- **Área de Soporte:** Mantenimiento de computadores (sólo equipos propiedad de la empresa). Generación de conceptos técnicos para tramitar baja de equipos. Realiza copias de seguridad de los sistemas de información y servidores virtuales que se encuentran en las dependencias de la empresa NOSTRADAMOS S.A.S.

Desde la dependencia de Sistemas, la asistencia que ofrece se divide así:

- **Apoya el servicio de correo electrónico institucional:** servicio que está contratado con Google, este servicio busca:
    - Comunicación con otros miembros de la entidad
    - Compartir archivos
    - Recibir comunicados oficiales
    - Brindar espacio de almacenamiento ilimitado
    - Dar prioridad a las actividades propuestas por el desarrollo académico del programa
- **Apoyo en la gestión y mantenimiento de activos informáticos:** servicio que cumple la función de mantener en optimo desempeño servicios tecnológicos como:
    - Equipos de cómputo de escritorio, móviles y servidores, televisores, videoproyectores
    - Software operativo y aplicativo
    - Servicio de Internet
    - Todo el equipamiento que se requiera para ayudar a dar cumplimiento al objeto social.
- **Apoyo en la gestión de usuarios y contraseñas:** Servicio que se enfoca en la gestión de usuarios y contraseñas usadas en las diferentes aplicaciones enfocadas en apoyar la gestión de NOSTRADAMUS S.A.S.:
    - Correo electrónico
    - Sistema de gestión de calidad
- **Apoyo a la dependencia de nómina y facturación:** En la dependencia de nómina y facturación se desarrollan las siguientes tareas:
    - Generación de nómina de trabajadores
    - Generación de recibos de pago
    - Creación, alimentación y custodia de Hojas de vida

- Control del seguimiento al talento humano
- Generación certificados laborales y relacionados con el modelo de negocio

6.3.2 Listas de chequeo

Las listas de chequeo ayudan a realizar el levantamiento de información previa y la verificación de las características de la empresa, especialmente enfocado al SGSI que se busca implementar. Es una herramienta muy útil para identificar puntos débiles, oportunidades de mejora, causas y medidas apropiadas en los ámbitos temáticos de cada lista, por medio de la verificación de los aspectos presentes o no del área que se revisa.

Para el desarrollo del proyecto de diseño para la posterior implementación del SGSI de NOSTRADAMUS S.A.S., se propone utilizar como base las listas de chequeo almacenadas en el Anexo B de este documento, tomadas de ISO27001 security[91], en las que se revisa el **Estado de Implementación ISO 27001**, en el que se enlista el estado de implementación de los documentos obligatorios para cumplir con la normativa ISO/IEC 27001:2013; y el **Estado y Aplicabilidad de controles de Seguridad de la Información**, en el que se enlistan los dominios y controles establecidos en el Anexo A de la ISO/IEC 27002:2013, ya mencionado dentro de este documento en la Tabla 1.

6.3.3 Metodología para la implementación del SGSI

Se han propuesto diferentes metodologías para lograr la implementación de un SGSI, el enfoque que se propone en este documento está basado en la norma ISO/IEC 27003:2010, el cual logra disminuir la incertidumbre del resultado ya que

[91] «ISO27k infosec management standards», accedido 14 de octubre de 2019, https://www.iso27001security.com/.

este enfoque permite abordar sistemáticamente el cumplimiento de todos los elementos necesarios para un SGSI.

Cinco fases componen la metodología propuesta, las cuales deben ejecutarse secuencialmente con la disposición de personal interno, tiempo y recursos, y con el respaldo de la alta dirección, vital para lograr el cumplimiento de los objetivos previstos.

Las cinco fases, con sus respectivas etapas, son de cumplimiento obligatorio si se quiere cumplir con los requisitos de la norma; a continuación, serán relacionadas en función a la norma ISO/IEC 27001:2013

Tabla 16. Fases de implementación de un SGSI y su relación con los numerales de la norma ISO/IEC 27001:2013[92]

Fases 27003:2010	Etapas	Numerales de la ISO/IEC 27001:2013
Fase 1: Obtener la aprobación de la Dirección para iniciar el proyecto	Establecimiento de las prioridades de la organización para desarrollar un SGSI Definir el alcance preliminar del SGSI Creación del plan del proyecto para ser aprobado por la Dirección	4.1 Conocimiento de la organización y de su contexto 4.2 Comprensión de las necesidades y expectativas de las partes interesadas 5.1 Liderazgo y compromiso 7.1 Recursos

[92] Francisco Javier Valencia-Duque y Mauricio Orozco-Alzate, «Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000», *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, n.º 22 (junio de 2017): 27000, https://doi.org/10.17013/risti.22.73-88.

Tabla 17. Fases de implementación de un SGSI y su relación con los numerales de la norma ISO/IEC 27001:2013 (continuación)

Fases 27003:2010	Etapas	Numerales de la ISO/IEC 27001:2013
Fase 2: Definir el alcance, los límites y la política del SGSI	Definir el alcance y los límites del SGSI Definir el alcance y los límites de las Tecnologías de la Información y Comunicaciones Definir el alcance y los límites físicos Desarrollar la política del SGSI y obtener la aprobación de la Dirección	4.3 Determinación del alcance del SGSI 5.1 Liderazgo y compromiso 5.2 Política 6.2 Objetivos de seguridad de la información y planes para mejorarlos
Fase 2: Definir el alcance, los límites y la política del SGSI	Definición de roles y responsabilidades del SGSI	5.3 Roles, responsabilidades y autoridades en la organización 7.2 Competencias 7.3 Toma de conciencia
Fase 3: Análisis de los requisitos de la seguridad de la información	Definir los requisitos de la información para los procesos del SGSI Identificar los activos dentro del alcance del SGSI Realizar una evaluación de la seguridad de la información	4.2 La organización debe determinar los requisitos de las partes interesadas pertinentes a la seguridad de la información. 6.1.2 Valoración de riesgos de seguridad de la información

Tabla 18. Fases de implementación de un SGSI y su relación con los numerales de la norma ISO/IEC 27001:2013 (continuación)

Fases 27003:2010	Etapas	Numerales de la ISO/IEC 27001:2013
Fase 4: Valoración de riesgos y planificar el tratamiento de riesgos	Realizar la valoración de riesgos	6.1.2 Valoración de riesgos de seguridad de la información
		6.1.3 Tratamiento de riegos de la seguridad de la información
	Seleccionar los objetivos de control y los controles	6.2 Objetivos de seguridad de la información y planes para lograrlo
	Obtener la autorización de la Dirección para implementar y operar el SGSI	5.1 Liderazgo y compromiso
Fase 5: Diseñar el SGSI	Diseñar la seguridad de la información de la organización	7.4 Comunicación
		7.5 Información documentada
		8.1 Planificación y control operacional
	Diseñar la seguridad física y de las Tecnologías de la Información y Comunicaciones	8.2 Valoración de riesgos de seguridad de la información
		8.3 Tratamiento de riesgos de seguridad de la información
	Diseñar la seguridad específica de un SGSI	9.1 Seguimiento, medición, análisis y evaluación
	Producir el plan del proyecto final del SGSI	9.2 Auditoria interna
		9.3 Revisión por la Dirección

Fuente: *Francisco Javier Valencia-Duque y Mauricio Orozco-Alzate, «Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000», RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação, n.º 22 (junio de 2017): 27000, https://doi.org/10.17013/risti.22.73-88.*

6.3.4 Fase 1: aprobación de la dirección para iniciar el proyecto

Es de vital importancia que toda la compañía, y en especial la alta dirección, esté involucrada con todo el ciclo de vida del SGSI: la planeación, el hacer, la verificación y el actuar. Por ello es que se deben establecer las prioridades de la organización para desarrollar el SGSI, se deben concretar los objetivos estratégicos de la organización, enfocadas en la seguridad de la información y se debe tener claridad sobre los requisitos normativos o de terceros frente a la seguridad de la información y conciencia sobre los diferentes sistemas de gestión existentes. En esta fase también se debe definir el alcance preliminar del SGSI, el plan de proyecto para su implementación, aprobado por la alta dirección, y los compromisos de ésta para con los procesos y actividades relacionados al establecimiento, implementación, operación, monitoreo, evaluación y mantenimiento permanente del SGSI (clausula 5 de la norma ISO 27001:2013).

6.3.5 Fase 2: definir el alcance, los límites y la política del SGSI

En esta fase se definen los siguientes elementos:

Alcance del SGSI

El alcance se establece con el fin de delimitar el proceso de gestión de riesgos y debe establecerse en función al quehacer del negocio, abarcando uno o varios de los procesos de la empresa, así como varios de sus servicios o sedes. Es importante que sea factible en términos de tiempo y recursos. Por ende el alcance

suele ser un párrafo que resuma lo que la empresa está protegiendo en la organización y hace parte de los documentos para la certificación.

En términos del caso de estudio tratado en este documento, una propuesta de alcance sería:

> El alcance del SGSI de NOSTRADAMUS S.A.S., debe abarcar solo el proceso de Gestión de Sistemas de la empresa, que involucra la gestión y mantenimiento de activos informáticos, la gestión de usuarios y contraseñas y los procesos de apoyo tecnológico a la dependencia de nómina y facturación.

Política del SGSI

La norma ISO/IEC 27001:2013, en su numeral 5.2 Política, indica que la Alta Dirección de una empresa debe definir una política de seguridad de la información que esté acorde al que hacer y los propósitos de cada organización, donde deben establecerse los objetivos de seguridad de la información, teniendo en cuenta las normativas vigentes relacionadas con seguridad de la información y el compromiso de la mejora continua por parte de la Alta Dirección. La siguiente es la propuesta de política general del SGSI que se definió:

> NOSTRADAMUS S.A.S., en cumplimiento a su misión, visión y objetivo estratégico, y para satisfacer las necesidades de sus clientes, externos e internos, de la comunidad y demás interesados, instaura la función de Seguridad de la Información en la Entidad, con el objetivo de:
>
> - Cumplir los requerimientos legales y reglamentarios aplicables a la empresa y al SGSI

- Asegurar la confidencialidad, integridad, disponibilidad y confiabilidad de la información necesaria para la prestación de los servicios ofrecidos por NOSTRADAMUS S.A.S.
- Gestionar los riesgos de la empresa a través de la aplicación de controles y estándares enfocados en preservar la seguridad de la información.
- Aplicar medidas y procesos que fortalezcan tanto la seguridad de la información como la seguridad informática de la empresa.
- Fortalecer la cultura de seguridad de la información en los trabajadores de NOSTRADAMUS S.A.S.
- Garantizar la continuidad de los servicios y la seguridad de la información.

Objetivos del SGSI

Los objetivos generales del SGSI deben estar articulados con las políticas establecidas y dentro del alcance previsto. Un ejemplo de objetivos generales para el caso de estudio NOSTRADAMUS S.A.S. son:

- Mejorar el nivel de eficacia de los controles de la empresa e implementar aquellos que hagan falta para mitigar los riesgos.
- Garantizar la disponibilidad de la información de NOSTRADAMUS S.A.S. de acuerdo con los criterios de seguridad que establezca la empresa y la normatividad vigente.
- Proteger la integridad de la información de NOSTRADAMUS S.A.S., teniendo en cuenta los requisitos de seguridad aplicables y los resultados del análisis de riesgos, así como de los controles que se establezcan.
- Asegurar que la información de NOSTRADAMUS S.A.S mantenga los criterios de confidencialidad que la empresa determine para que esté

disponible a los usuarios o procesos autorizados, en el momento que así lo requieran.

Aprobación de la Dirección

Es de vital importancia que en esta fase la alta dirección esté involucrada en la definición y aprobación del alcance, la política y los objetivos que regirán el SGSI, de allí que la normativa ISO/IEC 27001:2013, en el numeral 5.1 establezca como parte del compromiso de la dirección el hacer que la política y los objetivos sean definidos acorde a la dirección estratégica de la compañía.

6.3.6 Fase 3: análisis de los requisitos de seguridad de la información

Según la norma ISO/IEC 27003:2010 principalmente se deben identificar los activos de la información de la compañía. La norma diferencia dos tipos de activos de información: primarios y de soporte. Los procesos del negocio y la información de la empresa son los activos primarios, mientras que los activos de soporte son aquellos en los que se almacenan o de los que dependen los activos primarios y se clasifican en: hardware, software, redes, personal e infraestructura física.

Los activos se deben identificar y clasificar de acuerdo a los requerimientos de seguridad y los niveles de criticidad que implican para el negocio, a la vez que deben establecerse quién es el propietario del activo y quién el responsable de su seguridad[93].

[93] Gustavo Pallas y María Eugenia Corti, «Metodología de Implantación de un SGSI en grupos empresariales de relación jerárquica», *Uruguay Magister Thesis: Universidad de la República*, 2009.

6.3.7 Fase 4: valoración de riesgos y planificar el tratamiento de riesgos

El eje principal del SGSI, el cual puede ser evaluado desde diferentes metodologías, como la propuesta por la ISO/IEC 27005, OCTAVE, CRAMM, NIST, MEHARI y MAGERIT, la cual será utilizada en este documento para la evaluación de riegos del caso de estudio NOSTRADAMUS S.A.S.

MAGERIT es una metodología elaborada por el Consejo Superior de Administración Electrónica con el fin de garantizar la autenticidad, confidencialidad, disponibilidad, trazabilidad e integridad de los activos informáticos de la organización. Define en 3 libros el proceso para el análisis de riesgos, en el primero describe la estructura adecuada para un modelo de gestión de riesgos, en el segundo establece una serie de enfoques para el análisis de riesgos y en el último presenta guías de trabajo para tal fin. MAGERIT se enfoca especialmente en conocer el estado de seguridad de los sistemas de información, implementar medidas de seguridad, buscando que no queden elementos por fuera para mitigar vulnerabilidades. Esta es una de las metodologías más utilizadas en las organizaciones[94].

Para el desarrollo de esta fase se debe tener en cuenta establecer el contexto, los parámetros de probabilidad, los parámetros de impacto, la determinación de vulnerabilidades, los criterios de aceptación del riesgo, la valoración del riesgo, la identificación de los escenarios de riesgo, la estimación y la evaluación del riesgo, con lo que se pueden extraer mapas de riesgo o mapas de calor, y, como resultado final, establecer el tratamiento de riesgos, en el cual se plantean las acciones necesarias para llevar los riesgos identificados a un nivel aceptado por la organización.

[94] J. Pinzón, «Acercamiento a la Gestión de Riesgos con Magerit y las 4A», *Bogotá: sn*, 2009.

Con la información teórica disponible para el caso de estudio NOSTRADAMUS S.A.S., se desarrolla a manera de ejemplo el levantamiento de activos de la información y su valoración cuantitativa, teniendo presente la valoración de las dimensiones en las que el activo es importante, las cuales son[95]:

- **[D] Disponibilidad:** Nivel de afectación en caso de que el activo no estuviera disponible.
- **[I] Integridad de los datos:** Nivel de afectación en caso de que datos fueran modificados fuera de control.
- **[C] Confidencialidad de la información:** Nivel de afectación en caso de que los datos fueran conocidos por personas no autorizadas.
- **[A] Autenticidad:** Nivel de afectación en caso de que quien accede al servicio no sea realmente quien debería, o que los datos no fueran atribuibles a quien se cree.
- **[T] Trazabilidad:** Nivel de afectación en caso de que no quedara constancia fehaciente del uso del servicio ni constancia del acceso a los datos.

Para la valoración de cada una de las dimensiones se toma como referencia la siguiente escala de calificación; el riesgo resultante es el promedio de todas las dimensiones, teniendo en cuenta la misma escala:

Tabla 19. Escala de valoración del riesgo

Categoría	Valoración
Critico	21 a 25
Importante	16 a 20
Apreciable	10 a 15
Bajo	5 a 9
Despreciable	1 a 4

[95] Llibre II MAGERIT, «Catálogo de elementos», *Portal d'administració*, s. f.

Fuente: *Autor*

Tabla 20. Valoración cuantitativa de los activos de NOSTRADAMUS S.A.S.

Nombre	[A]	[T]	[C]	[I]	[D]	Riesgo
Servidor de Impresión	9	25	9	25	25	IMPORTANTE
Servidor Archivo FTP	25	25	9	15	25	IMPORTANTE
Página Web	20	25	25	25	25	CRITICO
Servidor de nómina y facturación	25	25	15	15	25	CRITICO
Sistemas de nómina y facturación	25	25	25	25	25	CRITICO
Servidor DHCP	9	4	9	25	20	APRECIABLE
Equipos de cómputo	25	25	9	15	20	IMPORTANTE
Cortafuegos Cisco ASA 5505	15	25	4	9	15	APRECIABLE
Sistemas operativos win 10 Pro	25	25	4	15	20	IMPORTANTE
Puntos de acceso alámbricos (hub)	4	9	9	15	25	APRECIABLE
Switches cisco catalyst 2960	4	9	25	15	20	APRECIABLE
Técnicos de mantenimiento	9	9	9	25	25	APRECIABLE
Teléfonos IP	25	25	25	15	25	CRITICO
Puntos de acceso	9	9	4	20	20	APRECIABLE
Respaldo de la información de los sistemas	25	4	9	15	20	APRECIABLE
Servicio de internet	9	9	9	9	9	BAJO
Cableado	25	25	15	15	20	IMPORTANTE

Fuente: *Autor*

Para identificar los riesgos potenciales se evalúan las vulnerabilidades que pueden llegar a materializarse como una amenaza, valorando que tan alto sería su impacto y probabilidad. Es importante identificar los distintos tipos de amenazas que pueden llegar a materializarse[96]:

Tabla 21. Tipos de amenaza

TIPO AMENAZA	AMENAZA
[N] Desastres naturales	[N1] Fuego
[N] Desastres naturales	[N2] Daños por agua
[N] Desastres naturales	[N*] Desastres naturales
[I] De origen industrial	[I1] Fuego
[I] De origen industrial	[I2] Daños por agua
[I] De origen industrial	[I*] Desastres industriales

[96] MAGERIT.

Tabla 22. Tipos de amenaza (continuación)

TIPO AMENAZA	AMENAZA
[I] De origen industrial	[I3] Contaminación mecánica
[I] De origen industrial	[I4] Contaminación electromagnética
[I] De origen industrial	[I5] Avería de origen físico o lógico
[I] De origen industrial	[I6] Corte del suministro eléctrico
[I] De origen industrial	[I7] Condiciones inadecuadas de temperatura o humedad
[I] De origen industrial	[I8] Fallo de servicios de comunicaciones
[I] De origen industrial	[I9] Interrupción de otros servicios y suministros esenciales
[I] De origen industrial	[I10] Degradación de los soportes de almacenamiento de la información
[I] De origen industrial	[I11] Emanaciones electromagnéticas
[E] Errores y fallos no intencionados	[E1] Errores de los usuarios
[E] Errores y fallos no intencionados	[E2] Errores del administrador
[E] Errores y fallos no intencionados	[E3] Errores de monitorización (log)
[E] Errores y fallos no intencionados	[E4] Errores de configuración
[E] Errores y fallos no intencionados	[E7] Deficiencias en la organización
[E] Errores y fallos no intencionados	[E8] Difusión de software dañino
[E] Errores y fallos no intencionados	[E9] Errores de [re-]encaminamiento
[E] Errores y fallos no intencionados	[E10] Errores de secuencia
[E] Errores y fallos no intencionados	[E14] Escapes de información
[E] Errores y fallos no intencionados	[E15] Alteración accidental de la información
[E] Errores y fallos no intencionados	[E18] Destrucción de información
[E] Errores y fallos no intencionados	[E19] Fugas de información
[E] Errores y fallos no intencionados	[E20] Vulnerabilidades de los programas (software)
[E] Errores y fallos no intencionados	[E21] Errores de mantenimiento / actualización de programas (software)
[E] Errores y fallos no intencionados	[E23] Errores de mantenimiento / actualización de equipos (hardware)
[E] Errores y fallos no intencionados	[E24] Caída del sistema por agotamiento de recursos
[E] Errores y fallos no intencionados	[E25] Pérdida de equipos

Tabla 23. Tipos de amenaza (continuación)

TIPO AMENAZA	AMENAZA
[E] Errores y fallos no intencionados	[E28] Indisponibilidad del personal
[A] Ataques intencionados	[A3] Manipulación de los registros de actividad (log)
[A] Ataques intencionados	[A4] Manipulación de la configuración
[A] Ataques intencionados	[A5] Suplantación de la identidad del usuario
[A] Ataques intencionados	[A6] Abuso de privilegios de acceso
[A] Ataques intencionados	[A7] Uso no previsto
[A] Ataques intencionados	[A8] Difusión de software dañino
[A] Ataques intencionados	[A9] [Re-]encaminamiento de mensajes
[A] Ataques intencionados	[A10] Alteración de secuencia
[A] Ataques intencionados	[A11] Acceso no autorizado
[A] Ataques intencionados	[A12] Análisis de tráfico
[A] Ataques intencionados	[A13] Repudio
[A] Ataques intencionados	[A14] Interceptación de información (escucha)
[A] Ataques intencionados	[A15] Modificación deliberada de la información
[A] Ataques intencionados	[A18] Destrucción de información
[A] Ataques intencionados	[A19] Divulgación de información
[A] Ataques intencionados	[A22] Manipulación de programas
[A] Ataques intencionados	[A23] Manipulación de los equipos
[A] Ataques intencionados	[A24] Denegación de servicio
[A] Ataques intencionados	[A25] Robo
[A] Ataques intencionados	[A26] Ataque destructivo
[A] Ataques intencionados	[A27] Ocupación enemiga
[A] Ataques intencionados	[A28] Indisponibilidad del personal
[A] Ataques intencionados	[A29] Extorsión
[A] Ataques intencionados	[A30] Ingeniería social (picaresca)

Fuente: Llibre II MAGERIT, «Catálogo de elementos», *Portal d'administració*, s. f.

Teniendo en cuenta esto, se identifican las amenazas asociadas a cada uno de los activos, la vulnerabilidad asociada y el control aplicado actualmente.

Tabla 24. Tabla de activos, amenazas y controles actuales

ID	Activo de información	Amenazas	Vulnerabilidades	Control aplicado actual
R1	[AUX] Cableado	[I8] Fallo de servicios de comunicaciones	Sin auditoria del cableado físico Redes sin mantenimiento	A.11.2.3 Seguridad del cableado

Tabla 25. Tabla de activos, amenazas y controles actuales (continuación)

ID	Activo de información	Amenazas	Vulnerabilidades	Control aplicado actual
R2	[HW] Cortafuegos Cisco ASA 5505	[E2] Errores del administrador	Poca experiencia en configuración del equipo	A9.1.2 Acceso a las redes y a los servicios de red
R3		[I6] Corte del suministro eléctrico	Ubicación inadecuada, Falta de estabilizador de energía.	A13.1.2 Seguridad de los servicios de red
R4		[I7] Condiciones inadecuadas de temperatura o humedad	Los servidores DHCP, HTTP y PBX se encuentran en un espacio donde no se cumplen condiciones de climatización óptimas	A13.1.2 Seguridad de los servicios de red
R5		[A8] Difusión de software dañino	Actualización de Software para evitar ataques cibernéticos	A11.2.2 Instalaciones de suministro
R6		[I5] Avería de origen físico o lógico	Mala manipulación del equipo, saboteo	A13.1.2 Seguridad de los servicios de red
R7	[HW] Cortafuegos Cisco ASA 5505	[I6] Corte del suministro eléctrico	Falla en la red eléctrica interna, falla externa	A13.1.2 Seguridad de los servicios de red
R8		[I*] Desastres industriales	Saboteo interno	A13.1.2 Seguridad de los servicios de red
R9		[A26] Ataque destructivo	Saboteo interno	A13.1.2 Seguridad de los servicios de red
R10		[E20] Vulnerabilidades de los programas (software)	Suplantación de usuarios, acceso a información no perfilada. Transporte de información sensible visible para todos.	A13.1.2 Seguridad de los servicios de red

Tabla 26. Tabla de activos, amenazas y controles actuales (continuación)

ID	Activo de información	Amenazas	Vulnerabilidades	Control aplicado actual
R11	[HW] Equipos de cómputo	[E21] Errores de mantenimiento / actualización de programas (software)	Poca experiencia en configuración del equipo	A11.2.1 Emplazamiento y protección de equipos
R12		[A26] Ataque destructivo	Saboteo interno	A.11.2.1 Ubicación y protección de los equipos
R13		[A11] Acceso no autorizado	Captura de usuario y contraseñas Phishing Sesiones abiertas	A.11.2.2 Servicios de suministro
R14		[A5] Suplantación de la identidad del usuario	Suplantación de Usuarios	A.11.2.1 Ubicación y protección de los equipos
R15		[E19] Fugas de información	Suplantación de usuarios, acceso a información no perfilada. Transporte de información sensible visible para todos.	A.11.2.1 Ubicación y protección de los equipos
R16		[A6] Abuso de privilegios de acceso	Acceso de personal no autorizado.	A9.4.2 Procedimientos seguros de inicio de sesión
R17	[SW] Página Web	[I8] Fallo de servicios de comunicaciones	Funcionamiento solo conectado a la red	A9.4.5 Control de acceso al código fuente de los programas A12.2.1 Controles contra el código malicioso
R18	[COM] Puntos de acceso	[I*] Desastres industriales	Saboteo redes de proveedor	A.11.2.3 Seguridad del cableado
R19		[E4] Errores de configuración	Poca experiencia en configuración del equipo	A13.1.1 Controles de red

Tabla 27. Tabla de activos, amenazas y controles actuales (continuación)

ID	Activo de información	Amenazas	Vulnerabilidades	Control aplicado actual
R20		[A11] Acceso no autorizado	Captura de usuario y contraseñas Phishing Sesiones abiertas	A13.1.1 Controles de red
R21		[I5] Avería de origen físico o lógico	Falla de fábrica Saboteo interno	A.11.2.3 Seguridad del cableado
R22	[D] Respaldo de la información de los sistemas	[A11] Acceso no autorizado	Desconocimiento del desarrollo de software suplantación de usuarios Perdida de código fuente	A.11.1.1 Perímetro de seguridad física
R23	[COM] Servicio de internet	[I8] Fallo de servicios de comunicaciones	Sin auditoria del cableado físico Redes sin mantenimiento	A13.1.2 Seguridad de los servicios de red
R24		[E4] Errores de configuración	Poca experiencia en configuración del equipo	A11.2.2 Instalaciones de suministro
R25	[COM] Servicio de internet	[I8] Fallo de servicios de comunicaciones	Falta de mantenimiento de la estructura de la red, suplantación de usuario.	A.11.1.4 Protección contra amenazas externas y ambientales
R26		[I8] Fallo de servicios de comunicaciones	Falta de mantenimiento de la estructura de la red.	A.11.1.4 Protección contra amenazas externas y ambientales
R27	[HW] Servidor Archivo FTP	[A11] Acceso no autorizado	Configuración de seguridad no optima	A9.1.2 Acceso a las redes y a los servicios de red A9.4.3 Sistema de gestión de contraseñas

Tabla 28. Tabla de activos, amenazas y controles actuales (continuación)

ID	Activo de información	Amenazas	Vulnerabilidades	Control aplicado actual
R28	[HW] Servidor de Impresión	[I7] Condiciones inadecuadas de temperatura o humedad	Mala ubicación de la red cableada	A12.4.1 Registro de eventos A9.1.2 Acceso a las redes y a los servicios de red
R29	[HW] Servidor de nómina y facturación	[I5] Avería de origen físico o lógico	Falla de fábrica, saboteo interno	A12.4.1 Registro de eventos
R30	[HW] Servidor DHCP	[I6] Corte del suministro eléctrico	Falla en la red eléctrica interna, falla externa	A12.4.1 Registro de eventos
R31	[SW] Sistemas de nómina y facturación	[A11] Acceso no autorizado	suplantación de Usuarios	A9.4.1 Restricción del acceso a la información
R32	[SW] Sistemas operativos win 10 Pro	[A23] Manipulación de los equipos	Mala manipulación del equipo, saboteo	A12.2.1 Controles contra el código malicioso
R33	[COM] Switches cisco catalyst 2960	[I5] Avería de origen físico o lógico	NOSTRADAMUS S.A.S al no contar con un sistema de seguridad biométrico o de monitoreo que permita tener control sobre la zona de sistemas.	A11.2.2 Instalaciones de suministro
R34		[I6] Corte del suministro eléctrico	Falla en la red eléctrica interna Falla externa	A.11.2.3 Seguridad del cableado
R35		[I*] Desastres industriales	Saboteo interno	A13.1.1 Controles de red

Tabla 29. Tabla de activos, amenazas y controles actuales (continuación)

ID	Activo de información	Amenazas	Vulnerabilidades	Control aplicado actual
R36	[P] Técnicos de mantenimiento	[I5] Avería de origen físico o lógico	Defectos de fabricación, vandalismo	A12.6.2 Restricción en la instalación de software A13.2.2 Acuerdos de intercambio de información A13.2.4 Acuerdos de confidencialidad o no revelación
R37	[COM] Teléfonos IP	[I6] Corte del suministro eléctrico	Falla en la red eléctrica interna, falla externa	A9.2.2 Suministro de acceso de usuarios

Fuente: *Autor*

Según la metodología MAGERIT[97] cuando un activo se ve afectado por una amenaza es necesario establecer el nivel del impacto que tiene sobre el activo, en otras palabras, que tan perjudicado se vio el activo por la materialización de la amenaza. De esto se sugiere la siguiente tabla de impacto:

Tabla 30. Escala de valoración del impacto

Nomenclatura	Categoría	Valoración
MA	Muy Alto	5
A	Alto	4
M	Medio	3
B	Bajo	2
MB	Muy Bajo	1

Fuente: *Autor*

[97] MA AMUTIO, J. Candau, y JA MAÑAS, *MAGERIT–versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II-Catálogo de Elementos* (Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012).

Además del impacto, debe evaluarse la probabilidad de que una amenaza se materialice; para ello Magerit también propone una escala nominal con valores de frecuencia:

Tabla 31. Escala de probabilidad de ocurrencia

Nomenclatura	Categoría	Valoración
S	Siempre	5
CS	Casi siempre	4
M	A menudo	3
AV	Algunas Veces	2
AN	Casi Nunca	1

Fuente: *Autor*

Teniendo en cuenta las escalas de valoración de impacto y probabilidad de que una amenaza se materialice, es necesario valorar cada uno de los activos en cuanto al impacto que cada una de las amenazas pueda tener sobre el activo y la probabilidad de que dicha amenaza se materialice.

Es importante tener en cuenta que la probabilidad de una vulnerabilidad depende de cada activo, no de la vulnerabilidad en sí.

Es justamente la calificación del impacto de una amenaza y la probabilidad de que esta se materialice lo que se denomina riesgo. A continuación, se presentará la valoración de las amenazas, teniendo en cuenta el identificador de amenaza utilizado en la Tabla de activos y amenazas, calificando su probabilidad e impacto según la naturaleza de la amenaza, descrita en la tabla 24:

Tabla 32. Tabla de activos y amenazas

ID	Activo	Amenaza	Probabilidad	Impacto
R1	[AUX] Cableado	[I8]	2	4
R2	[HW] Cortafuegos Cisco ASA 5505	[E2]	2	3
R3	[HW] Cortafuegos Cisco ASA 5505	[I6]	3	3
R4	[HW] Cortafuegos Cisco ASA 5505	[I7]	3	3
R5	[HW] Cortafuegos Cisco ASA 5505	[A8]	2	3
R6	[HW] Cortafuegos Cisco ASA 5505	[I5]	2	3
R7	[HW] Cortafuegos Cisco ASA 5505	[I6]	2	3
R8	[HW] Cortafuegos Cisco ASA 5505	[I*]	3	3
R9	[HW] Cortafuegos Cisco ASA 5505	[A26]	2	3
R10	[HW] Cortafuegos Cisco ASA 5505	[E20]	3	3
R11	[HW] Equipos de cómputo	[E21]	2	4
R12	[HW] Equipos de cómputo	[A26]	2	4
R13	[HW] Equipos de cómputo	[A11]	2	4
R14	[HW] Equipos de cómputo	[A5]	2	4
R15	[HW] Equipos de cómputo	[E19]	2	4
R16	[HW] Equipos de cómputo	[A6]	3	4
R17	[SW] Página Web	[I8]	2	5
R18	[COM] Puntos de acceso	[I*]	4	2
R19	[COM] Puntos de acceso alámbricos (hub)	[E4]	3	2
R20	[COM] Puntos de acceso alámbricos (hub)	[A11]	2	2
R21	[COM] Puntos de acceso alámbricos (hub)	[I5]	2	2
R22	[D] Respaldo de la información de los sistemas	[A11]	4	3
R23	[COM] Servicio de internet	[I8]	2	2
R24	[COM] Servicio de internet	[E4]	2	2
R25	[COM] Servicio de internet	[I8]	3	2
R26	[COM] Servicio de internet	[I8]	3	2
R27	[HW] Servidor Archivo FTP	[A11]	4	4
R28	[HW] Servidor de Impresión	[I7]	3	4
R29	[HW] Servidor de nómina y facturación	[I5]	3	4
R30	[HW] Servidor DHCP	[I6]	1	3
R31	[SW] Sistemas de nómina y facturación	[A11]	4	5
R32	[SW] Sistemas operativos win 10 Pro	[A23]	2	4
R33	[COM] Switches cisco catalyst 2960	[I5]	2	3
R34	[COM] Switches cisco catalyst 2960	[I6]	2	3
R35	[COM] Switches cisco catalyst 2960	[I*]	2	3
R36	[P] Técnicos de mantenimiento	[I5]	3	3
R37	[COM] Teléfonos IP	[I6]	3	5

Fuente: *Autor*

Una vez evaluada la probabilidad de ocurrencia y el impacto de cada una de las amenazas, se puede utilizar un mapa de calor, señalada en el libro 3 de técnicas de Magerit[98] como una herramienta visual y amigable que permite visualizar de manera rápida los valores de impacto y probabilidad de las amenazas. A continuación, se mostrará el mapa de calor resultante para el riesgo:

Figura 16. Mapa de calor del riesgo

PROBABILIDAD	MUY ALTA					
	ALTA		R18	R22	R27	R31
	MEDIA		R19, R25, R26	R3, R4, R8, R10, R36	R16, R28, R29	R37
	BAJA		R20, R21, R23, R24	R2, R5, R6, R7, R9, R33, R34, R35	R1, R11, R12, R13, R14, R15, R32	R17
	MUY BAJA			R30		
RIESGO		MUY BAJA	BAJA	MEDIA	ALTA	MUY ALTA
		IMPACTO				

Fuente: Autor

Luego de evaluar y visualizar la criticidad de los riesgos, es necesario realizar el tratamiento adecuado para mitigar cada riesgo al máximo, teniendo en cuenta que estos nunca desaparecen totalmente, pero puede disminuirse el daño al activo o la frecuencia de materialización de las amenazas, teniendo como resultado un riesgo residual que sea más fácil de controlar y predecir.

6.3.8 Fase 5: diseñar el SGSI

Son tres los componentes básicos para el diseño de un SGSI: La documentación obligatoria que debe tener el sistema, la implementación de los controles

[98] «Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro III: Guía de Técnicas», s. f., 42.

establecidos en el plan de tratamiento de riesgos y el monitoreo constante de la seguridad de la información.

Documentación del sistema

Los documentos que exige la norma ISO/IEC 27001 son el resultado de las fases ya mencionadas; una lista de chequeo de dichos documentos puede encontrarse en el ANEXO B de este documento.

Implementar el plan de tratamiento de riesgos

La alta dirección debe aprobar tanto el plan de tratamiento de riesgos, así como los recursos para llevarlo a cabo, así como el mantenimiento de los controles existentes, con el fin de que los riesgos se mantengan en el nivel de riesgo aceptado por la empresa. Por esta razón debe existir un monitoreo permanente sobre los controles y los nuevos escenarios de riesgos que puedan surgir con el pasar del tiempo.

Monitoreo de la seguridad de la información

La norma ISO/IEC 27001:2013, numeral 9, establece que la evaluación del desempeño del SGSI se debe realizar a través de la supervisión, medición, análisis y evaluación del sistema por medio de auditorías periódicas, por las personas denominadas para tal fin, y revisión de la alta dirección. Esto se mide con la definición de indicadores, desarrollados a nivel general del SGSI y la gestión de riesgos, que sirven para medir la eficacia y eficiencia de los controles establecidos. Se deben tener en cuenta tres normas al momento de establecer las auditorias: ISO 19022:2011, ISO/IEC 27007:2011, ISO/IEC TR-27008.

7 RESULTADOS

Con el desarrollo de este proyecto se obtienen los siguientes resultados:

Con respecto al enfoque técnico, mediante la aplicación de herramientas de pentesting como NMAP, Metasploit, LaZagne, Slow loris y SQLMap, se evidenció el grado de vulnerabilidad que tienen los equipos de NOSTRADAMUS S.A.S., según el ejercicio teórico, para que hubiesen sido exitosos los ataques de ingeniería social, elevación de privilegios, denegación de servicios, ataque ransomware y SQL injection.

Las herramientas utilizadas, en especial Kali Linux como agrupador de herramientas de pentesting, fueron de gran utilidad para la implementación del laboratorio de pentesting, a través del cual se ejecutaron en un entorno controlado ataques y defensas cibernéticas para el análisis de las vulnerabilidades mencionadas en el caso de estudio de NOSTRADAMUS S.A.S.

Se presenta una propuesta estratégica para la mitigación del riesgo de futuros ataques, incluyendo una propuesta comparativa para la implementación de un UTM en el que se incluya el monitoreo de red.

Frente al enfoque administrativo se plantea un diseño de proyecto para la implementación de un SGSI, basado en la norma ISO 27001, a través del cual se describen las características principales de un SGSI y, utilizando como base la información planteada en el caso de estudio de NOSTRADAMUS S.A.S, se establecen y analizan algunos de los conceptos fundamentales, como el alcance y las políticas del SGSI, listas de chequeo y metodologías de implementación de un SGSI.

Se realiza un análisis y la valoración de los riesgos asociados a los activos mencionados en el caso de estudio de NOSTRADAMUS S.A.S., así como la definición de los controles de seguridad de la información necesarios para mitigar los riesgos identificados.

Este proyecto en su totalidad está dirigido a fortalecer teóricamente tanto la seguridad informática como la seguridad de la información del caso de estudio NOSTRADAMUS S.A.S. Puede usarse como punto de referencia tanto para el desarrollo de un laboratorio de pentesting, con fines analíticos, como para la definición, construcción, puesta en marcha y monitoreo de un SGSI, con base en la norma 27001.

8 CONCLUSIONES

- Las herramientas de pentesting son un gran aporte a la seguridad informática ya que permiten a las organizaciones conocer de manera anticipada sus vulnerabilidades y sus sistemas e infraestructuras tecnológicas, especialmente ante aquellos servicios expuestos a internet, con el fin de mejorar su configuración.

- Existe una gran variedad de herramientas de pentesting, muchas de uso libre, entre las que se destacan algunas suites, o agrupadores, como Kali Linux, la cual ofrece utilidades que pueden usarse para el desarrollo de las pruebas de ataque y defensa cibernéticos.

- La implementación del laboratorio de pentesting permitió replicar los ataques cibernéticos del caso de estudio de NOSTRADAMUS S.A.S., con el fin de evaluar las mejores prácticas para la identificación, control y mitigación de vulnerabilidades presentes en los sistemas informáticos.

- La implementación de un SGSI en una organización debe ser una prioridad, con el fin de proteger los activos de información, tomando conciencia de la relevancia de diseñar, definir y establecer medidas que eviten la materialización de los riesgos que atenten contra la confidencialidad, integridad y disponibilidad de los activos informáticos de la organización.

- Se determinaron los riesgos, amenazas y vulnerabilidades que afectaron a NOSTRADAMUS S.A.S., según el inventario de activos del caso de estudio, lo cual permitió evidenciar cuales son los factores que ponen en riesgos los activos de información de una organización, y establecer cuáles son y como se deben utilizar los mecanismos para mitigarlos.

- Se realiza la verificación de controles de seguridad de la información mencionados en el caso de estudio de NOSTRADAMUS S.A.S., después de realizado el análisis y evaluación de riesgos, teniendo en cuenta los objetivos de control y controles de referencia basados en la norma ISO/IEC 27001, como un insumo para la mitigación de riesgos de la información.

- Se definen, de manera general, las directrices para la construcción de las políticas de seguridad de la información para NOSTRADAMUS S.A.S., lo que permite establecer mejores prácticas y lineamentos de seguridad de la información, además de proporcionar mecanismos y aspectos que deben ser aprobados por la alta gerencia de la organización, en busca de mantener la confidencialidad, integridad y disponibilidad de los activos informativos de la organización.

9 RECOMENDACIONES

- Hacer una constante evaluación de las vulnerabilidades tecnológicas de los sistemas de la organización, así como seguimiento a los controles establecidos, bien sea a través de la contratación de un tercero o la contratación directa de un especialista en seguridad informática que se encargue de realizar los estudios de pentesting.

- Existe un constante crecimiento de amenazas e identificación de vulnerabilidades que pone en riesgo la confidencialidad, integridad y disponibilidad de la información, por esto se hace de vital importancia invertir en controles suficientes que mitiguen los riesgos asociados a la pérdida de información y a recibir algún tipo de ataque informático. La implementación de un gestor unificado de amenazas (UTM) es una de las inversiones que toda organización debe hacer, especialmente si tiene servicios sensibles expuestos hacia internet.

- Es importante crear conciencia empresarial sobre la seguridad informática y la seguridad de la información, ya que en muchas ocasiones se presentan vulnerabilidades por usos indebidos de la tecnología o ser víctimas de ingeniería social, todo esto sin que el usuario sea consiente del error. Se debe crear la cultura de seguridad desde la alta gerencia y se deben establecer controles desde el área TIC.

- Mantener actualizados los sistemas disminuye la posibilidad de ataques informáticos, especialmente de los sistemas operativos, más aún si dichos equipos están expuestos a internet.

- Con respecto al plan para la implementación de un SGSI, el profesional en seguridad de la información no debe limitarse a las herramientas y normativas presentadas en el presente proyecto aplicado. Se recomienda realizar un análisis completo de las normas que permiten el diseño, implementación y seguimiento de un SGSI, con el fin de entender a profundidad cada una de las fases que lo componen.

- Desde el inicio será bueno contar con el respaldo de la alta gerencia y su apoyo a todo el proceso de diseño, implementación y mantenimiento de un SGSI. Este proceso sólo será eficaz y eficiente si se cuenta con el apoyo constante de la alta gerencia.

- La implementación de un SGSI no debe considerarse como una meta en sí, superada una vez se logra; el mantenimiento del sistema es de vital importancia para su éxito, por lo que se deben establecer revisiones periódicas y actualizaciones cada que sea necesario.

BIBLIOGRAFÍA

«(1) Kali Linux - Slowloris - DOS Attacking Tool - YouTube». Accedido 5 de mayo de 2019. https://www.youtube.com/watch?v=7LFKff42qEQ.

Almeida Coloma, Cesar Leonardo, y Jasson Alfredo Pincay Párraga. «Implementación de un laboratorio de seguridad de informática para la realización de técnicas de ataque y defensa (Pentesting) en un ambiente real controlado, utilizando una distribución de Kali Linux dentro de la empresa industrial siderúrgica Andec S.A.» Thesis, Universidad de Guayaquil. Facultad de Ciencias Matemáticas y Físicas. Carrera de Ingeniería En Networking y Telecomunicaciones, 2018. http://repositorio.ug.edu.ec/handle/redug/35450.

Ampuero Chang, Carlos. «Diseño de un Sistema de Gestión de Seguridad de Información para una compañía de Seguros», 2011. https://core.ac.uk/download/pdf/71403748.pdf.

AMUTIO, MA, J. Candau, y JA MAÑAS. *MAGERIT–versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II-Catálogo de Elementos*. Madrid: Ministerio de Hacienda y Administraciones Públicas, 2012.

«Análisis comparativo de los principales sistemas antivirus». Accedido 5 de mayo de 2019. http://scielo.sld.cu/scielo.php?pid=S1024-94352003000500005&script=sci_arttext&tlng=en.

«Análisis de riesgos en seguridad de la información | Ciencia, Innovación y Tecnología». Accedido 19 de abril de 2019. https://www.jdc.edu.co/revistas/index.php/rciyt/article/view/121.

antony daubuoi. *exploit ms17-010 with metasploit in kali-linux*. Accedido 28 de abril de 2019. https://www.youtube.com/watch?v=wpvWFEmqR-s.

Barrios, Monterroza, y Rafael Enrique. «Análisis, explotación y definición de estrategias de mitigación de vulnerabilidades en un sistema GNU/Linux», 7 de enero de 2019. http://openaccess.uoc.edu/webapps/o2/handle/10609/91846.

BetaFred. «Microsoft Security Bulletin MS17-010 - Critical». Accedido 28 de abril de 2019. https://docs.microsoft.com/en-us/security-updates/securitybulletins/2017/ms17-010.

Blanco, Esquerra, y Liliana de la Caridad. «Pruebas de penetración con la herramienta Kali Linux en la Universidad Central Marta Abreu de las Villas». Thesis, Universidad Central «Marta Abreu» de Las Villas, 2014. http://dspace.uclv.edu.cu/bitstream/handle/123456789/1350/Liliana%20de%20la%20Caridad%20Esquerra%20Blanco.pdf?sequence=1&isAllowed=y.

Bombón, Pichucho, y Jorge Aníbal. «ELABORACIÓN DE UN MÓDULO PARA PRÁCTICAS DE LABORATORIO DE GESTIÓN UNIFICADA DE AMENAZAS EN LA UNIVERSIDAD ISRAEL», 2017. https://repositorio.uisrael.edu.ec/handle/47000/1401.

Buiron, Hoyos, y Victor Antonio. «¿Que tal esta Colombia en cuestion de ciberseguridad?», 28 de enero de 2016. http://repository.unimilitar.edu.co/handle/10654/7794.

Cano, Jeimy J. «Inseguridad informática: un concepto dual en seguridad informática.» *Revista de Ingeniería* 0, n.º 19 (2004): 40-44-44. https://doi.org/10.16924/riua.v0i19.437.

Cañon Parada, Lady Johana. «Ataques informáticos, Ethical Hacking y conciencia de seguridad informática en niños». Universidad Piloto de Colombia, 2015. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2870/00002427.pdf?sequence=1. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2870/00002427.pdf?sequence=1.

Cardenas, Riveros, y Fredy Orlando. «Administración del riesgo cibernetico un enfoque desde la alta gerencia empresarial en Colombia». *observatorio de la ciberseguridad para america latina y el caribe. (10 de enero de 2016). observatorio de ciberseguridad. organizacion de estados americanos: banco interamericano de desarrollo. Obtenido de observatorio de ciberseguridad .*, 31 de enero de 2017. http://repository.unimilitar.edu.co/handle/10654/15837.

Cesar R. Cuenca Díaz. «Desarrollo Seguro: Principios y Buenas Prácticas», s. f., 23.

Ch, Raj, y el. «Múltiples formas de omitir UAC utilizando Metasploit», 16 de septiembre de 2018. //www.hackingarticles.in/multiple-ways-to-bypass-uac-using-metasploit/.

Clavijo, Ciro Antonio Dussán. «Políticas de seguridad informática». *Entramado* 2, n.º 1 (1 de junio de 2006): 86-92.

Colombiano, El. «Colombia, el sexto país con más ciberataques en 2017». www.elcolombiano.com. Accedido 18 de abril de 2019. https://www.elcolombiano.com/colombia/ciberataques-en-colombia-sexto-pais-mas-vulnerable-en-la-region-AB8535174.

coreyp-at-msft. «Cipher». Accedido 28 de abril de 2019. https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/cipher.

Cortés Borrero, Rodrigo. «Estado actual de la política pública de ciberseguridad y ciberdefensa en Colombia». *instname:Universidad Santo Tomás*, 2015. http://repository.usta.edu.co/handle/11634/14032.

Crespo, Adrián. «LaZagne, una utilidad que permite recuperar contraseñas de Windows y Linux». RedesZone, 28 de mayo de 2015. https://www.redeszone.net/2015/05/28/lazagne-una-utilidad-que-permite-recuperar-contrasenas-de-windows-y-linux/.

Cyber Shield. *Exploit Internet Explorer 8 on win 7*. Accedido 20 de abril de 2019. https://www.youtube.com/watch?v=h8xOnfQlxDE.

Dittrich, David, y Kenneth E. Himma. «Hackers, crackers, and computer criminals». *Handbook of Information Security. Bakersfield, CA: California State University*, 2006, 154-72.

«Escalar Privilegios en Windows Evadiendo UAC | Alonso Caballero / ReYDeS». Accedido 28 de abril de 2019. http://www.reydes.com/d/?q=Escalar_Privilegios_en_Windows_Evadiendo_UAC.

Espinosa, Villacís, y Miguel Leopoldo. «Diseño de un sistema de gestión de la seguridad de la información (SGSI) basado en la norma ISO 27001:2013 para la red corporativa de la empresa Ecuatronix.», febrero de 2016. http://dspace.ups.edu.ec/handle/123456789/12406.

«Exploiting MS11_003 Internet Explorer Vulnerability Using Metasploit Framework». Accedido 28 de abril de 2019. https://www.hacking-tutorial.com/hacking-tutorial/exploiting-ms11_003-internet-explorer-vulnerability-using-metasploit-framework/#sthash.rIdwMmbq.dpbs.

Juan Oliva. «Explotando Vulnerabilidad MS17-010 o WannaCry», 1 de junio de 2017. https://jroliva.net/2017/06/01/explotando-vulnerabilidad-wannacry-o-ms17-010/.

Flores, Aliaga, y Luis Carlos. «Diseño de un sistema de gestión de seguridad de información para un instituto educativo». *Pontificia Universidad Católica del Perú*, 2 de septiembre de 2013. http://tesis.pucp.edu.pe/repositorio//handle/20.500.12404/4721.

Fula Perilla, Pedro Antonio. «Lineamientos de política para ciberseguridad y ciberdefensa, documento CONPES 3701», 2016. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2723/00003294.pdf?sequence=1.

Gacharná, Federico Iván Gacharná. «El estigma Hacker, entre lo bueno y lo malo». *INVENTUM* 6, n.º 10 (1 de febrero de 2011): 24-27. https://doi.org/10.26620/uniminuto.inventum.6.10.2011.24-27.

Gijon, Florentino Mendez, Adrian Aquino Robles, Armando Ronquillo Jorge, y José Guillermo Valdez Besares. «Técnicas de Hacking Ético en un Laboratorio de Pentesting Virtualizado», 2011. https://www.researchgate.net/profile/Armando_Ronquillo/publication/308312418_Tecnicas_de_Hacking_Etico_en_un_Laboratorio_de_Pentesting_Virtualizado/links/57e04ed608aece48e9e1f4b4/Tecnicas-de-Hacking-Etico-en-un-Laboratorio-de-Pentesting-Virtualizado.pdf.

Gil Vera, Víctor Daniel, y Juan Carlos Gil Vera. «Seguridad informática organizacional: un modelo de simulación basado en dinámica de sistemas». *Scientia Et Technica* 22, n.º 2 (2017). http://www.redalyc.org/resumen.oa?id=84953103011.

Gómez, Ricardo, Diego Hernán Pérez, Yezid Donoso, y Andrea Herrera. «Metodología y gobierno de la gestión de riesgos de tecnologías de la información». *Revista de Ingeniería* 0, n.º 31 (23 de agosto de 2010): 109-118-118. https://doi.org/10.16924/riua.v0i31.217.

Guillem, Ferrando, y Anna Lourdes. «La ciberseguridad como reto internacional: la protección frente a las ciberamenazas», diciembre de 2018. http://openaccess.uoc.edu/webapps/o2/handle/10609/88685.

«idUS - Implementación y medida del rendimiento de un firewall para aplicaciones web (WAF) en un balanceador de carga». Accedido 5 de mayo de 2019. https://idus.us.es/xmlui/handle/11441/85834.

«ISO27k infosec management standards». Accedido 14 de octubre de 2019. https://www.iso27001security.com/.

Jara, Hector, y Federico G Pacheco. *Ethical Hacking 2.0*. Usershop, 2012. https://books.google.com.co/books?hl=es&lr=lang_es&id=PkDCIzakkB4C&oi=fnd&pg=PA4&dq=riesgo+de+ethical+hacking&ots=B4x48Tz38q&sig=LtD_o7zAxvXnRrsMzFPMkvrOHRY&redir_esc=y#v=onepage&q=riesgo%20de%20ethical%20hacking&f=false.

Macedo, Víctor Gabriel Reyes, y Moisés Salinas-Rosales. «WannaCry: Análisis del movimiento de recursos financieros en el blockchain de bitcoin.» *Research in Computing Science* 137 (2017): 147-55.

Macía Fernández, Gabriel. «Ataques de denegación de servicio a baja tasa contra servidores», 2007. http://digibug.ugr.es/bitstream/handle/10481/1543/16714763.pdf?sequence=1.

MAGERIT, Llibre II. «Catálogo de elementos». *Portal d'administració*, s. f.

«Magerit versión 3.0: Metodología de análisis y gestión de riesgos de los Sistemas de Información. Libro III: Guía de Técnicas», s. f., 42.

Martínez, R, y A García-Beltrán. «BREVE HISTORIA DE LA INFORMÁTICA», s. f., 20.

McKinley, Korey. «Manually Exploiting MS17-010». *LMG Security* (blog), 20 de febrero de 2018. https://lmgsecurity.com/manually-exploiting-ms17-010/.

Méndez Carvajal, Alejandro. «Estudio de metodologías de ingeniería social», diciembre de 2018. http://openaccess.uoc.edu/webapps/o2/handle/10609/90305.

Mendez, Monsalve, y Jaime Yesid. «Ciberseguridad: Principales Amenazas En Colombia (Ingeniería Social, Phishing y Dos)», 21 de noviembre de 2018. http://repository.unipiloto.edu.co/handle/20.500.12277/4663.

«Meterpreter Basic Commands». Accedido 28 de abril de 2019. https://www.offensive-security.com/metasploit-unleashed/meterpreter-basics/.

Nieves, Arlenys Carolina. «Diseño de un sistema de gestión de la seguridad de la información (SGSI) basados en la norma Iso/iec 27001:2013», 4 de agosto de 2017. http://alejandria.poligran.edu.co/handle/10823/994.

Ojeda-Pérez, Jorge Eliécer, Fernando Rincón-Rodríguez, Miguel Eugenio Arias-Flórez, y Libardo Alberto Daza-Martínez. «Delitos informáticos y entorno jurídico vigente en Colombia». *Cuadernos de Contabilidad* 11, n.º 28 (1 de junio de 2010). https://revistas.javeriana.edu.co/index.php/cuacont/article/view/3176.

Olmedo, Jorge Izaguirre, y Fernando León Gavilánez. «Análisis de los Ciberataques realizados en América Latina.» *INNOVA Research Journal* 3, n.º 9 (2018): 180-89.

Pallas, Gustavo, y María Eugenia Corti. «Metodología de Implantación de un SGSI en grupos empresariales de relación jerárquica». *Uruguay Magister Thesis: Universidad de la República*, 2009.

Pinzón, J. «Acercamiento a la Gestión de Riesgos con Magerit y las 4A». *Bogotá: sn*, 2009.

Proyecto de grado - Alejandro Mejia Escobar. Accedido 14 de octubre de 2019. https://www.youtube.com/watch?v=6at_3GJ8Tvg&feature=youtu.be.

Ramirez, Viver, y Aydee Mercedes. «Identificación de vulnerabilidades de la red LAN del Buque Oceanográfico de la autoridad Colombiana a través de las herramientas de pruebas de Pentesting.», 14 de junio de 2017. https://repository.unad.edu.co/bitstream/10596/12425/1/46646702.pdf.

«Repositorio Universidad de Guayaquil: Implementación de un gestor unificado de amenazas de seguridad para la red administrativa de la carrera de Ingeniería de Sistemas Computacionales, basado en el análisis de su infraestructura de red interna y de perímetro.» Accedido 5 de mayo de 2019. http://repositorio.ug.edu.ec/handle/redug/6672.

Rodríguez, Juan Antonio, Jesús Oduber, y Endira Mora. «Actividades rutinarias y cibervictimización en Venezuela». *URVIO: Revista Latinoamericana de Estudios de Seguridad*, n.º 20 (2017): 63-79.

Romero, Cadavid, y Diego Fernando. «Hallazgos de vulnerabilidades en los sistemas operativos y base de datos de la empresa ALDIM Acciones Logísticas en Distribución de Mercancías S.A.S.», 16 de marzo de 2018. http://repository.unad.edu.co/handle/10596/17412.

«RUA: Práctica 3. Protocolos de transporte TCP y UDP». Accedido 13 de octubre de 2019. http://rua.ua.es/dspace/handle/10045/11606.

Salinas, Salinas, y Wilson Enrique. «Comparación de los sistemas de gestión unificado y dispositivos de propósito específico que ayudan a prevenir las amenazas informáticas a que están expuestas las Pymes», 2013. http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/2591/00000789.pdf?sequence=1.

«Slowloris DDoS Attack | Cloudflare». Accedido 5 de mayo de 2019. https://www.cloudflare.com/learning/ddos/ddos-attack-tools/slowloris/.

Solarte, Francisco Nicolás Solarte, Edgar Rodrigo Enriquez Rosero, y Mirian del Carmen Benavides. «Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001». *Revista Tecnológica - ESPOL* 28, n.º 5 (31 de diciembre de 2015). http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456.

«Técnicas de mitigación para principales vulnerabilidades de seguridad en aplicaciones web - ProQuest». Accedido 5 de mayo de 2019. https://search.proquest.com/openview/ef48269d2b309b464f6d0070f79eee7b/1?pq-origsite=gscholar&cbl=1006393.

Trigo, Santiago, Martín Castellote, Ariel Podestá, Gonzalo Ruiz de Angeli, Sabrina Lamperti, y Bruno Constanzo. «Ransomware: seguridad, investigación y tareas forenses», 2017. http://hdl.handle.net/10915/65216.

Valencia-Duque, Francisco Javier, y Mauricio Orozco-Alzate. «Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000». *RISTI - Revista Ibérica de Sistemas e Tecnologias de Informação*, n.º 22 (junio de 2017): 73-88. https://doi.org/10.17013/risti.22.73-88.

Vect0r. *LaZagne Get all Passwords on a Computer (Windows and Linux)*. Accedido 28 de abril de 2019. https://www.youtube.com/watch?v=tyXFUBUeUDo.

Zafra, Guillén, y José Luis. «Introducción al pentesting», 20 de julio de 2017. http://diposit.ub.edu/dspace/bitstream/2445/124085/2/memoria.pdf.

Zanabria Ticona, Edson Denis, y Edwin Cayo Mamani. «Seguridad informática en dispositivos móviles con Sistemas Operativos Android mediante Pentesting». *Universidad Nacional del Altiplano*, 13 de abril de 2018. http://repositorio.unap.edu.pe/handle/UNAP/7047.

ANEXOS

ANEXO A – VIDEO DE PENTESTING

Proyecto de grado - Alejandro Mejia Escobar. (2019). YouTube. Recuperado el 17 de mayo 2019, desde https://www.youtube.com/watch?v=6at_3GJ8Tvg&feature=youtu.be

ANEXO B – LISTAS DE CHEQUEO

Lista de checkeo para el control de estado de implementación de la ISO 27001 y el estado y aplicabilidad de controles de seguridad de la información. Archivo basado en el documento "*ISO/IEC 27001:2013 ISMS Status, Statement of Applicability (SoA) and Controls Status (gap analysis) workbook*", extraido de http://www.ISO27001security.com