RECREACIÓN EN AMBIENTES CONTROLADOS PARA EL ANÁLISIS DE ATAQUES INFORMÁTICOS SUFRIDOS POR LA COMPAÑÍA DEL CASO DE ESTUDIO NOSTRADAMUS SAS, Y EL DISEÑO DE PROPUESTA DE ASEGURAMIENTO TOMANDO COMO REFERENCIA LA NORMATIVA ISO 27032 Y LA NORMATIVA ISO 27001

Delford J. Molinares Borda

Brinis Yosed Polo Polo

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ

2019

RECREACIÓN EN AMBIENTES CONTROLADOS PARA EL ANÁLISIS DE ATAQUES INFORMÁTICOS SUFRIDOS POR LA COMPAÑÍA DEL CASO DE ESTUDIO NOSTRADAMUS SAS, Y EL DISEÑO DE PROPUESTA DE ASEGURAMIENTO TOMANDO COMO REFERENCIA LA NORMATIVA ISO 27032 Y LA NORMATIVA ISO 27001

Delford J. Molinares Borda

Brinis Yosed Polo Polo

Trabajo de grado para optar por el título:

Especialista en Seguridad Informática

Director de Proyecto:

Yenny Stella Nuñez Alvarez

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA

ESCUELA DE CIENCIAS BÁSICAS TECNOLOGÍA E INGENIERÍA - ECBTI

ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA

BOGOTÁ

2019

Nota de Aceptación:

_____
_____
_____
_____
_____
_____
_____
_____

_____
Firma presidente del Jurado

_____
Firma Jurado

_____
Firma Jurado

Bogotá,_____de_____de 20____

DEDICATORIA

“El presente informe lo dedicamos primeramente a Dios, ya que es nuestro guía y darnos fuerzas en este proceso de obtener uno de nuestros logros; a nuestros padres por imprimir en nosotros el deseo de seguir siempre adelante, por los consejos, valores y principios que nos han inculcado; a nuestra familia por apoyo y comprensión, apoyo y creer en nuestros proyectos personales y profesionales, por ser nuestros motores en la vida para seguir creciendo profesionalmente; a la universidad nacional abierta y a distancia, por permitirnos realizar este paso que es muy importante en nuestras formación; a nuestros familiares, amigos, compañeros y conocidos por su apoyo y sus buenos consejos, animo, y por permitirnos aprender de ellos y de sus experiencias de vida”.

AGRADECIMIENTOS

“Son muchas las personas que han contribuido en el proceso y conclusión de este trabajo. En primer lugar le agradecemos a Dios por ser nuestro guía y por darnos las fuerzas necesarias para culminar de la mejor manera este paso de formación que significa mucho para nosotros; gracias a nuestros docentes por orientarnos en este camino, por compartir con nosotros su conocimiento y permitirnos aprender de ellos; gracias a nuestros padres por estar siempre apoyándonos y confiando en nosotros; gracias a nuestras familias por ser quienes nos motivan a seguir en cada paso que damos, por confiar en nosotros y apoyarnos en este gran paso; gracias también a nuestros amigos, compañeros y conocidos por aportarnos un poco de su conocimiento, por apoyarnos y motivarnos en todas las situaciones. Gracias a todas estas personas por hacer parte de este gran proyecto, cada aporte significó mucho en nuestra carrera.”

CONTENIDO

LISTA DE TABLAS

LISTA DE ILUSTRACIONES

LISTA DE ANEXOS

RESUMEN

NOSTRADAMUS S.A.S, es una empresa del sector tecnológico que brinda servicios a los sectores: educativo, corporativo y gubernamental en temas relacionados con proyectos de educación y capacitación a través del uso de TIC. Recientemente sufrió un ataque informático que afecto la imagen corporativa de la organización presentándose robo de información a partir de ataques remotos.

La empresa Zero Day Ltda. busca recrear los ataques informáticos con el fin de poder establecer las causas que originaron los incidentes, todo esto en ambientes controlados; además de realizar pruebas de penetración en busca de otras fallas o huecos de seguridad.

El marco para la ejecución de este informe tiene como finalidad ser el disparador de un conjunto de actividades o plan de trabajo que deberá desarrollar NOSTRADAMUS S.A.S de para reforzar al máximo la seguridad de está. Una vez sea entregado el resultado final de los pasos realizados por Zero Day Ltda. En un Informe para las Directivas de Nostradamus S.A.S, con las salvaguardas a implementar para la mitigación de las técnicas de ataques origen del robo de información, así como robustecer las políticas de seguridad de la red.

PALABRAS CLAVES: Seguridad informática, Ciberseguridad, Riesgos, Salvaguarda, ISO 27001, ISO 27032, SGSI, Confidencialidad, Integridad, Disponibilidad

ABSTRACT

NOSTRADAMUS S.A.S, is a company in the technology sector that provides services to the sectors: educational, corporate and government on issues related to education and training projects through the use of ICT. Recently he suffered a computer attack that affected the corporate image of the organization, reporting theft from remote attacks.

The company Zero Day Ltda. Seeks to recreate computer attacks in order to establish the causes that led to the incidents, all this in controlled environments; in addition to performing penetration tests in search of other failures or security holes.

The framework for the execution of this report is intended to be the trigger for a set of activities or work plan to be developed by NOSTRADAMUS S.A.S to reinforce the maximum security of this. Once the final result of the steps carried out by Zero Day Ltda. is delivered. In a Report for the Directives of Nostradamus SAS, with the safeguards to be implemented for the mitigation of the attack techniques origin of the theft of information, as well as to strengthen the policies of network security.

KEYWORDS: Informatic Security, Ciberseguridad, Risk, Safeguard, ISO 27001, ISO 27032, SGSI, Confidentiality, Integrity, Availability

INTRODUCCIÓN

La masificación del internet nos ha permitido estar más conectados y también nos ha cambiado nuestro estilo de vida, como nos comunicamos, y la forma de interactuar con nuestros semejantes. También ha facilitado que la información cobre cierta relevancia y sea hoy por hoy, el activado de mayor valor en cualquiera organización y para los usuarios.

El no dar un tratamiento adecuado a la información que se maneja en una entidad puede acarrear incumplimientos de normas vigentes, perdida de reputación y la quiebra de la misma; es aquí cuando toma sentido la adopción de un sistema de gestión de seguridad de la información (en adelante SGSI), el cual busca aplicar y consolidar en una empresa estándares que faciliten mejorar el manejo de la información, cualquiera sea su campo de acción; alineado los objetivos corporativos y legislaciones; ayudando además a conseguir un grado de madurez que ayude a la empresa a certificarse y de esta manera, monetizar toda esa experiencia que se acumula con el ciclo de mejora continua que incluye la implementación del SGSI.

Lo que busca este trabajo es presentar una propuesta que sirva de referencia a la entidad para la implementación de un SGSI, alineado a la misión y visión de esta y al cumplimiento de los objetivos corporativos, mitigando y en la medida de lo posible evitando se repitan sucesos como los descritos en el informe de los ataques recibidos.

1. PLANTEAMIENTO DEL PROBLEMA

DESCRIPCIÓN

La compañía NOSTRADAMUS SAS ha sufrido una sucesión de ataques cibernéticos, con los cuales han realizado robo de información importante, afectado su imagen corporativa a nivel global. Esto debido a que cuenta son sistemas débiles de protección para sus sistemas informáticos y no tienen implementados controles y políticas necesarias para prever e identificar ataques antes de que afecten sus Sistemas Informáticos.

A raíz estos problemas a decidido contratar una consultaría en Seguridad Informática con el fin de recrear estos ataques bajo ambientes controlados simulando las vulnerabilidades que los propiciaron. Estos ataques recibidos por la empresa NOSTRADAMUS SAS son los siguientes:

- Ramsonware.
- Denegación de Servicio.
- Infiltración de usuarios no permitidos por medio de elevación de privilegios.
- Inyección SQL.

1.2 FORMULACIÓN DEL PROBLEMA

¿Qué normas o estándares pueden servir de apoyo a NOSTRADAMUS SAS para establecer una política de seguridad y una postura tecnica, que facilite mitigar daños ante ataques cibernéticos y en forma paralela, facilite el logro de la misión y visión de esta?

2. JUSTIFICACIÓN

La masificación del internet ha permitido que cada vez haya más empresas conectadas en todo el mundo, pero también ha aumentado la necesidad de un departamento de ciberseguridad, pues al estar conectados también se está expuesto a ataques cibernéticos.

En 2018 durante el primer semestre del año fueron logro identificar unos 1,4 millones de ataques cifrados.

Esto supone un incremento del 275% en comparación con el año inmediatamente anterior. De estos datos se puede concluir que el 55% de las organizaciones a nivel global han sufrido de un ataque de Ransomware. Dentro de ellas, solo el 49,4% de pago por un rescate para recuperar la información[1].

Por todo lo anterior este proyecto busca que NOSTRADAMUS S.A.S, pueda evitar ser víctimas de alguna de estas modalidades de ataques, logrando implementar un sistema de seguridad informática y de la información, eficiente y eficaz; que cuente con el compromiso de todos, desde las directivas, hasta los usuarios. Además de contar con capacitaciones constantes al eslabón más débil y difícil de controlar en un sistema de información “el usuario final”.

[1] Tomado de https://sicrom.com/blog/ultimos-ataques-ciberseguridad-empresas/

3. OBJETIVOS

3.1 GENERAL

Diseño de un SGSI para la empresa del caso de estudio NOSTRADAMUS SAS, basados en el análisis y estudios realizados a los ataques presentados en dicha empresa, tomando como referencias las normas ISO 27000 e ISO 27032.

3.2 OBJETIVOS ESPECÍFICOS

- Recrear bajo un ambiente controlado los ataques sufridos por NOSTRADAMUS SAS, para la obtención de información sobre ellos y generar un informe gerencial con base a los resultados obtenidos en el análisis forense.

- Realizar un análisis de soluciones UTM de código abierto y dispositivos, que permita implementarse en la compañía NOSTRADAMUS SAS, de acuerdo con las buenas prácticas y técnicas de aseguramiento de la información.

- Realizar un análisis de riesgos de los activos de la compañía NOSTRADAMUS SAS basados en la metodología Magerit para plantear propuestas para la gestión de estos.

- Diseñar un SGSI basados en la norma ISO 27001 y 27032 que ayude a mitigar los riesgos y vulnerabilidades que presenta la compañía NOSTRADAMUS SAS.

4. MARCO REFERENCIAL

El pasado mes de marzo de 2019 ce celebraron 30 años del nacimiento de lo que hoy se conoce como internet, este último cual sin lugar a duda alguna ha cambiado la vida de muchas personas en el mundo, cosas como el comercio, la banca, la forma en que nos comunicamos no se realizan de la misma manera que años atrás. Pero no han sido avances o cambios para bien, pues esto también ha traído consigo dificultades, como el estar cada más expuestos, específicamente nuestra información, la cual ha cobrado mayor valor y relevancia en estos tiempos de digitalización.

Actualmente nos encontramos en la era de la tecnología, por lo cual la organización debe tener como principal objetivo el cuidado, la seguridad y la excedencia de su información; entre más tecnología y reconocimiento de la organización, mayor será el riesgo de la información al no existir una seguridad adecuada contra amenazas y debilidades.

Con normas preestablecidas y con una adecuada gestión de la información esta permitirá a la organización asegurar la disponibilidad de la información manejada. (htt2)

5. MARCO CONCEPTUAL

5.1 RIESGO INFORMÁTICO.

Es la posibilidad de que un suceso inesperado pueda evitar el cumplimiento de un objetivo, o interrumpir la prestación de un servicio. En temas específicos de seguridad informática existen diferentes riesgos a los que la información está expuesta pasando por riesgos físicos, ambiénteles o los lógicos.

Sin embargo, los riesgos pueden tratarse. Si somos precavidos en nuestra relación con el ambiente, y si tenemos pleno conocimiento de nuestras debilidades y vulnerabilidades frente a las amenazas existentes, podemos tomar acciones correctivas para mitigar o eliminar la posibilidad de que las amenazas no se conviertan en desastres. (htt)

5.2 MAGERIT.

Es una metodología realizar un análisis y medición de los riesgos a tratarse, permitiendo conocer la probabilidad vs el impacto del riesgo. Esta metodología también permite tipificar los elementos base del estudio de riesgos.

Una vez identificado y estimado, se puede conocer evaluar y así definir el tratamiento que se le dará al mismo; siendo las tres posibles opciones aceptar, controlar, mitigar, transferir.

Esta metodología suele ser una de las herramientas de trabajo a utilizar en la implementación o estudios de riegos necesarios en las normas ISO/IEC 3100; ISO/IEC 27032, ISO/IEC 27001, entre otras.

5.3 SGSI.

SGSI hace referencia a un Sistema de Gestión de la Seguridad de la información. Este permitirá establecer una metodología de trabajo para la gestión de la seguridad de la información de forma clara e involucrando a todos áreas de la compañía.

Este sistema viene integrado con la mejora continua, lo que implica que contantemente se debe está revisando los riesgos y controles propuestos para los mismos. Además, permite la integración con otras normas como: ISO 9001, ISO 14001, ISO 31000, OHSAS 18001, entre otras.

5.4 INFORME GERENCIAL.

Aplicado a la seguridad informática, un informe gerencial permitirá resumir el estado de la postura de seguridad de la información en la empresa o ambiente del cual se desee realizar el análisis, en él se indicarán las brechas, vulnerabilidades que sean halladas y las salvaguardas que se deben implementar para cerrarlas dichas brechas o eliminar dichas vulnerabilidades. Además de evidenciar las vulnerabilidades logias también se físicas evidenciarlas las físicas, humanas, las

naturales entre otras; pero en ultimas será responsabilidad de la entidad en estudio tomar las acciones necesarias y señaladas para poder robustecer la postura de seguridad de esta.

5.5 UTM (UNIFIED THREAT MANAGEMENT).

Los UTM son la evolución de los Firewall y dispositivos VPN, debido a que no solo brindan estas funcionalidades, si no que integran varios elementos o módulos que ayudan a combatir muchas de las amenazas a las cueles están expuestas nuestro centro de datos.

Estos UTM pueden contener los servicios de Firewall, VPN, Antivirus perimetral, AntiSPAM, IPS, entre otros. Y resultan una buena opción a la hora de proteger de manera perimetral cualquier red de datos.

5.6 ATAQUE INFORMÁTICOS.

Son considerados ataques Informáticos a todas aquellas acciones que aproveche una vulnerabilidad o debilidad en dispositivos (Hardware), software, o personas, con el fin de obtener algún beneficio o causar daños sobre algún dispositivo, o sistema informático.

5.6.1 Ingeniería Social. Se catalogan como ataques de Ingeniería Social a los que van dirigido directamente a las personas, haciendo que realicen ciertas acciones por medio de engaños. El más común son los emails en los cuales solicitan información bancaria o personal.

5.6.2 Elevación de privilegios. Es un fallo de seguridad ocasionado cuando un usuario puede aumentar los permisos inicialmente otorgados dentro de un sistema informativo para acceder a información o servicios a los que no tiene autorización legitima; esta vulnerabilidad esta originada por brechas facilitan ataques de denegación de servicio o descubrimiento de información.

5.6.3 Denegación de Servicio. Los ataques de denegación de servicio tienen como objetivo dejar indisponible algún servicio sobre una red de datos, estos se realizan mediando el envío de peticiones o tráfico sobre los canales de comunicación y dispositivos donde se prestan estos servicios.

5.6.4 Ransomware. Este es un tipo de Malware cuyo fin es el de secuestrar información y solicitar rescate por ella. Estos ataques son perpetuados principalmente con ayuda de ingeniería social. Y son considerados delitos informáticos.

5.6.5 Inyección de SQL. Estos ataques consisten en la inserción de código SQL sobre una consulta tipo SQL en una página Web para la modificación de una base de datos, elevación de privilegios, acciones no deseadas en la BD, entre otras. [8]

5.6.6 Virtualizador e Hipervisores. Es un Software que simula un servidor físico sobre un ambiente virtual, y que administra la infraestructura de física de la máquina que lo aloja para la emulación de las máquinas virtuales, estos virtualizadores incluyen un hipervisor que se encarga de monitorear las máquinas virtuales.

Encontramos varios virtualizadores con licencias gratuitas y pagan. Los más populares son los siguientes:

- VMWARE
- VirtualBox
- Cameyo
- Xen Hypervisor
- Citrix XenServer
- Microsoft Hyper-V Server

5.7 KALI LINUX

Kali Linux es una distribución de Linux inicialmente basada en Ubuntu y en las últimas versiones se basa en Debian, el cual contiene diversas herramientas que ayudan a realizar auditoría y analizar la seguridad en una red.

Aunque las herramientas que contiene Kali Linux ayudan a ejecutar ataques cibernéticos, estás están diseñadas para usarse de manera ética o educativa. También podemos realizar análisis para detección de vulnerabilidades, fallas, y actividades que no realicen daño a terceros.

5.8 SOC

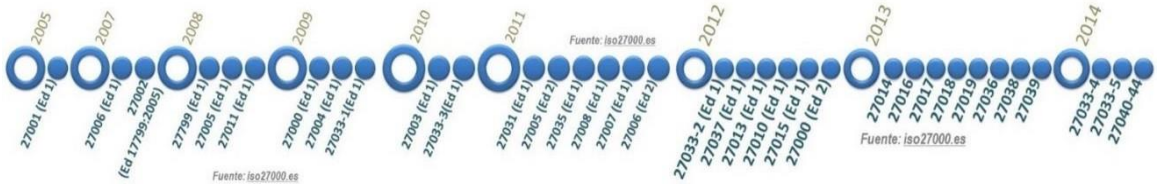
El SOC es un centro de operación que monitorea en tiempo real los sistemas de seguridad de una compañía o clientes, con el fin de realizar acciones proactivas que ayuden a mitigar los riesgos a los cuales están expuestos. Además, recolectan información con el fin de plantear sistemas más seguros y la mejora continua.

En la ilustración 1 observamos las diferentes normas generadas por la ISO y los años de publicación de estas.

5.9 NORMAS ISO/IEC 27000

la norma 27000 y entrega las bases de la importancia de la implantación de un SGSI, así como los pasos para el establecer, monitorear, mantener y mejorar un SGSI. involucra dentro de si el ciclo de mejora continua (deming Plan-Do-Check-Act) para buscar la madures del SGSI.

Ilustración 1 Evolución Norma 27000 (htt3)



Fuente: http://www.iso27000.es/iso27000.html

5.9.1 ISO/IEC 27001. Es una norma que busca la protección de la información sin importar el formato en que se maneje la misma; es decir los sistemas de información en lo referente al acceso, uso de estos, divulgación, interrupción de la disponibilidad de esta, modificación o destrucción no autorizados; con lo anterior busca garantizar la Confidencialidad, Integridad y Disponibilidad de la información independiente si esta se encuentra impresa, digital, o sea una propiedad intelectual.

5.9.2 ISO/IEC 27002. Es una guía de buenas prácticas en la cual describe los dominios y controles recomendados en cuanto a seguridad de la información.

5.9.3 ISO/IEC 27006. Especifica los requisitos para la acreditación a entidades de auditoría y certificación de sistemas de gestión de seguridad de la información. Es una versión revisada de EA-7/03 (Requisitos para la acreditación de entidades que operan certificación/registro de SGSIs) que añade a ISO/IEC 17021 (Requisitos para las entidades de auditoría y certificación de sistemas de gestión) los requisitos específicos relacionados con ISO 27001:2005 y los SGSI.

5.9.4 ISO/IEC 27005. Esta norma no es certificable. suministra instrucciones para la gestión del riesgo en la seguridad de la información. se apoya en los conceptos generales definidos en la norma iso/iec 27001 y su objetivo es ayudar a la aplicación satisfactoria de la seguridad de la información orientado en la gestión de riesgos.

5.9.5 ISO/IEC 27010. Consiste en una guía para la gestión de la seguridad de la información cuando se comparte entre organizaciones o sectores. ISO/IEC 27010:2012 es aplicable a todas las formas de intercambio y difusión de información sensible, tanto públicas como privadas, a nivel nacional e internacional, dentro de la misma industria o sector de mercado o entre sectores.

5.9.6 ISO/IEC 27011. Es una guía de interpretación de la implementación y gestión de la seguridad de la información en organizaciones del sector de telecomunicaciones basada en ISO/IEC 27002.

5.9.7 ISO/IEC 27013. Es una guía para la implementación integrada de la ISO/IEC 27001:2005 (gestión de seguridad de la información) y de ISO/IEC 20000-1 (gestión de servicios TI).

5.9.8 ISO/IEC 27014. Consiste en una guía de gobierno corporativo de la seguridad de la información.

5.9.9 ISO/IEC TR 27016. Es una guía de valoración de los aspectos financieros de la seguridad de la información.

5.9.10 ISO/IEC 27017. Es una guía de seguridad para Cloud Computing alineada con ISO/IEC 27002 y con controles adicionales específicos de estos entornos de nube.

5.9.11 ISO/IEC 27018. Es un código de buenas prácticas en controles de protección de datos para servicios de computación en cloud computing.

5.9.12 ISO/IEC 27023. En desarrollo, el desarrolla los requisitos de las competencias requeridas para los profesionales dedicados a los sistemas de gestión para la seguridad de la información.

5.9.13 ISO/IEC 27032. Es un estándar de seguridad que se enfoca en la ciberseguridad, y tiene cuatro focos de trabajo como los son:

- Seguridad de la información
- La Seguridad en la Redes
- Seguridad en Internet
- Protección de las Infraestructuras

Este marco basa su metodología en 4 fases de trabajo:

- Entendimiento de la organización
- Análisis de los riesgos
- Definición de un plan de acción
- Implementación del plan de acción propuesto, que suele ser la etapa con mayor compromiso y dedicación por parte de todos los stakeholders involucrados en el proyecto.

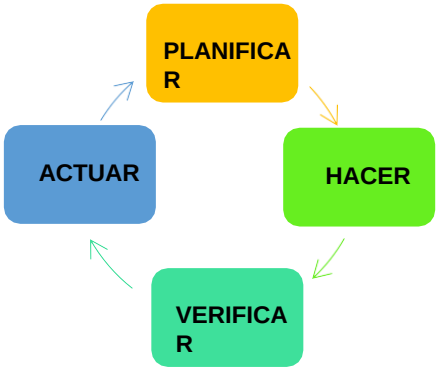
5.9.14 ISO/IEC 27033. El enfoque de esta norma es la seguridad de las redes y está conformada consistente en 6 partes:

- 27033-1, conceptos generales;
- 27033-2, directrices de diseño e implementación de seguridad en redes;
- 27033-3, escenarios de referencia de redes;
- 27033-4, aseguramiento de las comunicaciones entre redes mediante Gateway de seguridad;
- 27033-5, aseguramiento de comunicaciones mediante VPNs;
- 27033-6, seguridad de redes IP Wireless.

5.9.15 ISO/IEC 27037. Es una guía que proporciona directrices para las actividades relacionadas con la identificación, recopilación, consolidación y preservación de evidencias digitales potenciales localizadas en teléfonos móviles, tarjetas de memoria, dispositivos electrónicos personales, sistemas de navegación móvil, cámaras digitales y de video, redes TCP/IP, entre otros dispositivos y para que puedan ser utilizadas con valor probatorio y en el intercambio entre las diferentes jurisdicciones.

5.10 CICLO PDCA: E L CIRCULO DE DEMING DE MEJORA CONTINUA.

Ilustración 22 Ciclo PDCA (Para Proyectos)



Fuente: Elaboración Propia

El SGSI fundamentado en la norma ISO-27001 sigue el enfoque basado en procesos que usan el ciclo de Deming o el ciclo de mejora continua, que consiste en Planificar-Hacer-Verificar-Actuar (PHVA), conocido como PDCA por sus siglas en inglés. (htt6)

Tabla 1 Ciclo Deming (htt7)

PLANIFICAR	Se buscan las actividades susceptibles de mejora y se establecen los objetivos a alcanzar. Para buscar posibles mejoras se pueden realizar grupos de trabajo, escuchar las opiniones de los trabajadores, buscar nuevas tecnologías mejores a las que se están usando ahora, etc.
HACER	Se realizan los cambios para implantar la mejora propuesta. Generalmente conviene hacer una prueba piloto para probar el funcionamiento antes de realizar los cambios a gran escala.
VERIFICAR	Una vez implantada la mejora, se deja un periodo de prueba para verificar su correcto funcionamiento. Si la mejora no cumple las expectativas iniciales habrá que modificarla para ajustarla a los objetivos esperados.
ACTUAR	Una vez finalizado el periodo de prueba se deben estudiar los resultados y compararlos con el funcionamiento de las actividades antes de haber sido implantada la mejora. Si los resultados son satisfactorios se implantará la mejora de forma definitiva, y si no lo son habrá que decidir si realizar cambios para ajustar los resultados o si desecharla. Una vez terminado el paso 4, se debe volver al primer paso periódicamente para estudiar nuevas mejoras a implantar.

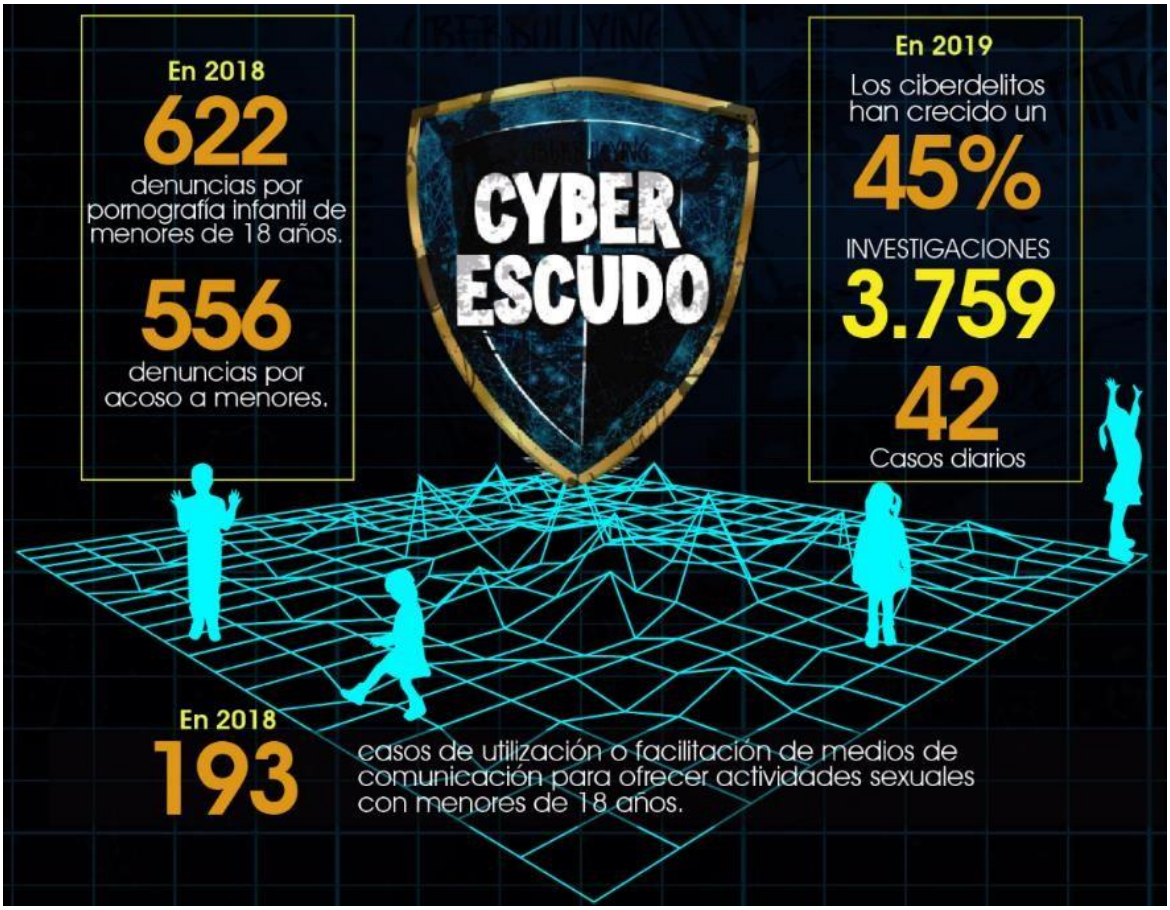
Fuente: https://www.esan.edu.pe/apuntes-empresariales/2016/05/norma-iso-27001-mejora-continua-en-la-gestion-de-seguridad-informacion/

6. MARCO LEGAL

Los delitos informáticos en Colombia han tenido un alarmante crecimiento en el 2019, en comparación con el 2018, según cifras entregadas por la fiscalía general de la nación, de ahí la importancia de contar con leyes que castiguen este tipo de actividades criminales.

En la actualidad en Colombia la ley 1273 de 2009 y la ley 599 de 2000 (Código penal), son las que amparan este tipo de conducta y establecen las penas a pagar por incurrir en ellas.

Ilustración 3 Delitos Informáticos en Colombia en 2019.



Fuente: https://partidomira.com/wp-content/uploads/2019/04/cyberescudo-cifras.jpg

Ilustración 4 . Ley 599 de 2000 (Cod. Penal) y Ley 1273 de 2009 (Art. 269) (htt12)

Artículo	Delito	Pena Meses	Multa
218	Pornografía con personas menores de 18 años	120-240	150-1500
220	Injuria	16-54	13-1500
244	Extorsión	192-288	800-1800
246	Estafa	32-144	66-1500
269A	Acceso abusivo a un sistema informático	48-96	100-1000
269B	Obstaculización ilegítima de sistema informático o red de telecomunicación	48-96	100-1000
269C	Interceptación de datos informáticos	36-72	-
269D	Daño informático	48-96	100-1000
269E	Uso de software malicioso	48-96	100-1000
269F	Violación de datos personales	48-96	100-1000
269G	Suplantación de sitios web para capturar datos personales	48-96	100-1000
269H	Circunstancias de agravación punitiva (de la ½ a las ¾): Servidores públicos, financiera, fines terroristas, entro otras.	Aumento de la ½ a las ¾	-
269I	Hurto por medios informáticos y semejantes	60-120	-
269J	Transferencia no consentida de activos	48-120	200-1500
347	Amenazas	48-96	13-150

Tomado de: https://fyaromo.com.co/2019/04/07/ciberdelitos-en-colombia-corte-a-31-de-marzo-de-2019/

La ley 1273 de 2009 ayudo con definición de penas para los diferentes tipos de delitos informáticos y de protección de seguridad de la información; sancionando con prisión y multas a los infractores.

Esta ley modifico el código penal, tipificando las conductas delictivas asociadas al manejo de la seguridad de la información; la norma esta divida en dos capítulos “De los atentados contra la confidencialidad, la integridad y la disponibilidad de los datos y de los sistemas informáticos” y “De los atentados informáticos y otras infracciones” (Gandini, Isaza, & Delgado, 2019)

7. MARCO ESPACIAL

NOSTRADAMUS S.A.S, es una empresa Ficticia de un caso estudio, creada para el desarrollo de este proyecto, y se cataloga como empresa privada del sector tecnológico fundada en 2019. Que busca ser una alternativa innovadora en la integración de la tecnología en las actividades diarias y procesos de las empresas que adquieren los servicios de esta.

Teniendo en cuenta el caso de estudio, como identidad corporativa se definen la misión y la visión de NOSTRADAMUS S.A.S.

7.1 MISIÓN

Prestar servicios a los sectores educativo, corporativo y gubernamental en temas relacionados con proyectos de educación y capacitación a través del uso de TIC desde la implementación y configuración de plataformas de aprendizaje brindando capacitación y soporte 24/7.

7.2 VISIÓN

Ser una empresa líder en la integración de la tecnología facilitando el desarrollo de los clientes, de manera sostenible y amigable; superando las expectativas proyectadas por nuestros clientes.

8. DISEÑO METODOLÓGICO

La metodología de investigación para este proyecto es mixta, por una parte, está un componente documental relacionado con las normas y estándares internacionales que permitieron medir el riesgo y vulnerabilidades, además de facilitar la definición de las salvaguardas necesarias para garantizar la protección de la seguridad, confidencialidad e integridad de los datos. Se debe dejar claro que al tratarse un caso estudio basado en un caso hipotético fue necesario asumir alguna información en la recolección inicial de los datos, para dejar claro un punto de partida.

Adicionalmente fue necesario investigar sobre los diferentes métodos de ataques que sufrió la empresa, esto permitió realizar una simulación en un ambiente controlado para la recreación de estos y recopilar información para la entrega de las salvaguardas necesarias para protegerse de estos ataques, con la utilización de un UTM basado en software libre con licencia GNU. Esta segunda parte de la investigación es tomada como experimento post-facto; ya que los ataques sufridos por NOSTRADAMUS S.A.S son el medio por el cual muchos hackers roban vulneran la seguridad de las empresas.

La Metodología utilizada comprende:

- Levantamiento de información de la situación actual de la empresa Nostradamus (asociado al SGSI).
- Análisis de la información de la red de Nostradamus.
- Identificación de vulnerabilidades
- Medición del riesgo.
- Planteamiento del SGSI.
- Recreación de ataques en ambiente controlado.
- Generación de informe de los ataques sufridos.
- Propuesta de aseguramiento de la red.

9. ANÁLISIS FORENSE DE LOS ATAQUES SUFRIDOS.

La compañía Nostradamus fue víctima de una serie de ataques cibernéticos que afectando la operación de muchas áreas internas. A raíz de estos ataques, se realiza un reporte gerencial detallado de la consecución de cada ataque sufrido bajo un ambiente controlado, exponiendo los resultados obtenidos.

9.1. DESARROLLO DE LAS SIMULACIONES CONTROLADAS.

Para desarrollar los ataques sufridos por la compañía Nostradamus, se implementa un laboratorio bajo ambiente controlado, en el cual se realizó las simulaciones de estos ataques sobre máquinas virtuales y se estudiaron a fondo las diferentes etapas concluidas por cada ataque. El resultado de estas simulaciones arrojó los datos necesarios para el desarrollo del reporte gerencial y establecer las salvaguardas necesarias para mitigar estas vulnerabilidades.

Las simulaciones para desarrollar son las siguientes:

a) Ataque a sistemas operativos Windows 7 a través de navegadores web haciendo uso de técnicas de ingeniería social con Metasploit
b) Acceso indebido, Ataque de elevación de privilegios y robo de información a sistemas operativos Windows, dejando huella del uso de un exe denominado Lazange
c) Denegación de servicio a la intranet de la empresa, alojada en un servidor con sistema operativo Windows (Se solicita simular a partir s/o Metasploitable)
d) Ataque de Ramsonware (Secuestro de información) utilizando la vulnerabilidad de Eternalblue al sistema operativo Windows que no contaban con el parche de seguridad MS17-010
e) El Sitio web de NOSTRADAMUS S.A.S fue vulnerado posiblemente con un ataque de inyección de SQL. Para para esta simulación se debe determinar 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

9.2. ATAQUE A SISTEMAS OPERATIVOS WINDOWS 7 A TRAVÉS DE NAVEGADORES WEB HACIENDO USO DE TÉCNICAS DE INGENIERÍA SOCIAL CON METASPLOIT

En esta simulación se realizó la clonación de una un correo electrónico para la recopilación de datos a través de la técnica de phishing. Herramientas y aplicaciones:

- Kali Linux;
- Social-Engineer Toolkit (SET)

La herramienta SET es un framework libre utilizado para ingeniería social, permitiendo utilizar varias técnicas en este campo, y es fácil de usar simplemente debemos indicar el vector de ataque que utilizaremos para la recopilación de las credenciales de los usuarios. Además, facilita la clonación del sitio que deseamos suplantar de forma fácil, y creando una copia exacta del mismos en el servidor que definamos se encargara de recibir el tráfico redireccionado.

En el siguiente enlace se encuentra el video de la ejecución del escenario.

https://youtu.be/xGOy6TtWluk

conclusiones del laboratorio:

los ataques de ingeniería social suelen ser la principal puerta de acceso a otros ataques que sufren las empresas diariamente, de ahí la importancia de realizar campañas de concientización a los empleados; pues esto deben tener las habilidades para ayudar a mitigar la efectividad de estos ataques. Adicionalmente a nivel técnico se debe implementar el envío de correo seguro para evitar la interceptación de estos y facilitar la lectura de los miso para robar información asociada a la empresa.

9.3. ACCESO INDEBIDO, ATAQUE DE ELEVACIÓN DE PRIVILEGIOS.

En esta simulación se realizó un ataque de elevación de privilegios sobre una máquina Windows 7 y se utilizaron las siguientes máquinas virtuales, herramientas y aplicaciones:

- Víctima, Máquina Virtual 1: Sistema Operativo Windows 7 SP1.
- Atacante, Máquina Virtual 2: Sistema Operativo Kali Linux versión 2019.1
- Virtualizador: VMWare Workstation 14 Player version 14.1.6 build-12368378.
- Aplicaciones: Metasploit, Zenmap, Lazagne.

El desarrollo de la simulación se basó en la explotación de la vulnerabilidad CVE-2017-0143, que compromete el servicio de Windows SMBv1 (Microsoft Server Message Block 1.0), el cual es utilizado por Windows para el intercambio de paquetes. El impacto que tiene esta vulnerabilidad sobre la maquina es el compromiso total de la integridad, confidencialidad y disponibilidad del sistema, por tal motivo es catalogada como Crítica.

Con la ayuda de la herramienta Metasploit, se logra obtener acceso a la víctima, ejecutando el exploit “EternalBlue SMB Remote Windows Kermel Pool Corruption”, el cual ejecuta código malicioso sobre el servicio SMB, inyectando un archivo DLL. Con esta ejecución se obtiene una sección en Metasploit con permisos de administrador.

Teniendo el acceso a la máquina como usuario administrador, se transfiere desde Metasploit un archivo con el malware LaZagne, la cual se ejecuta remotamente desde la consola para obtener las credenciales de los usuarios actuales de Windows. Adicional se procede a ejecutar los siguientes comandos desde la carpeta de Windows \Windows\System32, para elevar los privilegios de los usuarios actuales o crear nuevos usuarios administradores:

-net user /add Nombre

Dando por finalizada este laboratorio.

En el siguiente enlace se encuentra el video de la ejecución del escenario.

https://www.youtube.com/watch?v=Ld3D_ch0p7g

Conclusiones del Laboratorio:

La mayoría de los ciberataques tienen como finalidad la obtención de datos sensibles. El acceso a una maquina se puede hacer de diferentes maneras, una de ellas es la explotación de vulnerabilidad sobre los Sistemas Operativos, aplicaciones publicadas, conexiones de aplicaciones hacia internet e ingeniería social donde el ataque va dirigido al usuario directamente. Esto hace que nuestros equipos y sistemas de información estén expuestos de manera no controlada.

En este Laboratorio simulamos el ataque aprovechando la vulnerabilidad del Sistema Operativo CVE: 2017-0143, logrando el acceso a la máquina sin necesidad de usuarios administradores. Luego de obtener este acceso se logró, solo con dos comandos, realizar la elevación o creación de un nuevo usuario como administrador, exponiendo aún más la máquina.

9.4. DENEGACIÓN DE SERVICIO.

En este laboratorio se va a simula dos ataques de Denegación de Servicio a un Servidor que contiene una Intranet (Metasploitable). Para este laboratorio se utilizarán los siguientes recursos:

- Víctima, Máquina Virtual 1: Metasplotaible 2.
- Atacante, Máquina Virtual 2: Sistema Operativo Kali Linux versión 2019.1
- Usuario Intranet, Maquina física: sistema Operativo Windows 10.
- Virtualizador: VMWare Workstation 14 Player version 14.1.6 build-12368378.
- Aplicaciones: Metasploit, Zenmap, Lazagne.

Los ataques a desarrollar son los de Inundación SYN (SYN Flood), que consiste en el envío de paquetes de manera masiva con peticiones de conexión tipo SYN al servidor, consumiendo los recursos de red haciendo que la maquina desborde todos los puertos, se ralentice y deje de responder otras peticiones reales. También se realiza ataques de tipo Ping Flood (o ping de la muerte), el cual consiste en el envío masivo de paquetes ICMP de tamaños pesados, con la finalidad de ocupar el ancho de banda de la tarjeta de red del servidor, provocando perdida de paquete de las demás conexiones hacia el servidor. Estos ataques se realizan con ayuda de la aplicación HPING 3 desde una computadora alojada en la misma red.

Con la aplicación HPING 3, es una herramienta para el análisis y tratamiento de paquetes TCP/IP. Con ella se puede enviar paquetes tipo TCP, UDP, ICMP y RAW-IP y modificarlos a discreción para realizar ataques de Denegación de servicios.

En el siguiente video podemos observar el desarrollo de la simulación del ataque DDoS.

https://www.youtube.com/watch?v=wd6cPJ5y6AM&feature=youtu.be

Conclusión del Laboratorio:

La principal herramienta utilizada para desarrollar un ataque de Denegación de Servicio son el envío masivo de paquetes modificados con el objetivo de consumir recursos de la máquina víctima, ya sean de solicitud de conexiones o simplemente consumir el ancho de banda con el desbordamiento de paquetes.

Estos ataques pueden ser perpetuados desde una sola máquina o varias que actúan como Bots recibiendo ordenes de la maquina maestro. Para el caso del ataque a la Intranet de Nostradamus, teniendo en cuenta que el acceso a la plataforma solo se realiza desde la red LAN, este se debió presentar desde una maquina local, en la cual se utilizaron herramientas como HPING3 para su consecución.

Los ataques de DDoS son difíciles de detectar, como logramos observar en la simulación, los paquetes se pueden modificar utilizando diferentes parámetros que engañan a los servicios atacados y firewall, simulando solicitudes normales y reales. Para el caso de Inundación SYN, la IP de la fuente se modificaba aleatoriamente, simulando las peticiones desde diferentes dispositivos.

Estos ataques no explotan ninguna vulnerabilidad y pueden ser mitigados solo con actualizar el sistema, se debe tener un sistema más complejo de herramientas para mitigarlos o eliminarlo.

9.5. ATAQUE RAMSONWARE.

Los ataques de Ramsonware pueden ser perpetuados de diferentes maneras, la más común es con Ingeniería Social, ya sea con el envío de email, link en redes sociales, entre otros. Para la simulación de los ataques Ransomware, se habilitan 3 máquinas virtuales con las siguientes características:

- Víctimas, Máquina Virtual 1: Sistema Operativo: Windows 7 SP1.
- Atacante, Máquina Virtual 2: Sistema Operativo Kali Linux versión 2019.1
- Servidor Web, Máquina Virtual 3: Sistema Operativo Windows 7 con paquete de aplicaciones XAMPP.
- Virtualizador VMWare versión 14.
- Aplicaciones: Metasploit, Zenamp, Virtual Studio, Ransomware Hidden.

Para el desarrollo de este Laboratorio se utiliza el Ransomware “Hidden”, con el cual podemos encriptar con AES carpetas y tipo de archivos específicos en la víctima. Luego de que el malware se ejecuta en la víctima, esté genera una clave para desencriptar, la cual es enviada a un servidor Web donde se almacenará en un archivo de texto local.

Antes de iniciar el ataque, es necesario modificar el Malware con los parámetros que definamos para la ubicación de la carpeta a encriptar, dirección del servidor Web que recibirá la clave, tipos de archivos que queremos encriptar, entre otros. Para ellos utilizamos la herramienta Virtual Studio desde un pc Windows.

Luego de modificados el Malware, se procede a realizar un escaneo de las vulnerabilidades de los equipos que encontremos en la red, en este caso la Máquina Virtual victima con Windows 7.

En el escaneo se detectaron varias vulnerabilidades, y se procede a explotar la CVE-2017-0143, que como se explicó en el laboratorio de Elevación de Privilegios, compromete el servicio de Windows SMBv1 (Microsoft Server Message Block 1.0).

Para obtener acceso a la víctima se ejecuta el Exploit “EternalBlue SMB Remote Windows Kermel Pool Corruption” desde la aplicación Metasploit, instalada en la máquina virtual de Kali Linux. Este exploit contiene un código malicioso para explotar esta vulnerabilidad, obteniendo acceso remoto a la víctima sin necesidad de usuarios administradores.

Ya obtenido el acceso, se procede a transferir el Malware a cualquier carpeta, para esta simulación se instala en la unidad C y se ejecuta desde Metasploit, encriptando los archivos en las carpetas que configuramos en el Malware y enviando la clave para desencriptar la información al servidor Web. Paralelamente generar un archivo de texto, donde le informamos a la víctima que fue atacada y los pasos a seguir para desencriptarlos.

En el siguiente enlace se encuentra el video de la ejecución del escenario.

https://www.youtube.com/watch?v=gLYKswmy6eI&feature=youtu.be

Conclusión del Laboratorio:

Los ataques de Ransomware son los más sonados y dañinos en los últimos 4 años. Y su popularidad se disparó cuando una de las empresas de telecomunicaciones más grandes de mundo fue vulnerada con una Ramsonware llamado WannaCry en el año 2017, afectando gran parte de su operación.

Como observamos en el laboratorio, este ataque se logró perpetuar con la ayuda de una vulnerabilidad del sistema operativo, en la cual se ejecutó el Exploit de Eternalblue y se obtuvo acceso a la máquina, cargando el archivo ejecutable del Ransomware, afectando las carpetas y archivos de escritorio de Windows.

Nuestros sistemas operativos utilizan una gran cantidad de aplicaciones las cuales pueden interactuar con el usuario o pueden correr de manera oculta. Estas aplicaciones pueden generar vulnerabilidad, que en muchos casos son detectadas por los diseñadores mucho tiempo después, corrigiéndolas con actualizaciones constantes. Esto hace que nuestros dispositivos siempre estén expuestos y no lo sabemos.

9.6. INYECCIÓN SQL.

Los ataques de Inyección SQL se pueden ejecutar sobre bases de datos Relacionales (SQL) o No relacionales (No SQL), los cuales atacan vulnerabilidades propias de las bases de datos y debilidades en el acceso a los registros de las mísmas, ya sea por consultas de aplicaciones o ingresos de información por Web

Service. Para el desarrollo de esta simulación se utilizan las siguientes herramientas:

- Víctimas, Máquina Virtual 1: Servidor Web con Base de Datos MySQL y Php.
- Atacante, Máquina Virtual 2: Sistema Operativo Kali Linux versión 2019.1
- Virtualizador VMWare versión 14.
- Aplicaciones: jSQL Inject, MySQL, Apache. (MySQL y Apache están instaladas en el servidor Web.)

La simulación de este escenario se realiza la explotación de una vulnerabilidad sobre los registros y consultas en el servicio Web.

Con la ayuda de la herramienta jSQL Inject se ejecuta un ataque de Inyección SQL sobre los registros de la página Web http://104.236.31.57/Test_SQLInj/, directamente en el link http://104.236.31.57/Test_SQLInj/indez.php?id_registro=217, con la finalidad de obtener acceso a la base de datos, todas sus tablas y registros, y descargar información confidencial.

Con la aplicación jSQL Inject se pueden realizar ataques de inyección SQL a 18 motores de base de datos SQL como Acces, CUBRID, DB2, Derby, Firebird, H2, HSQLDB, Informix, Ingres, MariaDB, MaxDB, MySQL, Oracle, PostgreSQL, SQLite, SQL Server, Sybase, Teradata. Y realiza cuatro tipos de Inyección SQL:

- Normal
- Error
- Blind
- Tiempo

Las diferentes opciones que tenemos disponible son:

- SQL Engine para estudiar y optimizar expresiones SQL.
- Creación y visualización de shell Web y shell SQL.
- Métodos Get, Post, header, cookie.
- Buscar páginas de administración de la base de datos.
- Leer archivos desde el host.
- Bruteforce hash de la contraseña.
- Codificar y decodificar una cadena (encode, decode, base64, hex md5).
- Sistema de traducción de la comunidad: ar, cs, de, es, fr, in_ID, it, nl, pt, ru, tr, zh.
- Multi-thread control (start/pause/resume/stop)
- Opciones de Proxy.

En el siguiente enlace se encuentra el video de la ejecución del escenario.

https://www.youtube.com/watch?v=_bYpRD09HzY&feature=youtu.be

Conclusión del Laboratorio:

Los ataques de tipo Inyección SQL atacan principalmente a los campos de inserción de datos hacia los registros de la base de datos.

En este laboratorio se evidenció una deficiencia en las protecciones a nivel de Base de Datos y a nivel de Servicio Web, ya que no cuenta con nivel de protección suficiente para el ingreso de estos registros. Esto queda expuesto al realizar el ataque de Inyección y obtener el acceso a la base de datos, tablas y registros privados y públicos, dejando expuestos usuarios administradores de las bases de datos, datos privados de los usuarios que acceden a la herramienta, entre otros.

Es necesario realizar una revisión detallada de las políticas de seguridad establecida en los diferentes servicios prestados en el Servidor Web.

10. DESARROLLO DEL SGSI BASADOS EN LAS NORMAS ISO27001 E ISO27032.

Teniendo en cuenta las simulaciones controladas en los laboratorios, y las conclusiones que estos arrojaron, se procede a realizar un diseño de un Sistema de Gestión de Seguridad de la información (SGSI). En el cual se detecten los puntos débiles de los Sistemas de Información, Equipos de Red, Personal, y demás componentes de sus sistemas informáticos.

Este Sistema de Gestión de Seguridad de la Información (SGSI) ayudará a NOSTRADAMUS a eliminar, controlar o mitigar las vulnerabilidades y riesgos que actualmente posee la compañía.

El SGSI, como se especifica en la norma ISO27001, está basado en el ciclo de mejora continua o ciclo de Deming: Planear, Hacer, Verificar y Actuar (PHVA). Para lo cual definimos los pasos para su desarrollo:

Planear:

- Alcance de SGSI.
- Marco general y objetivos del SGSI para NOSTRADAMUS.
- Descripción de la metodología para la evaluación de los riesgos.
- Levantamiento de la información e identificación de activos.
- Identificación de las amenazas para cada activo y determinar los riesgos asociados a estas.
- Análisis y evaluación de los riesgos.

Hacer:

- Plan de tratamiento de Riesgo.
- Controles y gestión de los riesgos y recursos.

Verificar:

- Realizar auditorías internas para confirmar el estado de la implementación del SGSI.
- Medir la implementación de los controles.
- Modificar los planes de tratamientos de riesgos.

Actuar:

- Implementar las mejoras definidas.
- Ejecutar los controles preventivos y correctivos.
- Alinear las mejoras con los objetivos del SGSI.

El diseño del SGSI para la compañía NOSTRADAMUS solo se limitará hasta la fase de Planeación. En la fase de Hacer se analizará y planteará la implementación de un UTM de código abierto teniendo en cuenta las necesidades de la compañía. Y en las fases de verificar y actuar se desarrollan por tratarse de un escenario ficticio.

11. PLANEAR

Teniendo en cuenta la metodología Magerit y las recomendaciones de los puntos 7 y 8 de la norma ISO 27032; en esta etapa se realiza todo el levantamiento de información de los componentes del Sistemas de Información de la compañía, políticas de seguridad implementadas, evaluación de riesgos y demás actividades propias de la planeación, así como la identificación de los interesados al interior de la compañía. Entre las actividades a realiza encontramos las mencionadas a continuación.

11.1. MARCO GENERAL Y OBJETIVOS DEL SGSI PARA NOSTRADAMUS.

En este Marco General, se describe el alcance y objetivos de la implementación del SGSI para la compañía Nostradamus.

11.2. ALCANCE DEL SGSI.

Planeación para la implementación de un SGSI en la sede principal del NOSTRADAMUS SAS, aplicado a las personas, procesos y elementos de red, e instalaciones.

11.3. OBJETIVO DE SGSI

- Mejorar el manejo de la información y mejorar la seguridad por medio del establecimiento de niveles de acceso a la misma.
- Facilitar el cumplimiento de los objetivos misiones y la visión de NOSTRADAMUS SAS.

11.4. DESCRIPCIÓN DE LA METODOLOGÍA PARA LA EVALUACIÓN DE LOS RIESGOS.

Para este proyecto la metodología utilizada para la medición del riesgo de la seguridad de la información se basa en la metodología MAGERIT, la cual permite identificar riesgos y establecer controles a los riegos identificados; esta metodología fue desarrollada por el Consejo Superior de Administración Electrónica de España, quienes facilitaron una guía para el uso de la metodología, permitiendo identificar el impacto que puede ocasionar determinara vulnerabilidad o amenaza que se identifique en el análisis.

Para la identificación de los riesgos es necesario el trabajo en conjunto del equipo interdisciplinario encargado en el alcance del SGSI y las demás áreas de la compañía.

11.4.1 Análisis y evaluación de los riesgos utilizando la Metodología Magerit.

Para robustecer un sistema informático se debe pensar en una protección en capas, para ello debemos tener en consideración todos los elementos físicos y lógicos de la red.

Procediendo con lo anterior debemos realizar las siguientes fases:

- *Fase 1 – Levantamiento de información*
- Conocer el estado de las condiciones actuales de los componentes internos y servicios publicados y accedidos a través de Internet de la compañía NOSTRADAMUS S.A.S.
- Entrevistar personal.
- *Fase 2 – Análisis de información*
- se realizará la identificación de las vulnerabilidades, así como la estimación y valoración del riesgos y posibles amenazas de la red
- definiremos los objetivos generales y específicos, para diseñar un SGSI

- *Fase 3 - Diseño*
- Se realizará el aseguramiento de la red siguiendo normas y/o estándares, que permitan robustecer la postura de seguridad de la red, bajo las normas ISO 27001 y 27032.

Los anteriores pasos mencionados estarán apoyados en parte del manual de la Metodología Abierta de Testeo de Seguridad, pues esta permitirá tener una apropiada visión de las responsabilidades de quien realiza la prueba de seguridad, como los deberes de la compañía; también nos apoyaremos en metodologías como Magerit, para el análisis y la medición del riesgo.

11.4.2 Fase 1 – Levantamiento de información. Esta es la etapa más importante del proyecto en donde se recopila la información necesaria para desarrollo del estudio de amenazas y vulnerabilidades, se reconocen procesos internos, elementos de red, entre otra información que permita conocer plenamente los activos de la compañía.

Para poder realizar una recolección adecuada de datos, se identifican los activos de manera cualitativa y cuantitativa. Adicionalmente se utilizan fuentes primarias (entrevistas) y secundarias (artículos, libros, etc.) con el fin de conocer e identificar las necesidades de la empresa.

Teniendo en cuenta la metodología Magerit, estos activos se clasifican como se muestra en la siguiente tabla:

Tabla 2. Tipos de Activos

[D] DATOS
[K] CLAVES CRIPTOGRAFICAS
[S] SERVICIOS
[SW] SOFTWARE
[HW] EQUIPAMENTO INFORMÁTICO
[COM] REDES DE COMUNICACIONES
[Media] SOPORTE DE INFORMACIÓN
[AUX] EQUIPAMENTO AUXILIAR
[L] INSTALACIONES
[P] PERSONAL

Fuente: Elaboración Propia

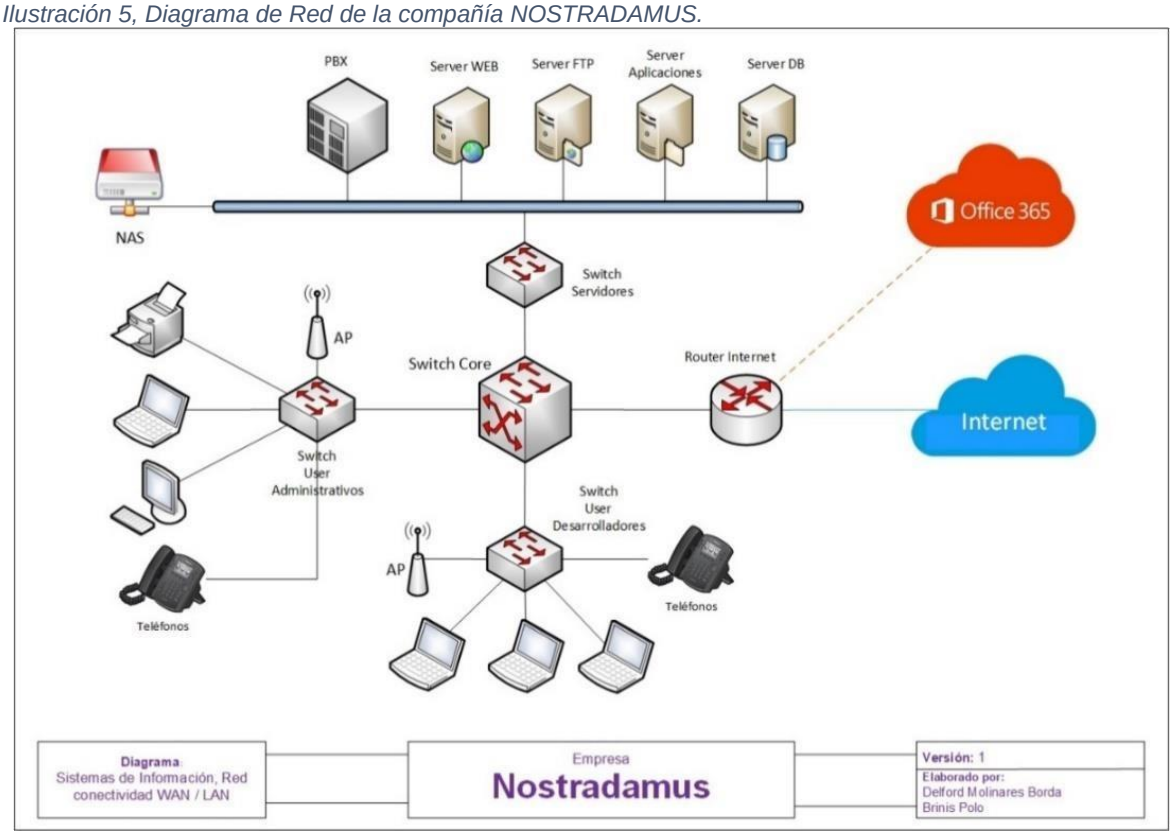
Para el desarrollo del análisis de riesgos de la empresa Nostradamus, se dimensionan los siguientes activos y diagrama de red:

Tabla 3 Activos empresa Nostradamus.

Activo	Cantidad	Observaciones
Servidores	1	Aplicación
	1	Base de Datos
	1	Web
	1	Servidor PBX
	1	FTP
	1	Email - Oficce 365
Portátiles	20	Usuarios
	10	Desarrolladores
	3	Administrativos
Router	1	
Switches Capa 2	3	
Switches Capa 3	1	
Internet	1	BW: 20 Mbps
Access Point	2	
Teléfonos IP	23	
Impresoras	1	
Software	1	
Datacenter	1	
Personal		Administrativo
		IT
		Comercial

Fuente: Elaboración Propia

Ilustración 5, Diagrama de Red de la compañía NOSTRADAMUS.



Fuente: Elaboración Propia

Se clasifican los activos según la metodología Magerit quedando de la siguiente manera:

Tabla 4. Activos clasificados según Magerit

No.	DATOS DEL ACTIVO DE INFORMACION			TIPO								
	Nombre del activo de información	Proceso propietario del activo	Responsable	[D] DAT	[K] CLAVES CRIPTOGRAFIC	[S] SERVICI	[SW] SOFTWA	[HW] EQUIPAMIENTO INFORMATIC	[COM] REDES DE COMUNICACION	[Media] SOPORTE DE INFORMACIC	[AUX] EQUIPAMIENTO AUXILI	[L] INSTALACION	[P] PERSON
1	[pc] Equipos de computos	Departamento de Sistemas	Ingeniero de Soporte					X					
2	[network][switch]Switches	Departamento de Sistemas	Ingeniero Infraestructura					X					
3	[network][router] Router Internet	Departamento de Sistemas	Ingeniero Infraestructura					X					
4	[wap] Aps	Departamento de Sistemas	Ingeniero Infraestructura					X					
5	[ipphone]IP Phone (Cisco 7960)	Departamento de Sistemas	Ingeniero Infraestructura					X					
6	[peripheral][print] Impresoras	Departamento de Sistemas	Ingeniero Infraestructura					X					
7	[int]Server Aplicaciones	Departamento de Sistemas	Ingeniero Desarrollo			X							
8	[pabx] Server PBX	Departamento de Sistemas	Ingeniero Desarrollo					X					
9	[ftp]Server FTP	Departamento de Sistemas	Ingeniero Desarrollo			X							
10	[dbms] Sistema de gestión de Bases de Datos	Departamento de Sistemas	Ingeniero Desarrollo				X						
11	[www] Servidor Web	Departamento de Sistemas	Ingeniero Desarrollo				X						
12	[email_server] Servidor de Correo.	Departamento de Sistemas	Ingeniero Infraestructura				X						
13	[internet] Punto de Acceso a Internet	Departamento de Sistemas	Ingeniero Infraestructura						X				
14	[des] Personal TI	Departamento de Sistemas	Area TI										X

Fuente: Elaboración Propia

Como se observa en la tabla anterior, la mayoría de los elementos o activos se clasifican como Equipamiento, pero no quiere decir que son los más críticos o importantes. Para determinar esto, se debe realizar el análisis de la información y calificación de los riesgos asociados, teniendo en cuenta varios factores.

11.4.3 Fase 2 - Análisis de la Información. Después de realizar el inventario de activos y conocer vulnerabilidades procedimentales, es hora de cuantificar el riesgo, en esta parte se hará huso de la metodología Magerit, el cual nos permite cruzar la probabilidad vs el impacto de un riesgo identificado.

Tabla 5. Tabla de valores de probabilidad e Impacto

PROBABILIDAD	DEFINICION
1	Raro
2	Improbable
3	Posible
4	Probable
5	Esperado

IMPACTO	DEFINICION
1	Insignificante
2	Menor
3	Moderado
4	Mayor
5	Catastrófico

Fuente: Elaboración Propia

Una vez los riesgos son medidos y evaluados se deben proponer salvaguardas para mitigar, controlar o transferir el mismo; luego de los cual se volverá a medir el riesgo, para sacar un mapa de riesgos residual.

11.4.4 Valoración Cualitativa. Teniendo en cuenta los activos de la compañía, se realiza un análisis cualitativo de cada uno de ellos, teniendo en cuenta las dimensiones de Autenticidad, Trazabilidad, Confidencialidad, Integridad y Disponibilidad. Se procede a calificarlos como se muestra en la siguiente tabla:

Tabla 6. Valoración cuantitativa de los Activos de la Información de Nostradamus.

No.	DATOS DEL ACTIVO DE INFORMACION	DIMENSION				
	Nombre del activo de información	Dimensión Autenticidad(B / M /A / MA/ MB)	Dimensión Trazabilidad (B / M /A / MA/ MB)	Dimensión Confidencilidad (B / M/A / MA/ MB)	Dimensión Integridad (B / M	Dimensión Disponibilidad (B /
1	[pc] Equipos de computos	A	M	M	B	M
2	[network][switch]Switches	A	M	A	A	MA
3	[network][router] Router Internet	A	M	A	A	MA
4	[wap] Aps	A	M	A	M	M
5	[ipphone]IP Phone (Cisco 7960)	M	B	A	B	M
6	[peripheral][print] Impresoras	B	B	B	B	M
7	[int]Server Aplicaciones	MA	A	A	MA	A
8	[pabx] Server PBX	A	A	M	A	A
9	[ftp]Server FTP	MA	MA	MA	M	A
10	[dbms] Sistema de gestión de Bases de Datos	MA	MA	MA	MA	MA
11	[www] Servidor Web	MA	MA	MA	MA	MA
12	[email_server] Servidor de Correo.	MA	A	A	A	A
13	[internet] Punto de Acceso a Internet	A	A	B	A	MA
14	[des] Personal TI	A	M	A	A	A

Fuente: Elaboración Propia

También se realiza valoración cualitativa teniendo en cuentas ciertos atributos.

Tabla 7. Valoración Cualitativa de los activos de Información

No.	DATOS DEL ACTIVO DE INFORMACION	ATRIBUTOS								
	Nombre del activo de información	¿Es activo de información de terceros o de clientes que debe protegerse?	¿Activo de información que debe ser restringido a un número limitado de empleados?	Activo de información que debe ser restringido a personas externas	Activo de información que puede ser alterado o comprometido para fraudes ó corrupción	Activo de información que es muy crítico para las	Activo de información que es muy crítico para el	Activo de información que		
								Leve	Importante	Grave
1	[pc] Equipos de computos	NO	SI	SI	SI	NO	NO	X		
2	[network][switch]Switches	NO	SI	SI	NO	SI	NO			X
3	[network][router] Router Internet	SI	SI	SI	NO	SI	NO			X
4	[wap] Aps	NO	SI	SI	NO	NO	NO	X		
5	[ipphone]IP Phone (Cisco 7960)	NO	SI	NO	SI	NO	NO	X		
6	[peripheral][print] Impresoras	NO	NO	SI	NO	NO	NO	X		
7	[int]Server Aplicaciones	NO	SI	SI	SI	SI	NO		X	
8	[pabx] Server PBX	NO	SI	SI	SI	SI	NO			X
9	[ftp]Server FTP	SI	SI	SI	SI	SI	SI			X
10	[dbms] Sistema de gestión de Bases de Datos	SI	SI	SI	SI	SI	SI			X
11	[www] Servidor Web	SI	SI	SI	SI	SI	SI			X
12	[email_server] Servidor de Correo.	SI	SI	SI	SI	SI	SI		X	
13	[internet] Punto de Acceso a Internet	SI	SI	SI	SI	SI	SI		X	
14	[des] Personal TI	NO	SI	SI	SI	SI	SI		X	

Fuente: Elaboración Propia

11.4.5 Valoración Cuantitativa. Para identificar los activos críticos de la compañía, se realiza una valoración cuantitativa teniendo en cuenta las dimensiones en la valoración cualitativa, asignándole valor teniendo en cuenta la siguiente tabla:

Tabla 8, Valoración Cuantitativa según valor cualitativo.

VALORACIÓN DEL RIESGO			
	Nomenclatura	Categoría	Valoración
Valoracion del riesgo	MA	Critico	21 a 25
	A	Importante	16 a 20
	M	Apreciable	10 a 15
	B	Bajo	5 a 9
	MB	Despreciable	1 a 4

Fuente: Elaboración Propia

Esta valoración la podemos observar en la siguiente tabla, en la cual identificamos los activos críticos, a los cuales se le realizará un plan de tratamiento de las amenazas.

Tabla 9, Valoración cuantitativa del riesgo Nostradamus

Fuente: Elaboración Propia

11.4.6 Riesgos de los activos Críticos. Teniendo en cuenta la valoración cuantitativa, se puede determinar que los activos más críticos son:

- Servidor de Aplicaciones.
- Servidor FTP.
- Servidor de Base de Datos.
- Servidor Web.
- Servidor de Correo.

Sobre estos activos se realiza un plan de tratamientos basados en los riesgos tipificados en la norma ISO27002.

Los riesgos a los cuales están expuestos estos activos críticos son los siguientes:

Ilustración 6. Riesgos Servidor de Aplicaciones

No. De Amen	Nombre del activo de información	VALORACIÓN DEL RIESGO DE LOS ACTIVOS	Amenazas Metodología Magerit	Vulnerabilidades	RIESGOS	Probabilidad de vulneración	Calculo del riesgo neto (Valoración del riesgo * probabilidad	Criticidad neta (1 a 4 despreciable (d) 5 a 9
82	[int]Server Aplicaciones	22	[N1] Fuego	Sin sistemas de contra Incendio, corto circuito.	Daños de equipos, perdida de información	1	22	C
83	[int]Server Aplicaciones	22	[I5] Avería de origen físico o lógico	Daño en componentes, caídas, golpes.	Daños de equipos, perdida de información	1	22	C
84	[int]Server Aplicaciones	22	[I6] Corte del suministro eléctrico	Falta de contingencia en sistema eléctrico	Pérdidas económicas por indisponibilidad de los servicios.	3	66	C
85	[int]Server Aplicaciones	22	[E1] Errores de los usuarios	Falta de actualizaciones y controles de cambios de los usuarios.	Integridad de los datos, fallo en equipos, perdida de información	3	66	C
86	[int]Server Aplicaciones	22	[E2] Errores del administrador	Falla humana o Falta de capacitación al personal administrador de la plataforma	Pérdidas economicas por fallos en la configuración y acceso a la información	2	44	C
87	[int]Server Aplicaciones	22	[E15] Alteración accidental de la información	Falla humana	Integridad de los datos, pérdida de información	3	66	C
88	[int]Server Aplicaciones	22	[E24] Caída del sistema por agotamiento de recursos	Actualización de plataforma y servidores que soporta en servicio	Fallo de equipos, perdida de información	1	22	C
89	[int]Server Aplicaciones	22	[A6] Abuso de privilegios de acceso	Responsabilidad del personal administrador del servicio	Perdida de información, alteración de información afectando la integridad de los datos	1	22	C
90	[int]Server Aplicaciones	22	[A15] Modificación deliberada de la información	Falta de parches y/o políticas de seguridad	Integridad de la información comprometida por acceso no autorizado	2	44	C
91	[int]Server Aplicaciones	22	[A18] Destrucción de información	Falta de controles de log y no implementación de backup	Perdida de información sensible para la operación de la empresa	2	44	C

Fuente: Elaboración Propia

Ilustración 7. Riesgos Servidor FTP

Fuente: Elaboración Propia

Ilustración 8. Riesgos Servidor de Base de Datos

No. De Amen	Nombre del activo de información	VALORACIÓN DEL RIESGO DE	Amenazas Metodología Magerit	Vulnerabilidades	RIESGOS	Probabilidad de vulneración	Calculo del riesgo neto (Valoración del riesgo * probabilidad	Criticidad neta (1 a 4 despreciable (D), 5 a 9 baja
22	[dbms] Sistema de gestión de Bases de Datos	25	[N1] Fuego	Sin sistemas de contra Incendio, corto circuito.	Daños de equipos, perdida de información	1	25	C
23	[dbms] Sistema de gestión de Bases de Datos	25	[N2] Daños por agua	Inundación, tubería rota.	Daños de equipos, perdida de información	1	25	C
24	[dbms] Sistema de gestión de Bases de Datos	25	[I5] Avería de origen físico o lógico	Daño en componentes, caídas, golpes.	Daños de equipos, perdida de información	1	25	C
25	[dbms] Sistema de gestión de Bases de Datos	25	[I6] Corte del suministro eléctrico	Falta de contingencia en sistema eléctrico	Fallas en la integridad de los datos, daños en equipos.	3	75	C
26	[dbms] Sistema de gestión de Bases de Datos	25	[I7] Condiciones inadecuadas de temperatura o humedad	Falla en sistema de aire acondicionado, falta de medidores de temperatura y humedad.	Fallo en equipos, perdida de información, por deterioro acelerado de los componentes	2	50	C
27	[dbms] Sistema de gestión de Bases de Datos	25	[E23] Errores de mantenimiento / actualización de equipos (hardware)	Fallo en hardware o Software	Retrasos en la operación ante la imposibilidad de acceso a la información	1	25	C
28	[dbms] Sistema de gestión de Bases de Datos	25	[E24] Caída del sistema por agotamiento de recursos	Falta de actualización de hardware de los equipos o cambio por obsolescencia.	Fallo de equipos, perdida de información	1	25	C
29	[dbms] Sistema de gestión de Bases de Datos	25	[A11] Acceso no autorizado	Falta de control acceso a personal a zonas no autorizadas y filtrado de credenciales de acceso. Falta de actualizaciones firmware	Perdida de equipos, perdida de información, divulgación de información, alteración de información	2	50	C
30	[dbms] Sistema de gestión de Bases de Datos	25	[A7] Uso no previsto	Falta de control acceso a personal a zonas no autorizadas. Fallos de seguridad y en configuración	Perdida de equipos, perdida de información, divulgación de información, alteración de información	1	25	C

Fuente: Elaboración Propia

Ilustración 9. Riesgos Servidor Web

Fuente: Elaboración Propia

Ilustración 10. Riesgos Servidor de Correo

Fuente: Elaboración Propia

12. HACER

Debido a los ataques sufridos por Nostradamus, los cuales son Ataques de denegación de servicios, inyección SQL, ingeniería social, entre otros, y el resultado de los deferentes riesgos analizados que afectan la confidencialidad, seguridad e integridad de la información propia de la empresa, se propone la implementación de una solución modular que permita protegerse de los ataques ya mencionados (para este caso un UTM - Unified Threat Management); el cual junto con la aplicación de las mejores prácticas en la implementación del equipo, una correcta planeación, despliegue y afinamiento del funcionamiento y políticas que se establezcan en el equipo, ofrecerá a la empresa y a los usuarios una mayor tranquilidad en la seguridad de los datos.

Algunas de las ventajas de la implementación de este tipo de soluciones es la presentación de un panel de control intuitivo, así como la configuración de umbrales para la generación de alarmas e incidentes de red.

A nivel de la capa de red será necesarios realizar la segmentación del tráfico de red LAN, es decir la creación de VLAN´s separar el tráfico de los usuarios cableados, de los usuarios inalámbricos, al igual que el tráfico de voz, entre otros servicios que funcionen en la red.

En cuanto a los servidores con servicios publicados, se recomienda la estandarización de la configuración de estos a nivel de seguridad (realizar Hardering); mantener las actualizaciones periódicas, generar registros de Log´s y por último instalar antivirus y antisoftware malware y realizar evaluaciones periódicas de vulnerabilidades.

En cuento al personal se deberán establecer reglas básicas para el comportamiento personal, tanto como individuo, como en forma de empleado[2]; durante el uso de los elementos de networking que dispone la empresa para la realización de sus funciones.

12.1 FASE 3 - PROPUESTA DE ASEGURAMIENTO

Para mejorar la seguridad de la red de NOSTRADAMUS SAS, se recomienda la utilización de un Unified Threat Management – UTM; Esta es una solución integral de seguridad que permite tener centralizada la protección del perímetro de la red, realizando tareas de monitoreo, antivirus, networking, antispyware, Routing, antispam, firewall de red, prevención y detección de intrusiones, QoS, filtrado de contenido, Web aplication firewall, etc. El UTM se complementa también con servicios end point como HIPS, y los antivirus para robustecer sus funcionalidades.

Esta labor se hace generalmente comparando el comportamiento de la red con una base de datos en la que se concentran firmas de diferentes ataques, contra los cuales se cruzaran los paquetes de red, para detectar comportamiento anómalo. Adicionalmente puede complementarse con bases de datos online, mejorando la identificación de amenazas.

Teniendo claro el alcance de un UTM, se recomienda implementar un UTM de código abierto en NOSTRADAMUS SAS, que preste una gran variedad de servicios que brinden una protección unificada de amenazas, que posea una interfaz gráfica de facilite uso, y que brinde una visibilidad del estado de la red e informes detallados por periodos de tiempo.

Teniendo en cuenta las recomendaciones de las normas 27001 y 27032; es importante que posterior a la instalación y configuración del UTM para la seguridad perimetral de la empresa; NOSTRADAMUS debe realizar periódicamente un análisis de vulnerabilidades con el fin de detectar brechas de seguridad en su red, sistemas de información y servicios publicados para el acceso o consulta desde internet; y con base en los resultados obtenidos, reforzar las políticas de seguridad configuradas en el UTM.

[2] Tomado de la norma ISO 27032:2015, punto 12.5.1 visión general

12.2 ANÁLISIS DE LAS DIFERENTES PROPUESTAS DEL MERCADO PARA UTM.

En el mercado existen muchas propuestas de seguridad, algunos que son apoyados bajo por grandes firmas (como Cisco, Fortinet, Palo Alto, Sonicwall; por nombrar algunas), otras que son open source y que cuentan con una comunidad de desarrollo bastante amplia. Es de aclarar que la propuesta de seguridad está basada en una solución con funciones de Next Generation Firewall – NGFW; o Unified Threat Management – UTM, el nombre variara según el vendor.

Por otra parte, está el hecho de que algunos proveedores y marcas vienen con hardware propietario, y otros son solo el software; sin que una u otra opción deje de ser menos segura que la anterior.

A continuación, mencionaremos algunas de las funcionalidades que pueden desempeñar este tipo de soluciones

- Filtrado de tráfico TCP y UDP""
- Enrutamiento por políticas
- Web Aplication Firewall
- Network Address Translation (NAT)
- Configuración en Alta disponibilidad
- Multi WAN
- IDS / IPS
- Balanceo de carga
- VPN
- Monitoreo gráfico y por logs
- DNS dinámico
- Virtual Private Network (VPN)
- Portal cautivo
- Crecimiento Modular
- Servidor DHCP y DHCP Relay.

12.2.1 Modos de configuración de un UTM. Básicamente estos equipos pueden tener dos modos de configuración:

- **Modo Proxy.** En este modo el equipo hace de puerta de enlace para la comunicación interna, además será el intermediario para los equipos que deseen salir a internet.

- **Modo Transparente.** En este escenario el equipo únicamente analiza en tiempo real los paquetes los paquetes de la red. Esta configuración requiere que el equipo sobre el cual este instalado deba contar con altas prestaciones de hardware. Para ello es necesario configurar el puerto del SW donde se vaya a conectar en modo escucha.

12.2.2 Software UTM. Para dar soluciones a los problemas presentados en la empresa Nostradamus hemos optado por la opción de UTM basado en software (aunque en el caso de Pfsense, también cuentan con su propio hardware), para lo cual indicaremos las características, funcionalidades y pasos para la instalación de dos de los nombres de soluciones de seguridad de software más nombrados a la hora de hablar de soluciones Open source mode seguridad, además de estar entre las primeras opciones en este campo, y muy utilizadas en empresas SoHo (Small Office-Home Office).

12.2.3 PfSense. Es un sistema basada en FreeBSD, fue diseñado para poder montar un firewall de manera fácil en PC's y Servidores; por medio una interface web bastante intuitiva. Permite integrarse con una variedad de Add-Ons que aumentar las funcionalidades ayudando robustecer la seguridad del sistema.

Características principales

- Firewall
- tabla de estado
- NAT
- PAT
- Redundancia
- Balance de Carga
- Inbound Load Balancing
- VPN
- IPsec
- PPTP Server
- PPPoE Server
- Reportes de estado
- Monitoreo en tiempo real
- DNS
- Portal Cautivo
- Servidor DHCP y Relay DHCP

12.2.4 OPNSense. Esta es una plataforma de enrutamiento y firewall, que también se basa en FreeBSD, además incluye la mayoría de las funcionalidades de firewalls comerciales, e inclusive muchos casos. Ofrece actualizaciones semanales de seguridad de manera que la base de datos pueda mantenerse actualizada ante las nuevas amenazas emergentes.

Características:

- Firewall
- Traffic Shaper
- Portal cautivo
- Forward Caching Proxy
- VPN
- Posibilidad de Configuración en HA y Failover de hardware
- IDS
- Herramientas para generación de informes y monitoreo
- Exportador de Netflow
- Monitoreo del tráfico de red
- Servidor DNS y DNS Dinámico
- Servidor DHCP y DHCP Delay
- Opción para guardar copia de la configuración de manera encriptada en Google Drive
- Cortafuegos Stateful
- Compatible con VLAN 802.1Q

Después de la versión 2.4 es necesario que los procesadores de las maquinas en las cuales se instala cuenten con AES-NI (Advanced Encryption Standard New Instructions) ya que permite cifrar y descifrar datos a una grandísima velocidad.

12.2.5 Comparativa entre OPNsense® vs pfSense®

A continuación, se puede ver un cuadro comparativo de ambas soluciones

Tabla 10 Comparativa OPNsense vs pfSense

Características	OPNsense®	pfSense®
Cortafuegos	stateful	stateful
Interfaz gráfica basada en web	Bootstrap basado en Phalcon PHP Framework	* Desde 2.3 migrado a Bootstrap

Asistente de configuración de instalación	Si	si
Tablero configurable	Si	si
Soporte de IPv4 e IPv6	Si	si
Punto de acceso inalámbrico	Si	si
Soporte de cliente inalámbrico	Si	si
Configurar y filtrar / aislar múltiples	-	si
Interfaces (LAN] DMZ] etc.)	Si	si
Modelado de tráfico	Si	si
Controles de tabla de estado	Si	si
NAT	Si	si
Redundancia / Alta Disponibilidad	Si	si
Soporte Multi-WAN	Si	si
Equilibrio de carga entrante del servidor	Sí (configuración del servidor virtual)	si
Utilidades de diagnóstico de red	Vea abajo	Vea abajo
[silbido]	Si	si
[traceroute]	Si	si
[pruebas de puerto a través de la GUI]	Si	más con paquetes] como nmap
VPN		
[IPsec (incluida la fase 2 NAT)]	Si	si
[OpenVPN]	Si	si
[L2TP]	Sí (complemento tramite)	Sí (a través del paquete)
[PPPoE]	Sí (complemento tramite)	Sí (a través del paquete)
[PPTP]	Sí (no considerada suricura)	No (tomado porque no estoy seguro)
RRD Graphs	No (estado del sistema)	Si

Gráficos de tráfico de interfaz en tiempo real	Si	Si
DNS Dinámico	Si	Si
Portal cautivo	Si	Si
Servidor DHCP y retransmisión (IPv4 e IPv6)	Si	Si
Línea de comando shell acceso	Si	Si
Activación de la LAN	Si	Si
Construido en captura de paquetes / sniffer	Si	Si
Copia de seguridad y restaurar la configuración de fw	Si	Si
Editar archivos a través de la GUI web	Si	Si
Interfaces virtuales para:		
[VLAN]	Si	Si
[LAGG / LACP]	Si / No	Sí / Sí
[GIF]	Si	Si
[GRE]	Si	Si
[PPPoE / PPTP / L2TP / PPP WANs]	Si / si / si / si	Si / si / si / si
[QinQ] y puentes]	Si	Si
Reenvío / resolución de DNS de almacenamiento en caché	Si	Si
Se puede ejecutar en muchos entornos de virtualización.	Si	Si
Servidor proxy	Si	usando paquetes
IPS	Sí (basado en Suricata)	SNORT (PAQUETE EXTRA)
IDS	Sí (basado en Suricata)	SNORT (PAQUETE EXTRA)
Actualización de seguridad	Si semanal	Sí, con lanzamiento de parche

Software de incursión	Sí no oficialmente compatible *	Sí totalmente compatible

Fuente: tomada y traducida de https://www.firewallhardware.it/en/pfsense-vs-opnsense-technical-comparison/

Luego de realizar el análisis de la tabla comparativa. Se recomendación utilizar OPNSense, la cual es una plataforma de enrutamiento y firewall de código abierto basado en BSD, esta plataforma tiene sus inicios en 2014 y su primer lanzamiento oficial fue en 2015. Ofrece dentro de sus muchas características la autenticación de dos factores lo que le da mayor seguridad al manejo de dashboard de la herramienta; la cual además es más intuitiva que la de PfSense; por ultimo y no menos importante el poder recibir actualizaciones de seguridad semanales; nos inclina a tomar esta herramienta como la mejor opción para las necesidades de seguridad que presenta la empresa Nostratamus.

OPNSense cuenta con el respaldo de Deciso B.V. la cual es una compañía con una vasta experiencia en soluciones de seguridad de código abierto. Adicionalmente la interfaz gráfica es mucho más intuitiva que la de PfSense.

12.2.6 Implementación del UTM OPNSense en ambiente controlado.

Con la finalidad de conocer las características del UTM de código abierto seleccionado, cómo ayudaría en la protección perimetral de la red de Nostradamus, y como se integraría en su red de datos, se realizó la instalación del UTM sobre una máquina virtual en un ambiente controlado y se realizaron pruebas de funcionamiento en algunos de los escenarios estudiados sobre los ataques recibidos por NOSTRADAMUS.

12.2.7 Instalación OPNSense.

A continuación, explicaremos cómo se instala la aplicación OPNSense sobre una máquina virtual ejecutada en VMWare.

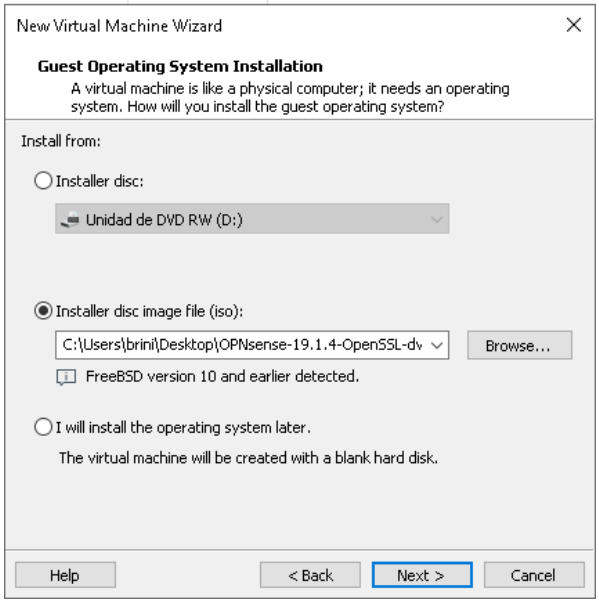
El primer paso es abrir VMWare y seleccionamos en File New Virtual Machine, la opción de forma Típica y le damos en next:

Ilustración 11 Instalación OPNSense Paso 1

Fuente: Elaboración Propia

Seleccionamos la opción “Installer disc image file” e ingresamos la ubicación del archivo de OPNsense en los medios de almacenamiento del equipo:

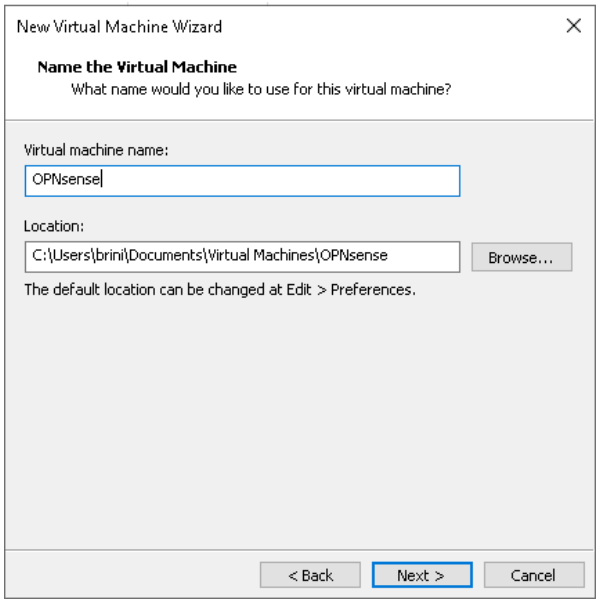
Ilustración 12 Instalación OPNSense Paso 2



Fuente: Elaboración Propia

Le asignamos un nombre a nuestra máquina virtual y la ubicación en la cual la vamos a guardar:

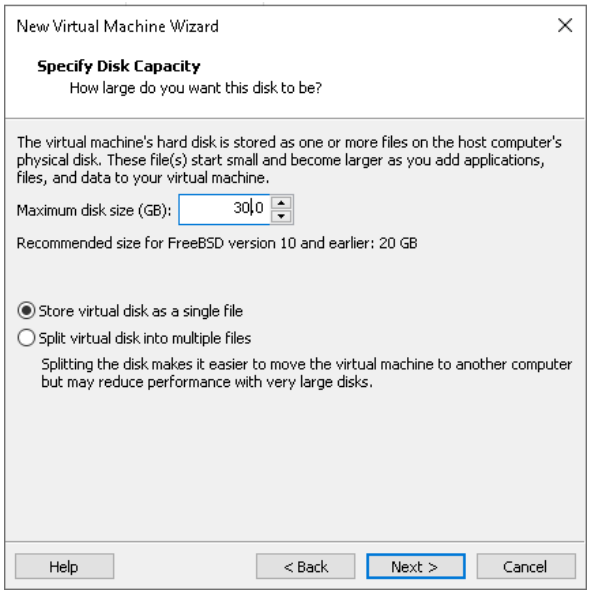
Ilustración 13 Instalación OPNSense Paso 3



Fuente: Elaboración Propia

Seleccionamos la capacidad de nuestro disco duro y marcamos la opción Store virtual disk as a single file:

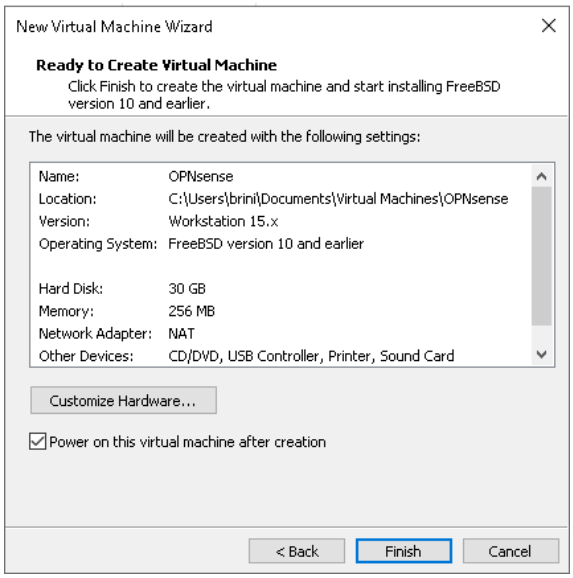
Ilustración 14 Instalación OPNSense Paso 4



Fuente: Elaboración Propia

En esta ventana seleccionamos Customize Hardware para asignar los atributos de la VM:

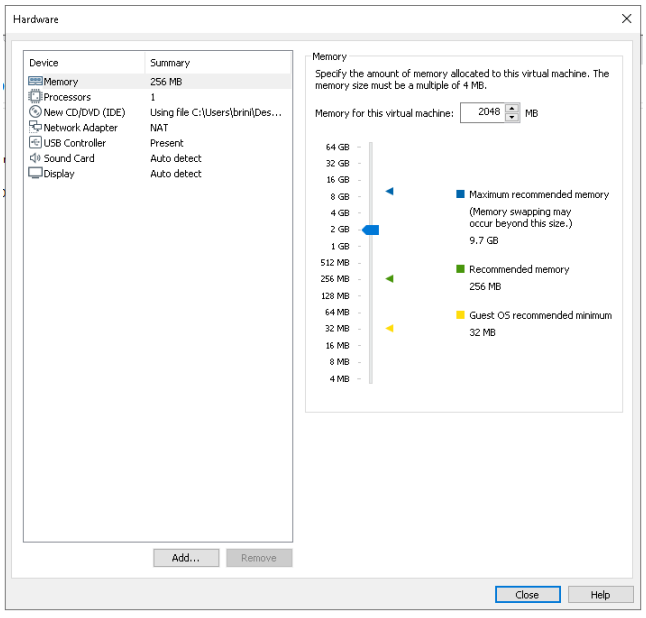
Ilustración 15 Instalación OPNSense Paso 5



Fuente: Elaboración Propia

En la opción Memory seleccionamos 2 GB de memoria:

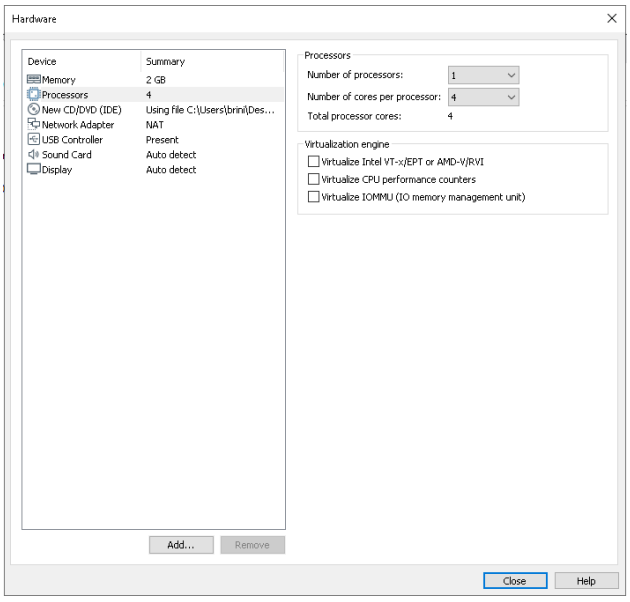
Ilustración 16 Instalación OPNSense Paso 6



Fuente: Elaboración Propia

En la opción de Processors, seleccionamos Number of cores per processors La cantidad de 4:

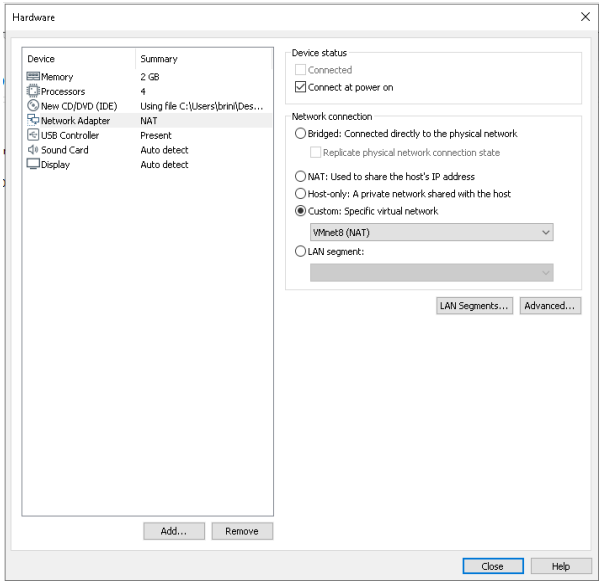
Ilustración 17 Instalación OPNSense Paso 7



Fuente: Elaboración Propia

En la opción Network Adapter, marcamos la opción Custom, y VMnet8:

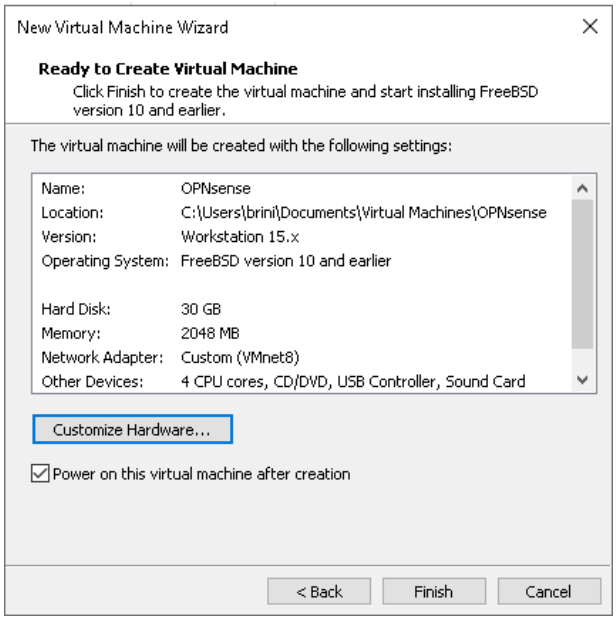
Ilustración 18 Instalación OPNSense Paso 8



Fuente: Elaboración Propia

Ahora finalizamos la creación de la VM en el botón “Finish” y nuestra máquina virtual arrancará:

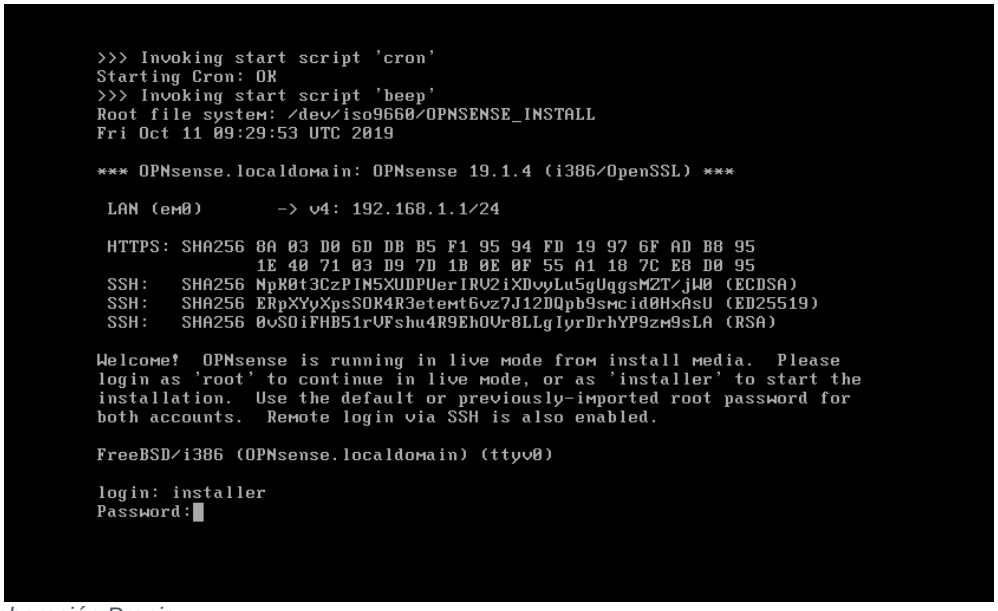
Ilustración 19 Instalación OPNSense Paso 9



Fuente: Elaboración Propia

Después de arrancar y esperar nos pedirá un login y password, los cuales por defecto son: installer y opnsense, respectivamente.

Ilustración 20 Instalación OPNSense Paso 10



Fuente: Elaboración Propia

Luego nos saldrá la siguiente ventana y seleccionamos Ok, let's go para continuar:

Ilustración 21 Instalación OPNSense Paso 11

Fuente: Elaboración Propia

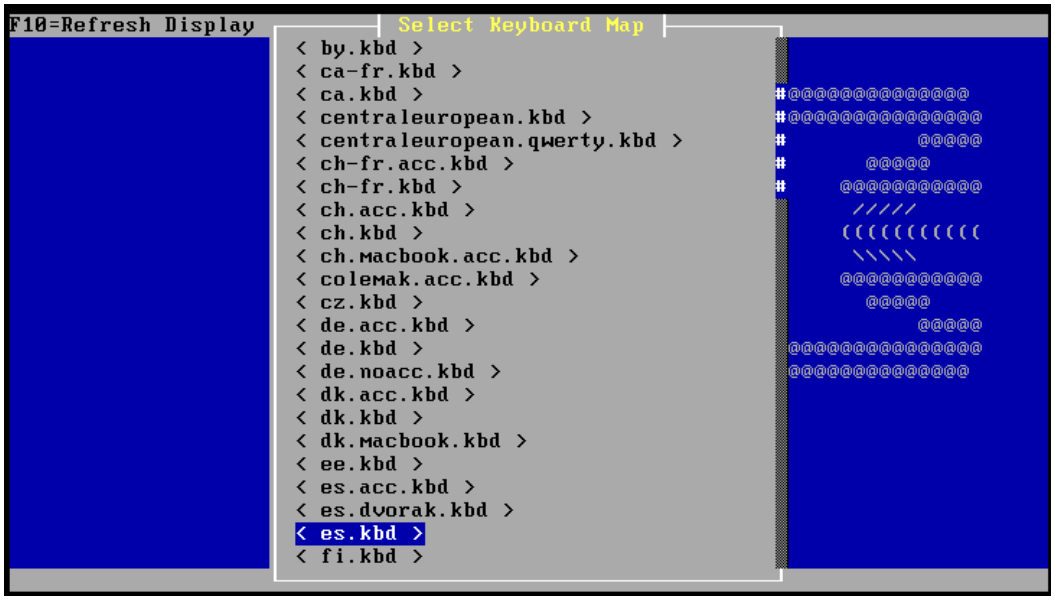
Le damos en change keymap (teclado) y elegimos nuestra distribución de teclado:

Ilustración 22 Instalación OPNSense Paso 12

Fuente: Elaboración Propia

En mi caso serie en español que seria es. Kdb:

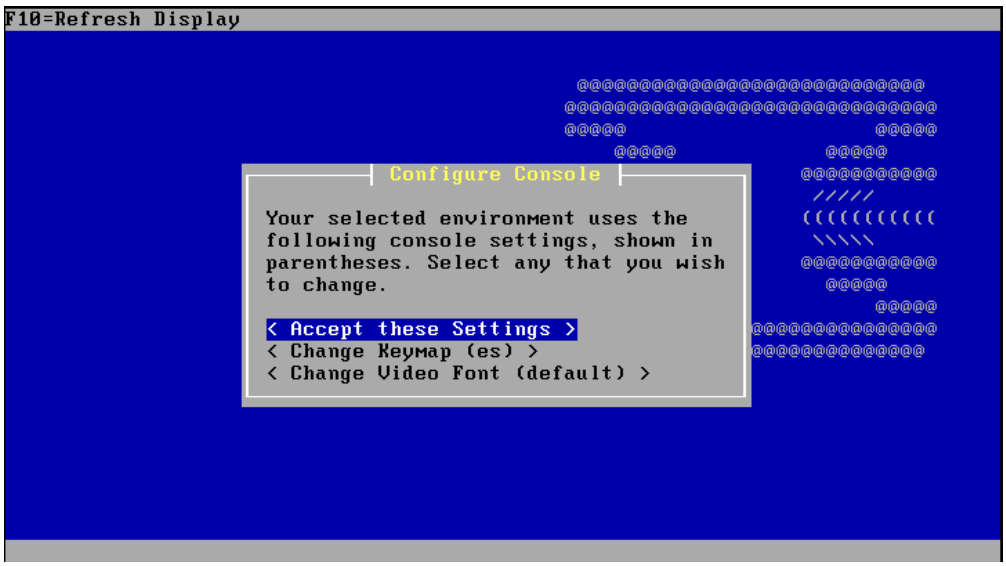
Ilustración 23 Instalación OPNSense Paso 13



Fuente: Elaboración Propia

Luego procedemos a aceptar las configuraciones en la opción “Accep these settings” para agregar los cambios:

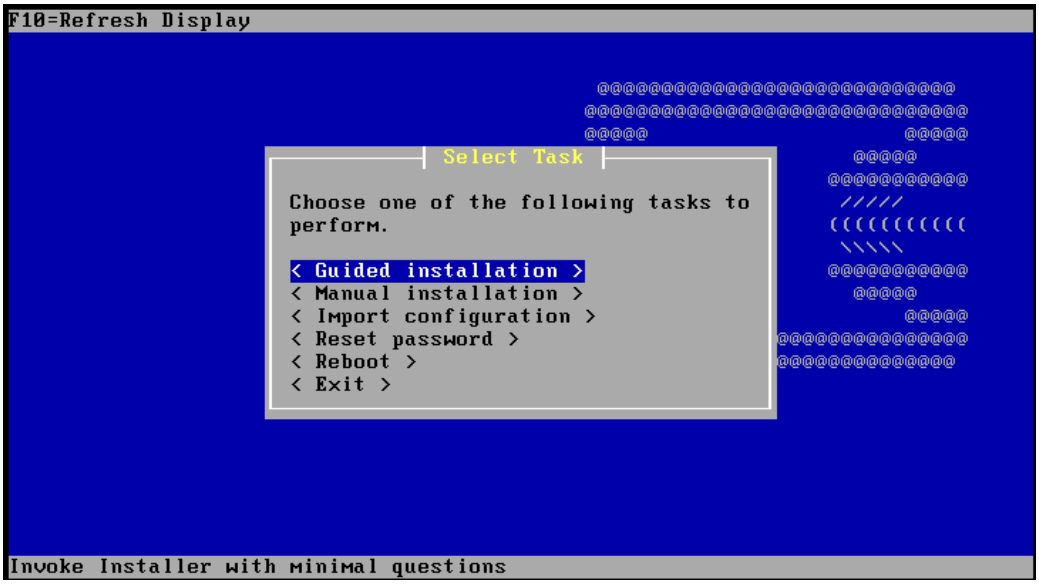
Ilustración 24 Instalación OPNSense Paso 14



Fuente: Elaboración Propia

En esta pantalla le damos en Guided installation para continuar con la instalación guiada:

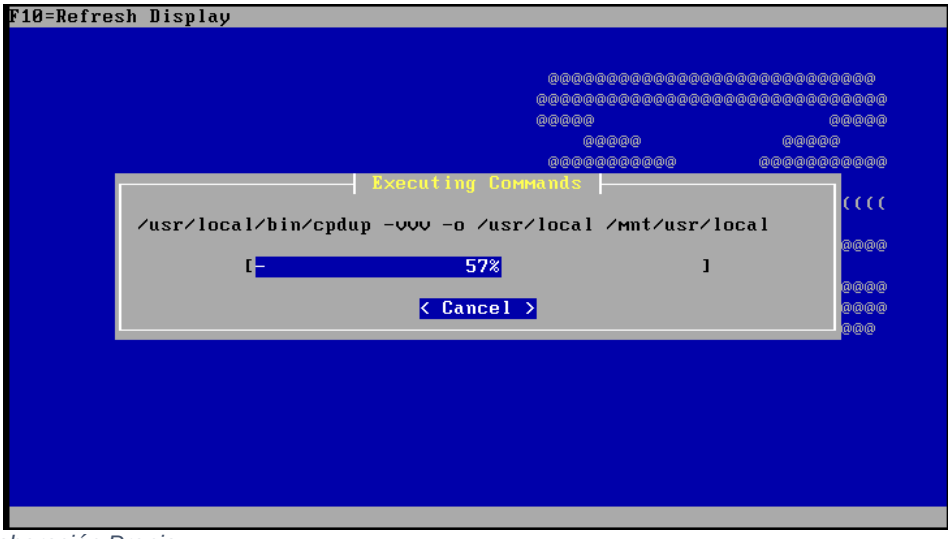
Ilustración 25 Instalación OPNSense Paso 15



Fuente: Elaboración Propia

Ahora nos mostrara los discos que detecta el sistema y procedemos a darle intro:

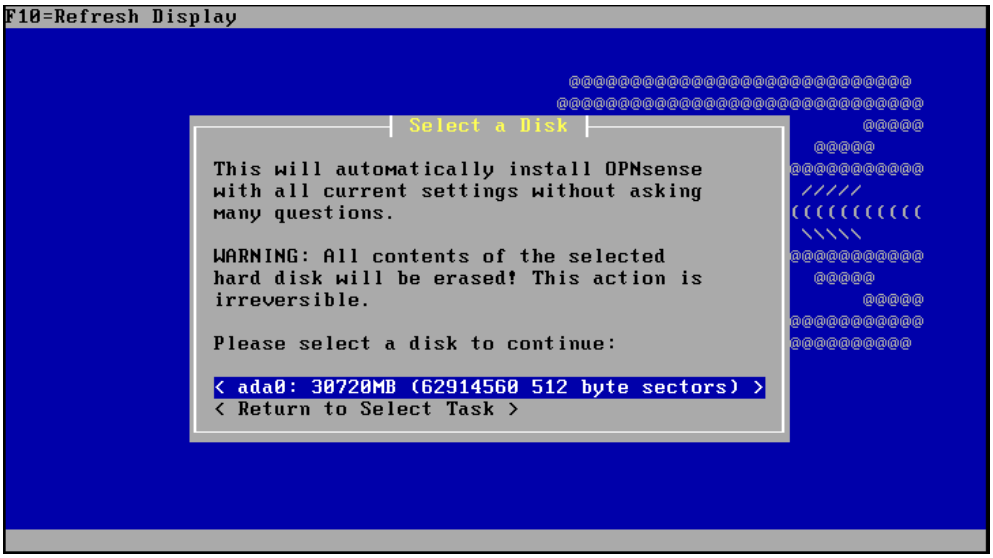
Ilustración 26 Instalación OPNSense Paso 16



Fuente: Elaboración Propia

después de seleccionar el disco duro y el modo de instalación UEFI procederá con la instalación:

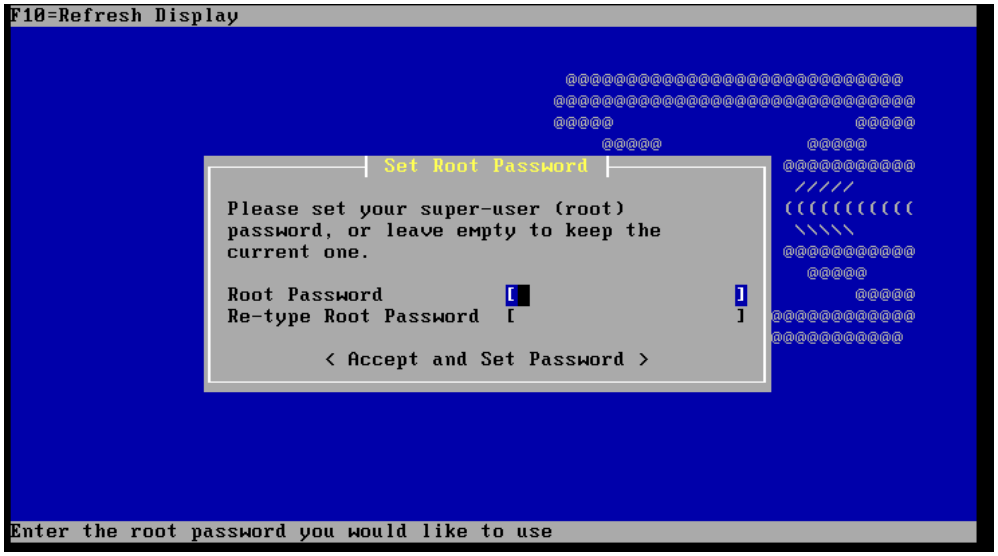
Ilustración 27 Instalación OPNSense Paso 17



Fuente: Elaboración Propia

Al finalizar la instalación nos pedirá que establezcamos una contraseña de usuario root:

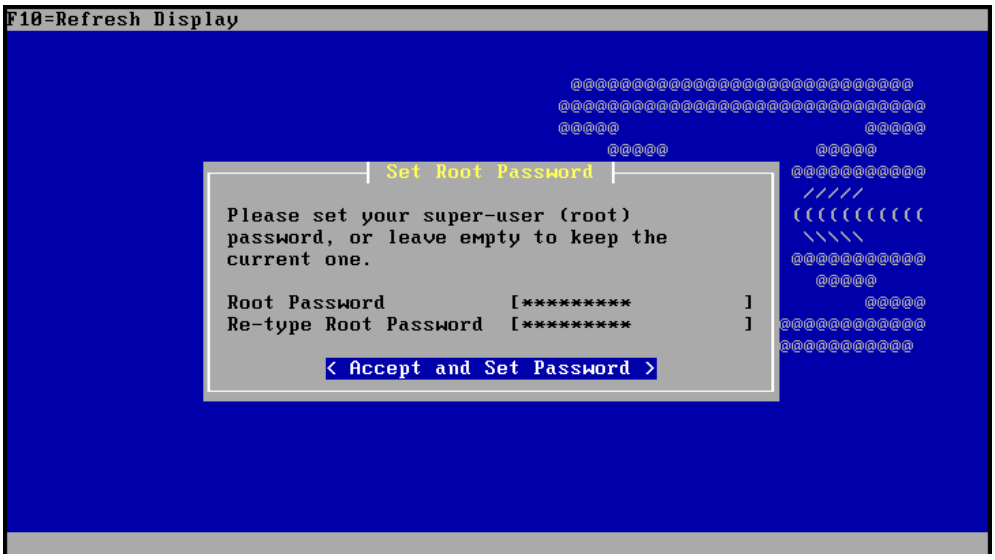
Ilustración 28 Instalación OPNSense Paso 18



Fuente: Elaboración Propia

Después de establecer una contraseña le damos Accep and set password :

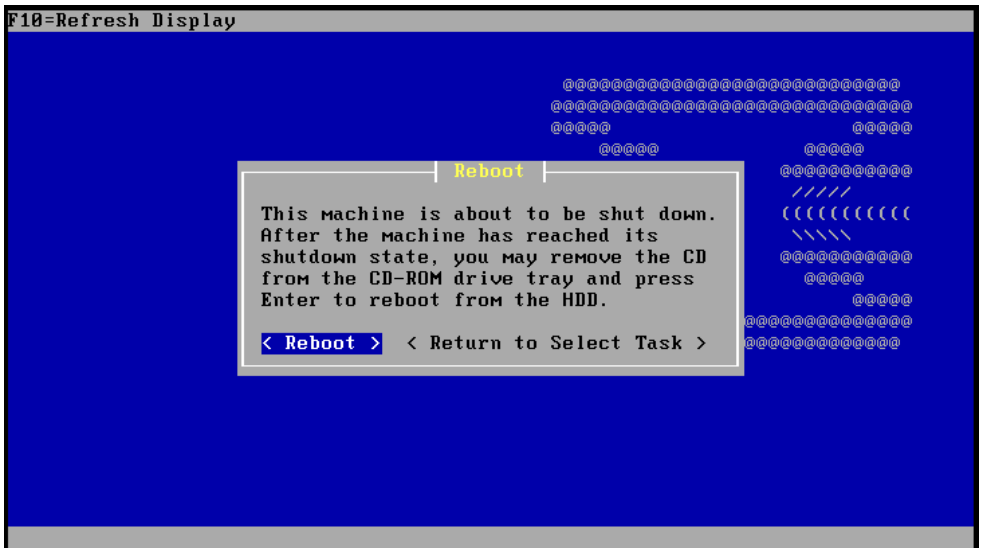
Ilustración 29 Instalación OPNSense Paso 19



Fuente: Elaboración Propia

Ahora le damos en reboot y esperamos que se reinicie el sistema:

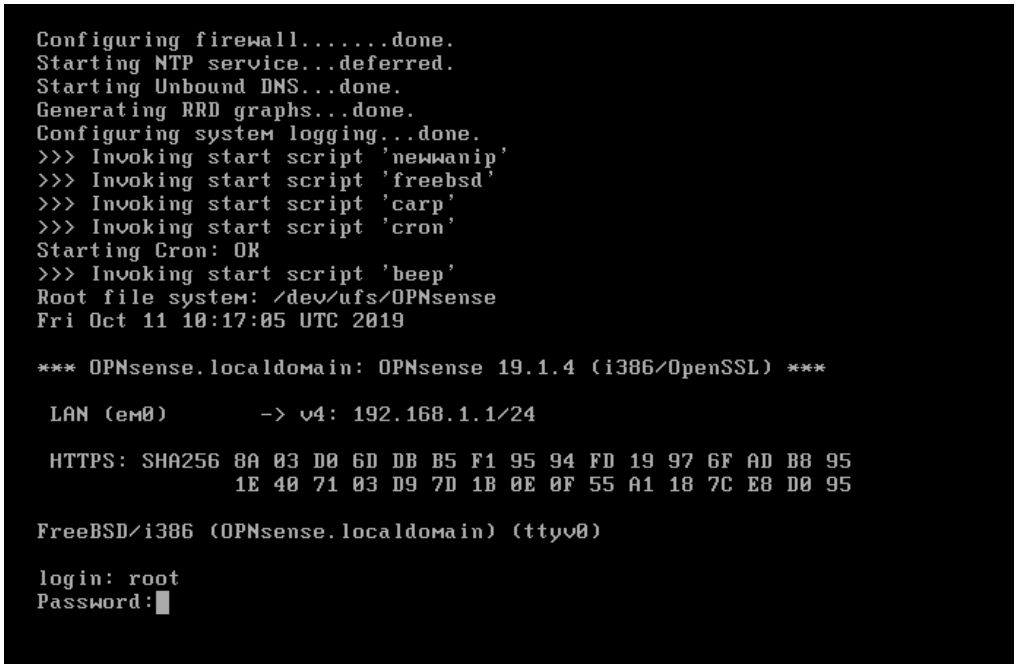
Ilustración 30 Instalación OPNSense Paso 20



Fuente: Elaboración Propia

Ahora accedemos como usuario: root y password el que hemos colocado anteriormente:

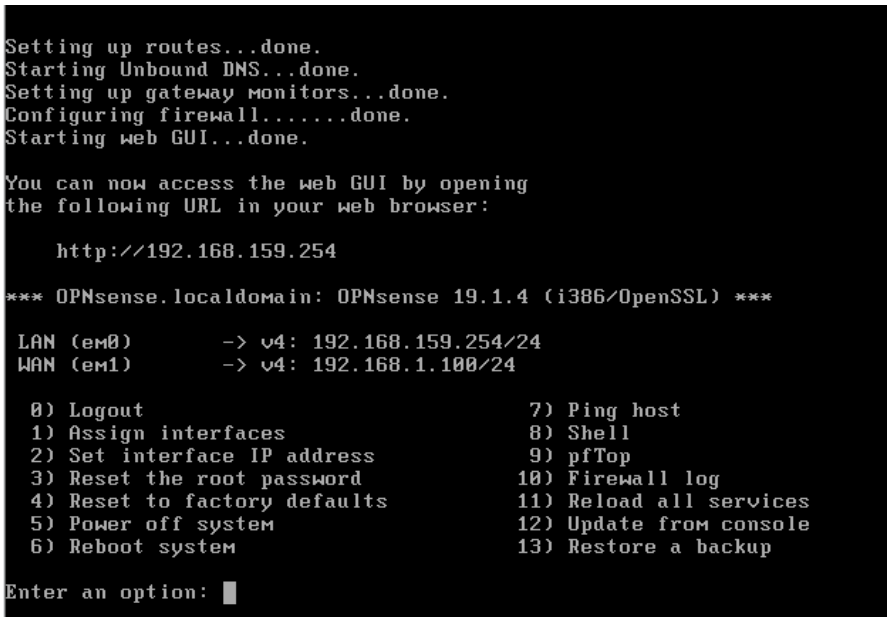
Ilustración 31 Instalación OPNSense Paso 21



Fuente: Elaboración Propia

Aquí en esta pantalla vemos la dirección ip de nuestras tarjetas de red:

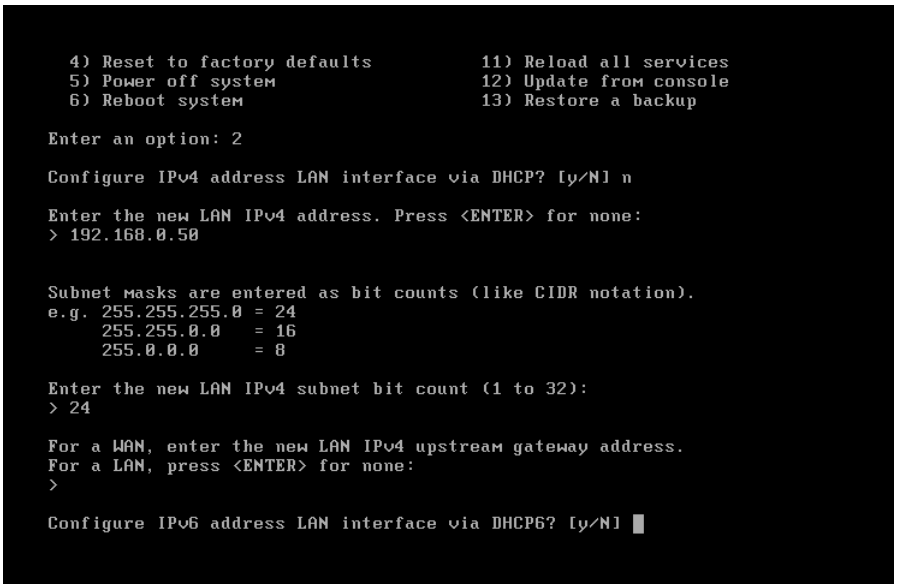
Ilustración 32 Instalación OPNSense Paso 22



Fuente: Elaboración Propia

para cambiar el ip de OPNsense seleccionamos la opción 2 y le damos nuestra nueva ip y nuestra mascara de red, presionamos enter y colocamos n en la configuración de la ipv6:

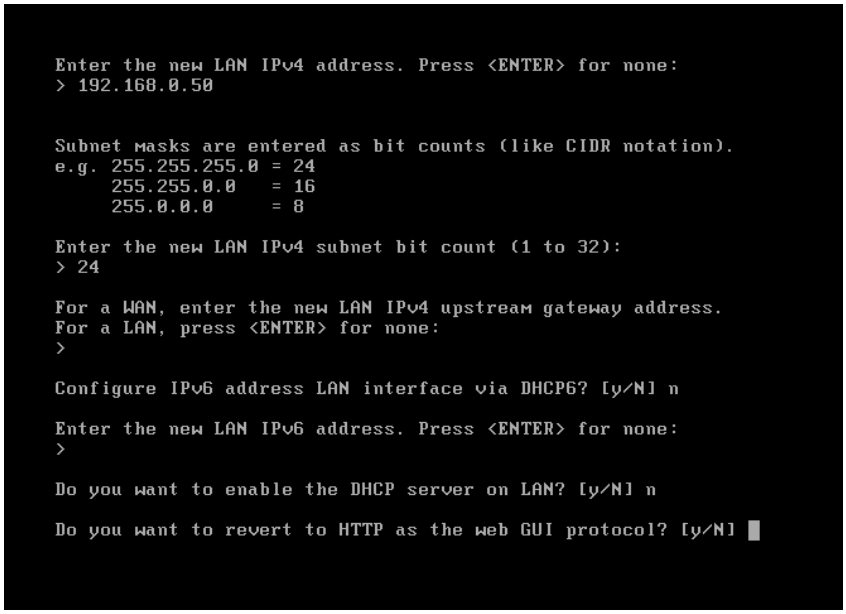
Ilustración 33 Instalación OPNSense Paso 23



Fuente: Elaboración Propia

Cuando nos pide el ipv6 lo dejamos vacío y en activar el DHCP le colocamos n, igualmente en revertir el HTTP:

Ilustración 34 Instalación OPNSense Paso 24



Fuente: Elaboración Propia

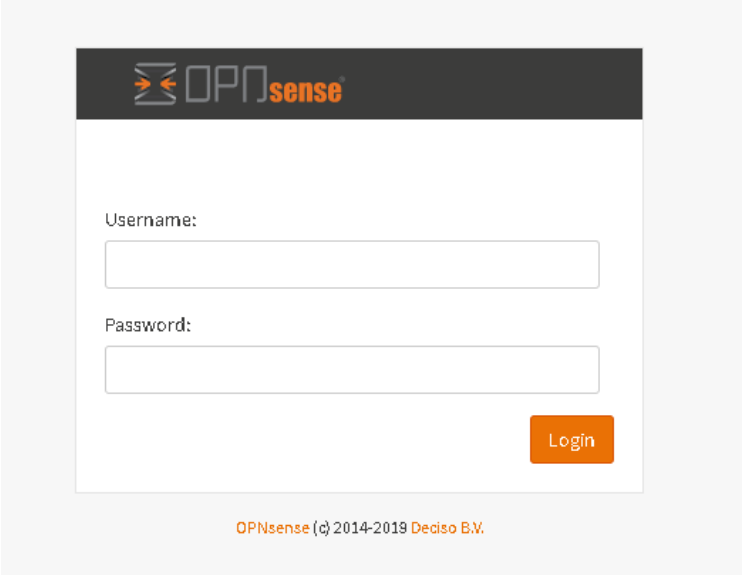
finalmente nos arroja la ip desde la que podemos acceder a OPNsense desde nuestro navegador:

Ilustración 35 Instalación OPNSense Paso 25

Fuente: Elaboración Propia

Al acceder a la IP que hemos configurado tenemos que acceder con el usuario: root y la contraseña que hemos colocado anteriormente:

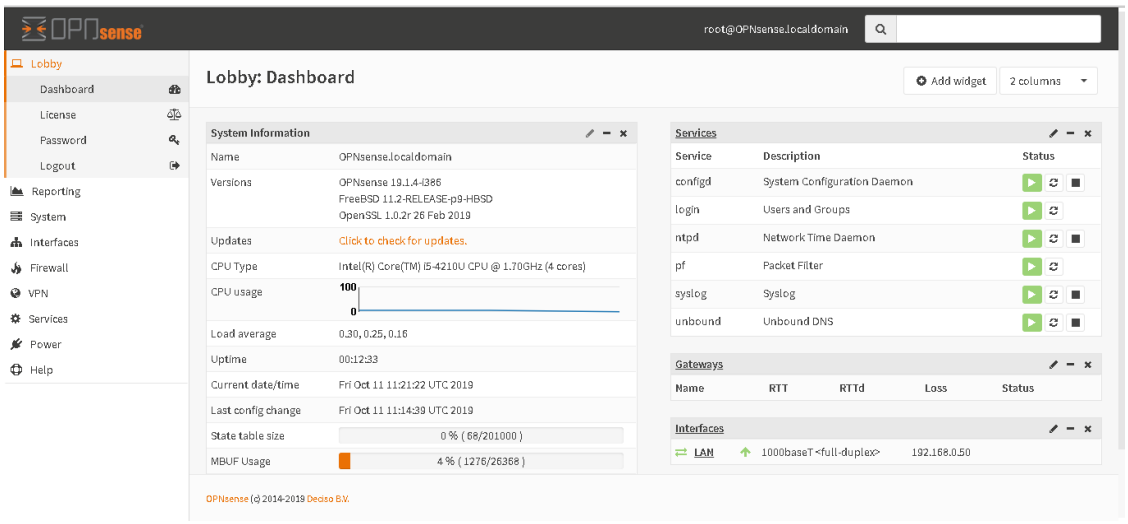
Ilustración 36 Instalación OPNSense Paso 26



Fuente: Elaboración Propia

al ingresar nos aparecerá la siguiente pantalla:

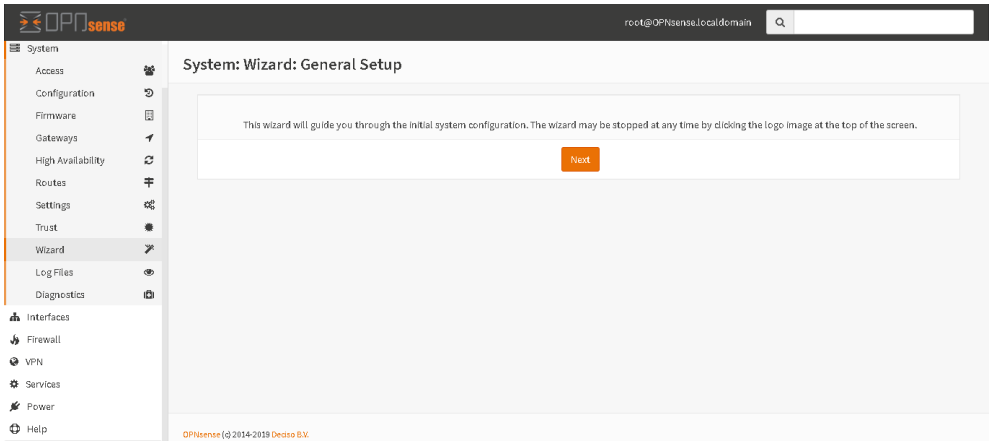
Ilustración 37 Instalación OPNSense Paso 27



Fuente: Elaboración Propia

Ahora nos vamos a system y a wizard y aquí encontraremos el asistente de configuración:

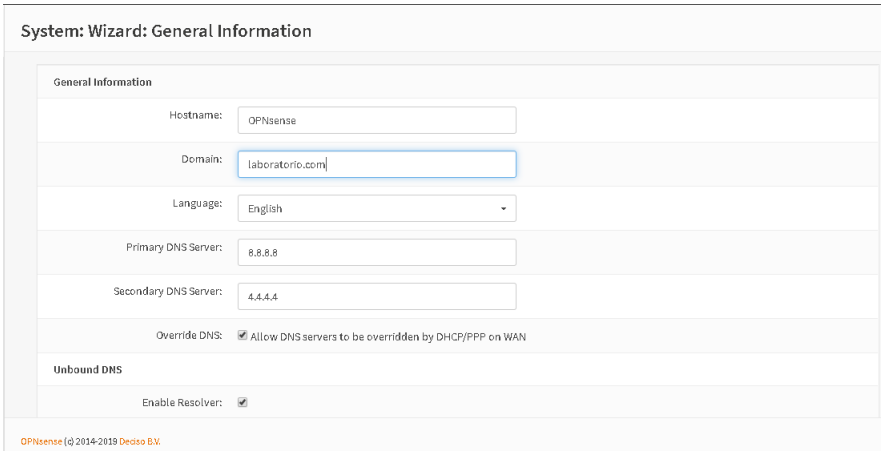
Ilustración 38 Instalación OPNSense Paso 28



Fuente: Elaboración Propia

En Hostname colocamos el nombre y en domain sería como un apellido, como la página con la que te identificaras:

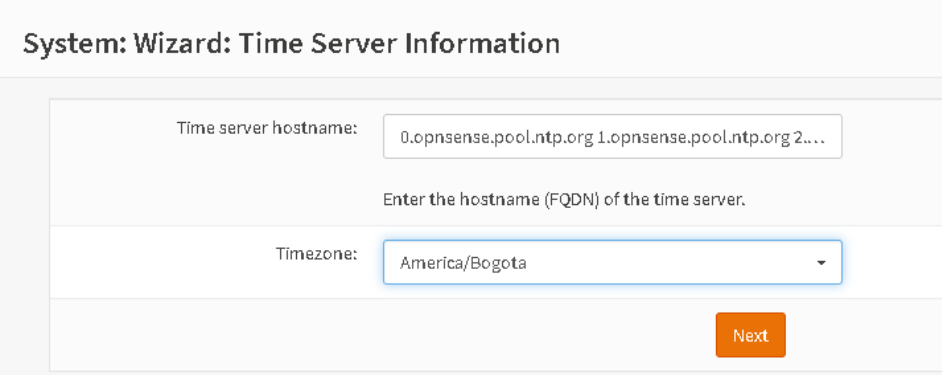
Ilustración 39 Instalación OPNSense Paso 29



Fuente: Elaboración Propia

En TimeZone seleccionamos Nuestra zona horaria:

Ilustración 40 Instalación OPNSense Paso 30



Fuente: Elaboración Propia

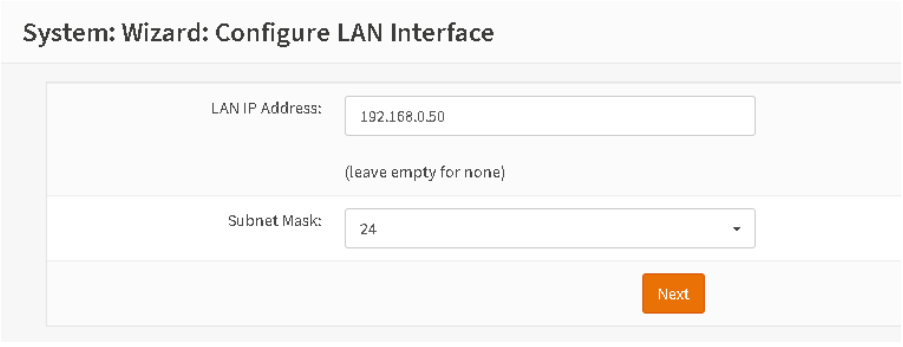
Ahora nos vamos a Static IP configuration y colocamos la ip de nuestra WAN y el Gateway, después le damos Next:

Ilustración 41 Instalación OPNSense Paso 31

Fuente: Elaboración Propia

Aquí nos pide que confirmemos la ip que hemos cambiado:

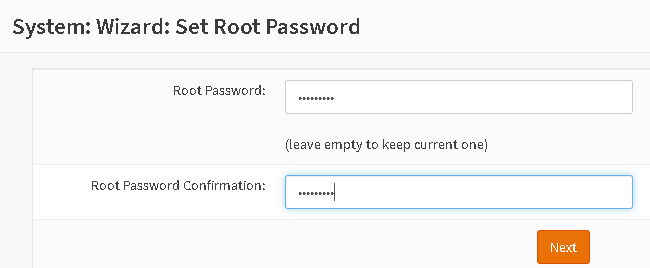
Ilustración 42 Instalación OPNSense Paso 32



Fuente: Elaboración Propia

Ahora nos da la opción de cambiar la contraseña o dejar la que estaba antes:

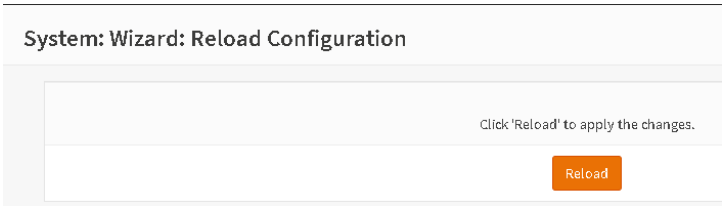
Ilustración 43 Instalación OPNSense Paso 33



Fuente: Elaboración Propia

Después nos pide que volvamos a cargar para aplicar a los cambios en la interfaz:

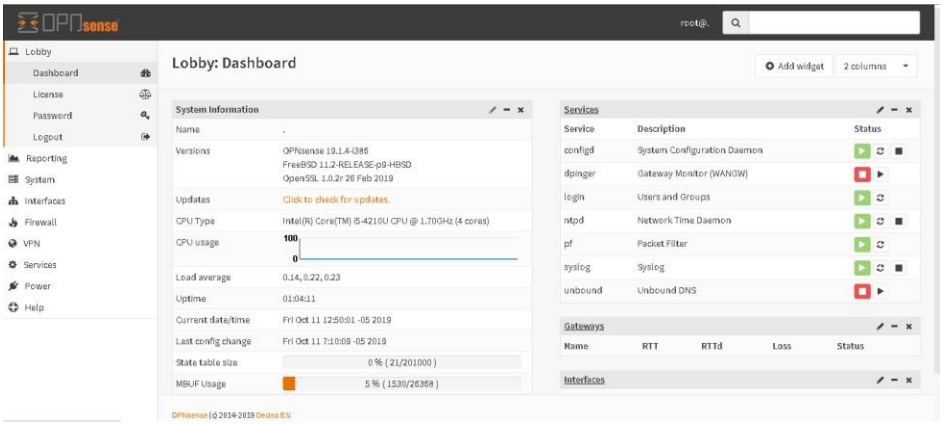
Ilustración 44 Instalación OPNSense Paso 34



Fuente: Elaboración Propia

Ahora nos muestra el dashboard o el tablero donde nos mostrara lo que hemos configurado anteriormente, siendo esta una de las configuraciones básicas de OPNsense:

Ilustración 45. Instalación OPNSense Paso 35



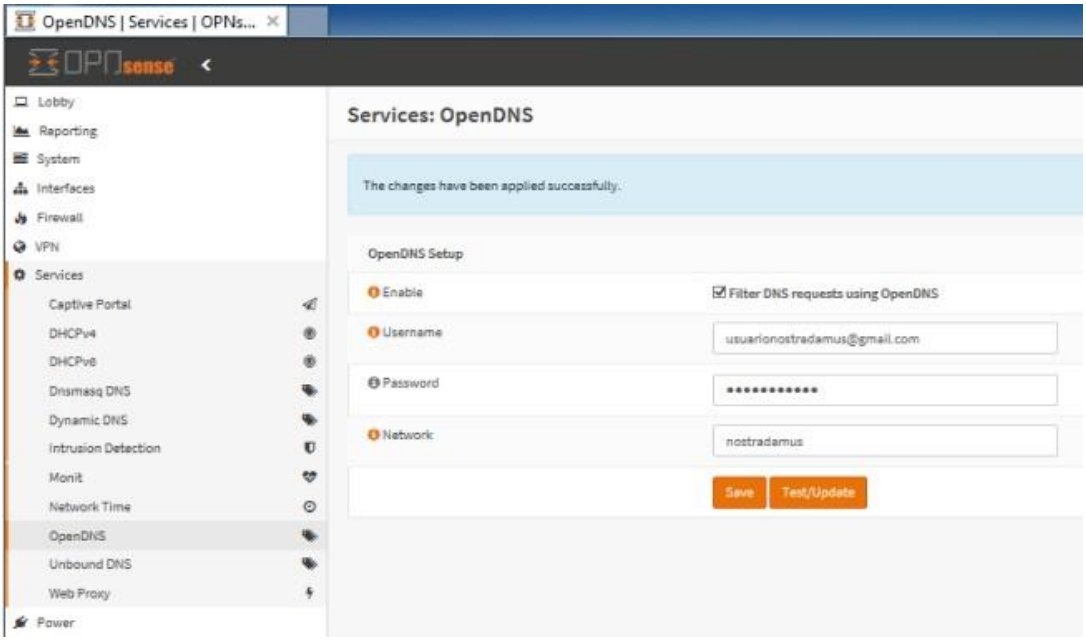
Fuente: Elaboración Propia

12.2.8 Configuraciones de seguridad en Opnsense

Una de las primeras configuraciones a realizar es la habilitación de los DNS de la herramienta OPENDNS, la cual nos ayudara a evitar ataques de tipo phishing, ya que viene tiene algunos filtros predefinidos para este tipo de ataques. Para esto se requiere que crees una cuenta en la página de https://www.opendns.com; ahí deberás indicar cuál es tu IP Publica y se te indicara cual son los DNS que debes configurar en tu DHCP.

En OPNSense debes ir a **servicios** >> **OPENDNS** y colocar las credenciales de la cuenta creada,

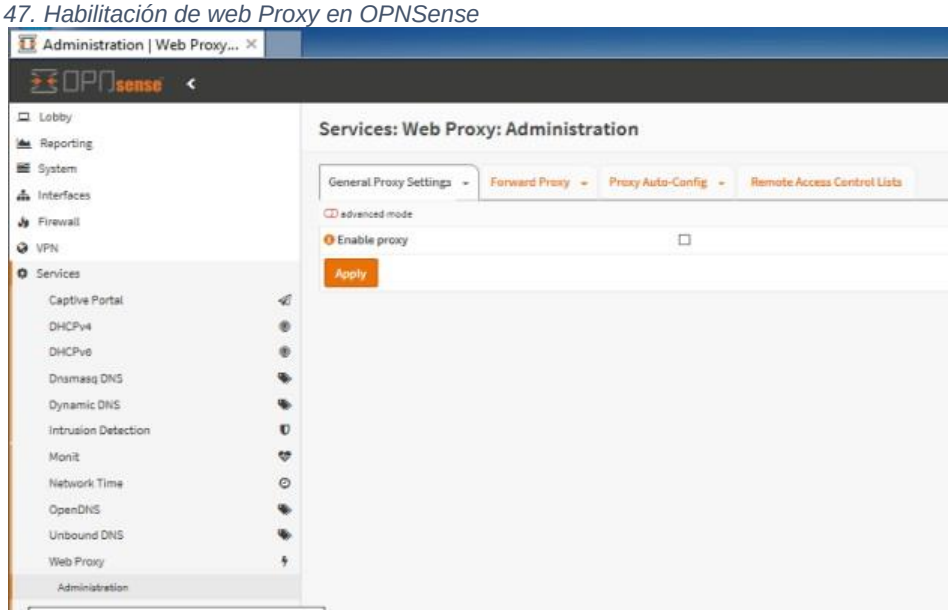
Ilustración 46. activación de Open DNS en OPNSense



Fuente: Elaboración Propia

Otra de las funcionalidades a habilitar es el servidor web Proxy; para ello nos dirigimos a **servicios >> Web Proxy >> Administration** y seleccionamos la casilla de habilitar y por último seleccionamos **aplicar**

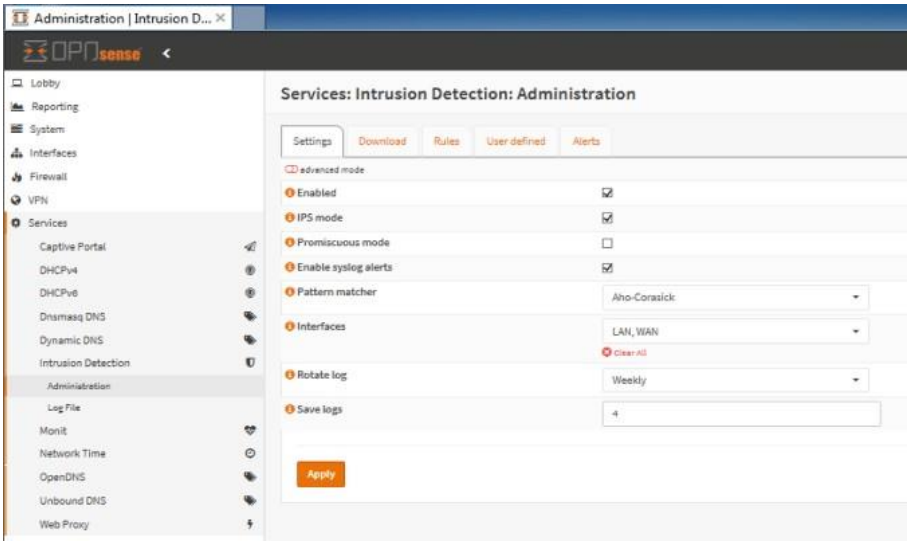
Ilustración 47. Habilitación de web Proxy en OPNSense



Fuente: Elaboración Propia

Una funcionalidad importante es la de IDS/IPS, para habilitarla debemos ir a **servicios >> Detección de Intrusos >> Administración**, y habilitamos las casillas de **habilitar, modo IPS, syslog de alertas** y en las interfaces escogemos **WAN y LAN**

Ilustración 48. Habilitación de IDS/IPS en OPNSense



Fuente: Elaboración Propia

13. CONCLUSIONES

La recreación en un ambiente controlado dentro de la organización permitió obtener la información necesaria sobre ellos vectores de ataques utilizados para vulnerar la red; facilitando la generación de un informe con las salvaguardas implementadas para mitigar los ataques.

En el planteamiento de seguridad de la información basados en la norma ISO/IEC 27000, la cual se basa en mejoras prácticas de herramientas que permiten identificar los diferentes aspectos que deben tener en cuenta las instituciones u organizaciones para establecer un modelo sostenible de un sistema de seguridad de la información.

Es necesario identificar algún método o estándar para la medición y tipificación del riesgo, además de establecer una periodicidad para la revisión de estos, considerando que los riesgos no son estáticos y que cualquier cambio en la red o en las políticas de seguridad puede cambiar la criticidad del riesgo.

Basados en el análisis y estudios realizados a la organización y tomando como referencia la norma ISO/IEC 27000, se proyectó una planeación del SGSI. El cual dentro del plan de mejora continua debe comprometer a la alta gerencia a realizar campañas periódicas de sensibilización para los empleados, en materia de seguridad de la información, con el fin de concientizarlos con relación al buen manejo que se deba dar a la información y a los elementos que dispone la empresa para su manipulación.

Por otra parte, es importante establecer umbrales en los equipos encargados del monitoreo de la red para poder generar alarmas de manera oportuna, y de esta manera aplicar las medidas que se hayan establecidos en la configuración del sistema. Además, se requiere contar con un equipo para el monitoreo de los logs de todos los dispositivos de red, preferiblemente un SIEM; considerando que son de gran ayuda para la detección de amenazas persistentes, malware, ramsonware, entre otros; los cuales son riesgos y amenazas propiamente relacionadas con la ciberseguridad, como se abordan en la ISO 27032:2015.

Por ultimo y dentro de las políticas de seguridad que se establezcan es necesario incluir en el contrato de los actuales y los nuevos trabajadores, una cláusula de confidencialidad de los datos manejados en la empresa. Además de otras políticas que permitan garantizar el cumplimiento del alcance de SGSI.

14. RECOMENDACIONES

Estandarizar el uso de formatos, que sean de fácil entendimiento para toda la empresa.

Realizar revisiones periódicas de los riesgos y las salvaguardas establecidas para los mismos.

Realizar auditorías internas para garantizar el cumplimiento de los acuerdos establecidos en el marco del SGSI.

Mantener actualizados los sistemas operativos de los PC y elementos de red.

Realizar campañas periódicas para la educación de los usuarios finales en cuanto al tratamiento de los datos.

Alinear el alcance del SGSI al cumplimiento de la MISION y VISION de la empresa.

REFERENCIAS

Deciso B.V. ABOUT OPNsense®. {En línea}. {octubre de 2019}. Obtenido de https://opnsense.org/about/about-opnsense/

OWASP®. owasp.org. {En línea}. {Ocutbre de 2019}. Obtenido de https://owasp.org/www-project-web-security-testing-guide/stable/4-Web_Application_Security_Testing/

JIMENEZ, Alejandro. Aspectos Éticos Y Legales Seguridad Informática En Colombia {En línea}. {20 marzo de 2019}. Disponible en: http://alejandrojimenezg.blogspot.es/1464187590/aspectos-eticos-y-legales-seguridad-informatica-en-colombia/

ALBERALEZ, Roberto. Modelos de madurez de seguridad de la informacion. {En línea} {En línea}. {20 marzo de 2019}. Disponible en: http://52.1.175.72/portal/sites/all/themes/argo/assets/img/Pagina/05-ModelosMadurezSeguridadInformatica.pdf

WELIVESECURITY. Auditando con Nmap y sus scripts para escanear vulnerabilidades. 2015. {En línea}. {mayo 2019}. Disponible en: https://www.welivesecurity.com/la-es/2015/02/12/auditando-nmap-scripts-escanear-vulnerabilidades/

Goodwin Gill, G. CÓDIGOS DE CONDUCTA PARA LAS ELECCIONES {En línea}. (1998). {20 marzo de 2019}. Disponible en: http://archive.ipu.org/. Obtenido de http://archive.ipu.org/PDF/publications/CODES_s.pdf

BERTOLÍN, Javier Areitio. Seguridad de la información. Redes, informática y sistemas de información. España. Editorial Paraninfo, 2008.

PICHUCHO BOMBÓN, Jorge Anibal. Elaboración De Un Módulo Para Prácticas De Laboratorio De Gestión Unificada De Amenazas En La Universidad Israel. Quito. 2017. Tesis (Ingeniero/a en Electrónica Digital y Telecomunicaciones).

CAJAS, Alexander. BENAVIDES, José. GÓMEZ, Lenin. Denegación de servicios con Hping3, herramientas virtuales, ataque y mitigación, Pag 2. {En línea}. {23 marzo de 2019}. Disponible en: https://www.researchgate.net/profile/Jose_Benavides5/publication/283084088_Denegacion_de_servicios_con_Hping3_herramientas_virtuales_ataque_y_mitigacion/links/5629b43908aef25a243d86c5

CANO DE BENITO, Juan. Despliegue de Sistema Multi-Agente para la detección y mitigación de ataques de denegación de servicios. 2018, Pag 8 y 9. {En línea}. {23 marzo de 2019}. Disponible en: http://oa.upm.es/52771/1/TFG_JUAN_CANO_DE_BENITO.pdf

Cebrián, J. M. A., Sacristán, A. G., Durán, P. L., & Bailón, A. M. Ataques a aplicaciones web. Seguridad en Bases de Datos, Módulo, 2.

CASAS MORENO, Yamil (2010). UTM: Administración Unificada de Amenazas. En: Ventana Informática. No. 22 (ene-jun., 2010). Manizales (Colombia): Universidad de Manizales. p.173-185. ISSN: 0123-9678

CORONEL AULESTIA, Luis Italo; SOTOMAYOR TORRES, Andres Fernando. Configuración e implementación de servidores DHCP, Control de tráfico y seguridad UTM en plataforma a Linux para la Universidad Católica de Cuenca Sede San Pablo de La Troncal. 2014.

COSTAS SANTOS, Jesús. Seguridad informática. España, Editorial RA-MA, 2010.

DETECCIÓN Y RESPUESTA SOBRE ATAQUES DIRIGIDOS Y MALWARE AVANZADO, Auditech, {En línea}. {20 junio de 2019}. Disponible en: https://auditech.es/endpoint-detection-response

DIARIO OFICIAL, LEY 1273 DE 2009, publicado el lunes 5 de enero de 2009. {En línea}. {20 marzo de 2019}. Disponible en: http://acueductopopayan.com.co/wp-content/uploads/2012/08/ley-1273-2009.pdf

DÍAZ OBANDO, Francisco Javier. GONZALEZ TORRES, Carlos Eduardo. Trabajo de Grado Implantación un UTM basado en software libre para gestión de seguridad lógica y perimetral en la alcaldía de Restrepo Valle. Bogotá. 2017. Trabajo de Grado (Especialista en Seguridad Informática). Universidad Abierta Y A Distancia. Escuela de Ciencias Básicas, Tecnologías e Ingeniería.

DUARTE, E. blog.capacityacademy.com. {En línea}. {3 noviembre de 2019}. Disponible en: http://blog.capacityacademy.com/2013/08/16/seguridad-informatica-cifrado-simetrico-asimetrico-hashing/

ECHENIQUE GARCÍA, José Antonio. Auditoría en informática. México: McGraw-Hill, 2001.

RAMÍREZ LUNA, César M. El Perfil Criminológico Del Delincuente Informático, 2019. {En línea}. {3 noviembre de 2019}. Disponible en: https://derecho.usmp.edu.pe/centro_estudios_criminologia/revista/articulos_revista/2013/Articulo_Prof_Cesar_Ramirez_Luna.pdf

FERNÁNDEZ MACIA, G. Ataques de denegación de servicio a baja tasa contra servidores. Granada, 2007. Tesis Doctoral. Doctor Ingeniero en Telecomunicaciones. Universidad de Granada. Departamento de Teoría de la señal telemática y comunicaciones.

OSTECBLOG. Firewall UTM Open. {En línea}. {abril de 2019}. Disponible en: https://ostec.blog/es/seguridad-perimetral/firewall-utm-open-source

FLÓREZ, Wilmar; ARBOLEDA, Carlos A.; CADAVID, John F. Solución integral de seguridad para las pymes mediante un UTM. Revista Ingenierías USBMed, 3(1), 35-42.

GAONA VÁSQUEZ, Karina del Rocío. Aplicación de la metodología Magerit para el análisis y gestión de riesgos de la seguridad de la información aplicado a la empresa Pesquera e Industrial Bravito SA en la ciudad de Machala. Cuenca, 2013. Tesis de Licenciatura (Ingeniería de Sistemas). Universidad Politécnica Salesiana.

GÓMEZ FERNÁNDEZ, L., & FERNÁNDEZ RIVERO, P. P. Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad. España: AENOR Editores. (2018).

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA. Guía para la administración del riesgo. 2011. {En línea}. {20 marzo de 2019}. Disponible en: http://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba

HERNÁNDEZ SAUCEDO, Ana Laura, MEJIA MIRANDA, Jezreel. Guía de ataques, vulnerabilidades, técnicas y herramientas para aplicaciones web. ReCIBE. Revista electrónica de Computación, Informática, Biomédica y Electrónica. {En línea}. {22 de Julio de 2019}. Disponible en: https://www.redalyc.org/articulo.oa?id=512251501005

RAMÍREZ R., Guadalupe; ÁLVAREZ D., Ezzard. Auditoría a la Gestión de las Tecnologías y Sistemas de Información Industrial. Universidad Nacional Mayor de San Marcos. {En línea}. {22 de Julio de 2019}. Disponible en: http://www.redalyc.org/articulo.oa?id=81606114

ISO27001.ES. El portal de ISO 27001 en español, {En línea}. {mayo de 2019}. Disponible en http://www.iso27000.es/iso27000.html

jSQL Injection. blog.elhacker.net. {En línea}. {mayo de 2019}. Disponible en https://blog.elhacker.net/2017/04/jsql-injection-herramienta-automatizada-java-ataques-inyeccion-sql.html

Ley de Delitos Informáticos en Colombia 2019, Delta asesores, {En línea}. {mayo de 2019} Disponible en: https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

MAIWALD, Eric; MIGUEL, Efrén Alatorre. Fundamentos de seguridad de redes. 2ª Edición. McGraw-Hill, 2005.

MARTÍNEZ SÁNCHEZ, José María. Plataforma VMware para academia virtual. 2014. Trabajo de grado (I. T. T. Telemática). Universidad Politécnica de Cartagena. Escuela Técnica Superior de Ingeniería de Telecomunicación.

MIFSUD, Elvira. Introducción a la seguridad informática-Vulnerabilidades de un sistema informático. 2012. {En línea}. {mayo 2019}. Disponible en internet http://recursostic.educacion.es/observatorio/web/es/software/software-general/1040-introduccion-a-la-seguridadinformatica?start=1

GUTIÉRREZ AMAYA H. Camilo. Metodología practica para gestión de riesgos. {En línea}. 14 de mayo de 2013. {mayo 20190}. Disponible en https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/

Mieres, J. (2009). Ataques informáticos. Debilidades de seguridad comúnmente explotadas). Recuperado http://proton.ucting.udg.mx/tutorial/hackers/hacking.pdf.

MIREYA, Deinys. Riesgos Informáticos. 2014. {En línea}. {mayo 2019}. Disponible en http://informaticaempresarialdeinys.blogspot.com/p/riesgosinformaticos-gestion-de-riesgo.html.

NARVÁEZ PORTILLO, María Elizabeth. Análisis de la distribución Kali Linux, su aplicación en la configuración de un sistema detector de intrusiones y la validación del sistema en la red de datos de la sede sur de Quito de la Universidad Politécnica Salesiana. Quito, Ecuador. 2015. 146p.Tesis de Licenciatura Ingeniería Eletrónica.

OPENSENSE:ORG. OPNSense. {En linea}. {mayo 2019}. Disponible en https://www.deciso.com/wp-content/uploads/2015/10/Deciso_About_OPNsense_latest.pdf.

OLIVEIRA, Joana; JIMÉNEZ, Rosa. El ataque de 'ransomware' se extiende a escala global {En linea}. 15 de mayo de 2017. Disponible en https://elpais.com/tecnologia/2017/05/12/actualidad/1494586960_025438.html.

ORDÓÑEZ PACHECO, Lucas D. La tecnología de virtualización en las computadoras. CienciaUAT, 2009, vol. 3, no 4.

PULGAR MONTERO, Renato Sebastián. Plan de negocios para la creación de una empresa que oferte servicios de monitoreo de incidentes informáticos llamado SOC (security operation center) para instituciones financieras en la ciudad de Quito. Quito. 2016. Tesis de Licenciatura: Universidad de las Américas, 2016.

AGUIRRE TOBAR, Ricardo Andrés. ZAMBRANO ORDOÑEZ, Andrés Fernando. Estudio para la Implementación del Sistema de Gestión de Seguridad de la Información para la Secretaria de Educación Departamental de Nariño, basado en la Norma ISO/IEC 27001. Pasto, 2015, 170p, Especialización en Seguridad Informática, Universidad Nacional Abierta y a Distancia (UNAD).

SOLARTE, Francisco. ENRIQUEZ, Edgar. BENAVIDES, María del Carmen. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. En Revista Tecnológica-ESPOL, diciembre de 2014.

TRIGO, Santiago, CASTELLOTE, Martín. PODESTÁ, Ariel. RUIZ DE ANGELI, Gonzalo, LAMPERT, Sabrina, CONSTANZO, Bruno. Ransomware: seguridad, investigación y tareas forenses {En linea}. {mayo 2019}. Disponible en https://www.researchgate.net/publication/321037574_Ransomware_seguridad_investigacion_y_tareas_forenses

GÓMEZ VIEITES, Alvaro. Auditoría de seguridad informática. Edición 2013. 148p. Ediciones de la U.

VALENCIA-DUQUE, Francisco Javier; OROZCO-ALZATE, Mauricio. 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 Tecnologías de Información, 2017, no 22, p. 73-88.

VILLALBA, Luis Javier García, et al. Malware detection system by payload analysis of network traffic. En International Workshop on Recent Advances in Intrusion Detection. Springer, Berlin, Heidelberg, 2012.

WONG, Virgilio Mosíah Montemayor. Modelo de Implementación y Operación de un Security Operation Center a Partir de sus Procesos Específicos y Basado en ITIL. Julio 2018. 88p. Maestro en Administración de Tecnologías de Información. Tecnológico de Monterrey.

MICROSOFT CSS SECURITY TEAM. Lanzamiento de actualización de seguridad de Microsoft de marzo de 2017. 2017.{En línea}. {Consultado mayo de 2019}. Disponible en https://blogs.technet.microsoft.com/seguridad/2017/03/14/lanzamiento-de-actualizacion-de-seguridad-de-microsoft-de-marzo-de-2017/

ISO27000.ES. SGSI Información fundamental sobre el significado y sentido de implantación y mantenimiento de los Sistemas de Gestión de la Seguridad de la Información. {En línea}. {marzo 2019}. Disponible en http://www.iso27000.es/sgsi.html#seccion4

MAGERIT v.3: Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. {En línea}. {marzo 2019}. Disponible en https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.XJb6xyhKjIU

ISECAUDITORS. Implementación de un Marco de Ciberseguridad ISO 27032. {En línea}. 23 de marzo de 2019. {mayo 2019}. Disponible en https://www.isecauditors.com/consultoria-csf-iso-27032

SINGH BHADAURIYA, Amit. Diferencias entre la Ciberseguridad y la Seguridad de la Información. {En línea}. Marzo 2019. {mayo 2019}. Disponible en https://blog.segu-info.com.ar/2019/03/diferencias-entre-la-ciberseguridad-y.html

ISO 27032 Gestión de Riesgos de Ciberseguridad. {En línea}. {Mayo de 2019} Disponible en https://tacticaledge.co/Gestion_de_riesgos_de_ciberseguridad_basado_en_ISO_27032.pdf

OSSTMM. Manual de la Metodología Abierta de Testeo de Seguridad. {En línea}. {mayo de 2019} Disponible en https://www.dragonjar.org/osstmm-manual-de-la-metodologia-abierta-de-testeo-de-seguridad.xhtml

GOMEZ MORALES, Giancarlo. Gestión de la Ciberseguridad según el ISO/IEC 27032:2012. {En línea}. Marzo 2017. {mayo 2019}. Disponible en https://www.linkedin.com/pulse/gesti%C3%B3n-de-la-ciberseguridad-seg%C3%BAn-el-isoiec-gianncarlo-g%C3%B3mez-morales

GOBIERNO DE COLOMBIA. Modelo Nacional de Gestión de Riesgos de Seguridad Digital. {En línea}. {mayo de 2019}. Disponible en https://www.urnadecristal.gov.co/sites/default/files/Modelo%20Gestio%CC%81n%20de%20Riesgos%20de%20Seguridad%20Digital%20Ajustado%20OAJ%20Nov%2030-2017.pdf

F1INFORMATICS. Resumen de Diferentes Informes Sobre Seguridad Informática {En Línea}. {mayo de 2019}. Disponible en http://www.f1informatics.cat/index.php/resumen-de-diferentes-informes-sobre-seguridad-informatica?lang=es.

MORENO PALOMEQUE Letty Yaneth. PALACIOS PALACIOS, Yaciry Enith. Diseño de un Sistema de Gestión de Seguridad de la Información (Sgsi) Bajo la Norma ISO 27001:2013 Para la Empresa Unisanar Ips De Quibdó. Quibdó. 2018, 195p, Especialización en Seguridad Informática, Universidad Nacional Abierta y a Distancia (UNAD).

La importancia de la norma ISO 27001. {En línea}. Abril 2013. {mayo 2019}. Disponible en https://www.esan.edu.pe/apuntes-empresariales/2016/05/norma-iso-27001-mejora-continua-en-la-gestion-de-seguridad-informacion/.

DEPARTAMENTO ADMINISTRATIVO DE LA FUNCIÓN PÚBLICA (DAFP). Guía para la administración del riesgo. {En Línea}. {mayo 2019}. Disponible en http://www.funcionpublica.gov.co/documents/418537/506911/1592.pdf/73e5a159-2d8f-41aa-8182-eb99e8c4f3ba.

SICROMTEAM. Últimos ataques de ciberseguridad a empresas. {En Línea}. {Mayo 2019}. Disponible en https://sicrom.com/blog/ultimos-ataques-ciberseguridad-empresas/

ALBERÁLEZ , Roberto. Modelos de Madurez de la Seguridad de la Información. {En Línea}. {mayo 2019}. Disponible en

http://52.1.175.72/portal/sites/all/themes/argo/assets/img/Pagina/05-ModelosMadurezSeguridadInformatica.pdf

JIMENEZ, Alejandro. Aspectos Éticos y Legales de la Seguridad Informática en Colombia. {En Línea}. {mayo 2019}. Disponible en http://alejandrojimenezg.blogspot.es/1464187590/aspectos-eticos-y-legales-seguridad-informatica-en-colombia/

ARANZAMENDI ORELLANA, Mario Ernesto. GÓMEZ COMAYAGUA, Yeferson Alexander. HÉRCULES ORELLANA, Kevin Hernán. MELÉNDEZ GARCÍA, Diego Antonio. CRIPTOGRAFÍA. El Salvador, 2017, 74p. Licenciatura en Matemáticas. Universidad de El Salvador.

AMAZON. ¿Qué es un ataque DDOS?. {En Línea}. {mayo 2019}. Disponible en https://aws.amazon.com/es/shield/ddos-attack-protection/

RAMÍREZ LUNA, César M. El Perfil Criminologico Del Delincuente Informatico. {En línea}. {mayo 2019} Disponible en https://derecho.usmp.edu.pe/centro_estudios_criminologia/revista/articulos_revista/2013/Articulo_Prof_Cesar_Ramirez_Luna.pdf.

DONGEE. La historia detrás de los ataques DoS. {En línea}. 13 de mayo de 2019. {mayo 2019} Disponible en https://blog.dongee.com/la-historia-detr%C3%A1s-de-los-ataques-dos-2f31ba1423cb.

DUARTE, E. (10 de 11 de 2019). blog.capacityacademy.com. Disponible en http://blog.capacityacademy.com/2013/08/16/seguridad-informatica-cifrado-simetrico-asimetrico-hashing/

DACCACH T, José Camilo. Ley de Delitos Informáticos en Colombia. {En línea}. {mayo 2019}. Disponible en https://www.deltaasesores.com/ley-de-delitos-informaticos-en-colombia/

FERNÁNDEZ, Luis Gómez. RIVERO, Pedro Pablo Fernández. Cómo implantar un SGSI según UNE-EN ISO/IEC 27001 y su aplicación en el Esquema Nacional de Seguridad. Edición 2018. España: AENOR Internacional, 2018.

GUTIÉRREZ AMAYA, H. Camilo, MAGERIT: metodología práctica para gestionar riesgos, {En línea}, 14 de mayo de 2013. {mayo 2019}. Disponible en https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/.

HERNÁNDEZ VILLARREAL, Yohan Esneider. Guía de remediación de vulnerabilidades informáticas para el software. Bogota, 2017, 105p. Ingeniería De Sistemas. Fundación Universitaria Los Libertadores.

PIEDRAHITA VILLARRAGA, Elkin Mauricio, et al. Análisis comparativo de un Firewall de aplicaciones web comerciales y un Open Source frente al top 10 de Owasp. Bogota, 2016, 98p, Especialización en Seguridad Informática, Universidad Nacional Abierta y a Distancia (UNAD).