PROYECTO APLICADO

Aseguramiento de la seguridad de la información desde el análisis de vulnerabilidades en la infraestructura cibernética de la empresa NOSTRADAMUS S.A.S

MARIA ALEJANDRA HURTADO VANEGAS
CHRISTIAN DAVID SIERRA BALCERO

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2020

Aseguramiento de la seguridad de la información desde el análisis de vulnerabilidades en la infraestructura cibernética de la empresa NOSTRADAMUS S.A.S

MARIA ALEJANDRA HURTADO VANEGAS
CHRISTIAN DAVID SIERRA BALCERO

Proyecto aplicado para optar por el título de Especialista en Seguridad Informática

Director/Asesor de opción de trabajo de grado
EDGAR MAURICIO LOPEZ ROJAS

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA
ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
BOGOTÁ D.C.
2020

Nota de aceptación:

_____

_____

_____

_____

Firma del presidente del jurado

_____

Firma del jurado

_____

Firma del jurado

DEDICATORIA

Christian David Sierra B.

Quiero dedicar el trabajo de proyecto de grado a mi familia, a mis compañeros de la universidad y a los docentes los cuales me apoyaron constantemente. A mi familia por estar siempre apoyándome a salir adelante y no parar cuando de conocimiento y estudio se trata. A dios por permitirme tener salud, trabajo y lograr tener el tiempo, dedicación y amor para construir este trabajo. A los docentes de la universidad que apoyaron todo el proceso de la especialización dando guías, ejemplos, casos de la vida real, retroalimentaciones y entregarme su conocimiento para ser un mejor procesional y especialista de seguridad informática.

María Alejandra Hurtado Vanegas

El presente trabajo de investigación lo dedico principalmente a Dios, por darme la motivación, fuerza, entrega, perseverancia, paciencia y sabiduría para entender y afrontar de manera correcta la realización de las diferentes actividades del trabajo.
A mis padres por su amor incondicional y apoyo durante todo este tiempo, por su esfuerzo y dedicación para brindarme estabilidad emocional y económico.
Al director del curso por su apoyo constante para el buen desarrollo del trabajo, fue una guía en el transcurso del curso.

AGRADECIMIENTOS

Christian David Sierra B.

Mi mayor agradecimiento es a mi familia por apoyarme en los momentos donde debía estar dedicado a la universidad, adicional a la universidad que por medio de un entorno virtual permite amoldarse a la vida laboral de los estudiantes.
A mi compañera de proyecto María Alejandra Hurtado Vanegas por ser una compañera constante y apoyar en la construcción no solo del proyecto de grado si no un aprendizaje mutuo en diferentes asignaturas.

María Alejandra Hurtado Vanegas

Agradezco a Dios por permitirme estudiar y prepárame para crecer cada día más profesionalmente y personalmente. A mis padres por ser mis cómplices en esta aventura de conocimiento que me enriquece como persona para ser parte de una mejor sociedad. A mis compañeros, jefes de mi entorno laboral, por permitirme realizar prácticas y socializar temas acerca de la temática vista en el curso.
A mi compañero de proyecto Christian D. Sierra B. por participar activamente en la elaboración del trabajo y debatir coherentemente los puntos de las actividades, esto fue muy enriquecedor para lograr un excelente trabajo en equipo.

CONTENIDO

Pág.

LISTA DE TABLAS

Pág.

LISTA DE FIGURAS

Pág.

LISTA DE ANEXOS

Pág.

GLOSARIO

Incidente de Seguridad de la Información: Para la norma ISO 27000 de Seguridad de la información, un incidente de seguridad es "uno o una serie de eventos de seguridad de la información no deseados o inesperados que tienen una probabilidad significativa de comprometer las operaciones comerciales y amenazar la seguridad de la información."[1]

Delito informático: Es toda acción declarada en la ley colombiana, 1273 de 2009, que atentan contra la integridad, confidencialidad y disponibilidad de la información.

Análisis de riesgos: Es el proceso que ayuda a comprender y evidenciar la naturaleza del riesgo y determinar su nivel, clasificarlo y realizar priorización.

Evaluación de riesgo: Proceso que identifica, analiza y evalúa el riesgo.

Estimación o apetito de riesgo: Es el proceso que ayuda a comprender los resultados del análisis con los criterios definidos para validar y poder determinar si el riesgo y/o su impacto son aceptados o tolerados para la organización. "De aquí se desprende el componente de continuidad de negocio"

Gestión de riesgos: Son actividades/tareas planificadas para orientar y controlar a una empresa con su mapa de riesgos.

Tratamiento de riesgos: Es el proceso que modifica o altera de manera positivo o negativa el riesgo, tener presente que si un control es mal implementado este podría representar o transformarse en otro riesgo.

Control: Es el mecanismo por el cual se contrarresta una amenaza y se reduce la probabilidad o impacto de la materialización de un riesgo.

Riesgo residual: Riesgo que queda luego de haber implementado controles o alguna acción relevante que disminuya su probabilidad o impacto.

Riesgo aceptado: Este puede ser tomado como aceptado cuando el apetito de riesgo lo permite y se pueda contrarrestar un posible impacto de manera positiva o si este llegase a impactar de manera negativa lograr sobrevivir al evento.

Vulnerabilidad: Es la debilidad de un activo "físico/digital" o de un control que puede ser aprovechado por una amenaza para ser explotado. **Amenaza:** Es el potencial de hacer daño a los activos, este se asocia con el aspecto negativo de

[1] Norma ISO/IEC 27000:2014(E). Information technology — Security techniques — Information security management systems — Overview and vocabulary. 15 de enero de 2014. p. 3.

riesgo; de aquí también se desprender los agentes de amenaza como persona o grupo que tienen una motivación o interés para hacer daño.

RESUMEN

Hoy en día con la tecnología ha generado una dependencia en los procesos y actividades de las organizaciones. El manejo de la información de los sistemas se hace cada vez más robusto y ha generado aplicar protocolos y controles de seguridad que garanticen su confidencialidad, disponibilidad e integridad de los datos.

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

Al ser una empresa de tecnología debe garantizar la confiabilidad del manejo de la información desde cliente aplicando todas las reglas y los protocolos necesarios para brindar la integridad y seguridad de los datos.

La empresa Zero Day Ltda. Presenta en el documento un servicio integral en el desarrollo del análisis, levantamiento de información hasta la fase de simulación de los ataques en entornos controlados. Generando como entregables el análisis detallado de las vulnerabilidades e incluyendo recomendaciones para su implementación. Las pruebas se basarán en los ataques identificados y se evidenciara el nivel de riesgo e impacto al explotar los fallos de seguridad sobre las tecnologías de información y comunicación. Concentramos la experiencia y formación de todo el equipo para lograr el objetivo de este proyecto.

NOSTRADAMUS S.A.S deberá reforzar su seguridad, mejorar su sistema de gestión de seguridad de la información y tomar en conjunto con la alta dirección las medidas a implementar en un corto, mediano y largo plazo.

Palabras claves: Ciberseguridad, Seguridad de la información, Seguridad informática, Riesgos, ciberseguridad, ataques, ISO 27001, SGSI.

ABSTRACT

Today with technology has generated a dependence on the processes and activities of companies. The management of the information of the systems is becoming more and more robust and the control measures that guarantee their confidentiality, integrity and availability of the data have been applied. NOSTRADAMUS SAS is a company in the technology sector that provides services to the educational, corporate and government sectors in issues related to education and training projects through the use of ICT in the implementation and configuration of learning platforms providing training and support 24 / 7. Being a technology company must guarantee confidence in the handling of information.

The company Zero Day Ltda Presents in the document an integral service in the development of the analysis, the lifting of the information up to the simulation phase of the attacks in the controlled environments. Generate detailed analysis of vulnerabilities as deliverables and include recommendations for their implementation. The evidence is based on the attacks and the level of risk and the impact on the exploitation of security on information and communication technologies are evident. Concentrate on the experience and training of the entire team to achieve the objective of this project. NOSTRADAMUS S.A.S has to do with its security, improve its information security management system and take, together with senior management, the measures to be implemented in a short, medium and long term.

Keywords: Cybersecurity, Information Security, Computer Security, Risks, Cybersecurity, Attacks, ISO 27001, ISMS.

INTRODUCCION

El presente informe se basa en el Enfoque Técnico estratégico de la empresa Nostradamus, el cual se selecciona con el fin de establecer una guía de métodos y protocolos de seguridad basados en la replicación de acontecimientos sucedidos a través de vulnerabilidades presentadas en sus sistemas de información.

Con el auge de los avances tecnológicos, las empresas se ven obligadas a ofrecer servicios que provean a sus clientes, la oportunidad de manejar la información, por ejemplo: Compras en línea, actualización de datos en línea, etc. Pero esto con lleva a garantizar y asegurar esta información para que no se use indebidamente, por eso es de importancia la seguridad informática, para establecer los controles, protocolos y demás métodos que salvaguarden la información almacenada digitalmente.
Con la elaboración del presente trabajo, se pretende establecer una propuesta guía que establezca protocolos, métodos y políticas necesarias para mitigar los posibles riesgos que conllevan exponer la información a través de la red, para esto se define el tipo de investigación Aplicada.

En el cuerpo del presente trabajo se definen las metodologías a utilizar para la construcción y desarrollo de las actividades propuestas, de acuerdo a los objetivos propuestos del presente trabajo.

1.PROBLEMA DE INVESTIGACION

1.1 ANTECEDENTES DEL PROBLEMA

Con el paso de los años se ha evidenciado los avances tecnológicos y con ellos la implementación de nuevas herramientas que ofrecen más estabilidad en la seguridad de las comunicaciones a través de la red para asegurar la transferencia segura de la información.

Pero esto sucede por los múltiples ataques de ciberdelincuentes que aprovechan las debilidades de los sistemas de información y con las vulnerabilidades identificadas acceden a través de herramientas pagas o gratuitas.

1.2 PLANTEAMIENTO DEL PROBLEMA

La imagen corporativa de la empresa está siendo haciendo afecta debido a la vulnerabilidad de sus sistemas de información por causa de ataques informáticos que han generado inestabilidad, pérdida de información e impacto reputacional.

Actualmente no existen procedimientos, manuales, instructivos definidos de seguridad de la información o seguridad informática, como tampoco existen adecuados controles, políticas y planes de contingencia y continuidad que permitan mitigar un posible evento negativo y poder continuar la operación del negocio.

Lamentablemente muchas empresas no tienen la conciencia en ciberseguridad y seguridad de la información, lo que genera a tener un panorama de riesgos muy amplio y un apetito de riesgo sin cuantificar. Los sistemas informáticos no contienen controles adecuados de seguridad “Autenticación y autorización” y esto incrementa la probabilidad de un ataque cibernético.–Actualmente los atacantes usan técnicas en donde simulan direcciones falsas, cambiando la dirección original engañando sin dejar rastros y continuar con sus ataques.

1.3 FORMULACION DEL PROBLEMA

¿Cómo el aseguramiento de la infraestructura de la compañía se puede realizar luego de un análisis y ejecución de vulnerabilidades sobre la infraestructura cibernética de la empresa?
Debido al incremento exponencial de vulnerabilidades e impacto a nivel mundial por los ataques cibernéticos, la compañía se encuentra en una exposición continua de vulnerabilidades y amenazas que pueden llevar a que varios riesgos se materialicen. Aunque los colaboradores internos no tengan el conocimiento técnico, se ha demostrado que se puede llegar atacar a infraestructura afectando su integridad, confidencialidad o disponibilidad de los sistemas de información generando un impacto mayor a su imagen corporativa, pérdida de clientes,

impactos legales y/o económicos.
A raíz de estos problemas la compañía decidió contratar una consultoría en Seguridad Informática con la empresa Zero Day Ltda., con el fin de recrear estos ataques bajo ambientes controlados simulando la explotación de vulnerabilidades, como primer reconocimiento se identificaron los siguientes ataques.

- Ransomware. “Secuestro de información”
- Denegación de Servicio.
- Infiltración de usuarios no permitidos por medio de elevación de privilegios. “robo de credenciales”
- Inyección SQL. “modificación del sistema”

2.JUSTIFICACIÓN

La evolución tecnológica ha permitido que cada vez nuestros activos de información se encuentren expuestos a múltiples amenazas conocidas y desconocidas, adicional el entorno del ciberespacio cada día crece con más empresas y usuarios conectados; esto genera un aumento positivo en áreas y procesos encargados en la ciberseguridad de una empresa. Durante "el 2018 más de 1 millón de ataques fueron efectivos el cual tiene un incremento inferior a más de 229% referente con el 2017"[2], de aquí surge la incertidumbre si las empresas están preparadas para soportar un ataque como el ransomware el cual afectó a más del 60% de compañías conectadas a internet. Sin mencionar que se desconoce las empresas que pagaron por el rescate y fueron robadas.

La empresa NOSTRADAMUS S.A.S evidencia que no todos sus procesos establecen protocolos en seguridad de la información. Es necesario establecer directrices y controles de mejoramiento continuo de los procesos de ciberseguridad y seguridad de la información. El ciberespacio se encuentra rodeado de delincuentes informáticos que se dedican al robo de información, afectar la imagen de una compañía o por medio de sus acciones apoyar un partido político, religioso, social etc. Generando una afectación operativa, económica, legal y reputacional a las compañías, personas y /o gobiernos. Dentro del análisis global de la empresa podemos encontrar amenazas externas e internas:

Amenazas externas: Ataques cibernéticos por medio de la red. "denegación de servicio"

Amenazas Internas: Robo de información por parte del personal de la misma empresa. "fraude interno"[3]

La consumación de protocolos y métodos de seguridad nivel de la infraestructura y desarrollo del software garantizaran y mitigaran el acceso no autorizado a la información por personal ajeno a la organización, generando confianza en sus clientes y proyectando así nuevas oportunidades de negocio al establecerse como una empresa que brinda plataformas seguras para la transaccionalidad y manejo de la información, Este proyecto entregará a la empresa NOSTRADAMUS S.A.S mecanismos y apoyo para la implementación de un SGSI-Sistema de seguridad de la información eficiente y efectivo, dando como primer ganancia un aseguramiento de su infraestructura con software robusto pero a bajo costo, adicional como valor agregado se entregará un set de capacitación y sensibilización a la compañía y recalcar que se tendrá etapa de estabilización del servicio.

---

[2] *Gonzalez, M. (2018) Los ataques cibernéticos se incrementaron este año.* [En línea]. Bogotá: Disponible en *https://www.dinero.com/internacional/articulo/incremento-de-ataques-ciberneticos-en-el-2018/264180*

[3] Reporte anual de ciberseguridad, CISCO 2018 Disponible en: https://www.cisco.com/c/dam/global/es_mx/solutions/pdf/reporte-anual-cisco-2018-espan.pdf

3. OBJETIVOS

3.1 OBJETIVO GENERAL

Presentar una propuesta que garantice el aseguramiento de la información partiendo del análisis de vulnerabilidades existentes en los protocolos de seguridad de la información actuales de la empresa Caso de estudio Nostradamus S.A.S

3.2 OBJETIVOS ESPECIFICOS

- Establecer la metodología a implementar de acuerdo a la norma ISO27001:2013 contemplando todos los activos de la empresa para generar el análisis de riesgos.
- Analizar el nivel de madurez del sistema de gestión de seguridad de la compañía identificando su estructura y descripción del proceso de aplicación con alcance a la infraestructura crítica y a la definición de nuevos protocolos de seguridad
- Determinar mediante el uso de herramientas de seguridad y penetración, las posibles vulnerabilidades que posee el sistema de seguridad de la empresa implicada.
- Documentar un plan de mejoramiento en temas de normatividad y protocolos de seguridad implementados en la empresa implicada para disminuir el riesgo de sufrir ATAQUES CIBERNETICOS u otros RIESGOS que afecten la seguridad de los sistemas informáticos de la empresa.

4.MARCO DE REFERENCIA

4.1 MARCO TEORICO

En la actualidad se considera la información como un activo importante en nuestra vida, define nuestro modo de vida y así como nos ayuda a llevar una vida cómoda también nos puede llevar a la muerte. pensémoslo así, si en tiempos de guerra se pusieron en juego cientos de miles de vidas por información importante, el bando que contara con la información correcta podía llevar al triunfo de sus campañas militares, y por lo contrario el que no tuviera la información correcta o suficiente podía llevar a la muerte a sus camaradas. No podemos pensar que esta premisa solo se cumple en tiempos de guerra, recordemos que esto es un caso extremo de la cotidianidad, pero si detallamos con cuidado se cumple de maneras semejantes en nuestra vida. Desde nuestros trabajos hasta nuestro entorno familiar.

En nuestro día a día obtenemos información de manera continua y asidua, y en función de esta información tomamos decisiones en cada día a día. Los sistemas informáticos funcionan a partir de principios semejantes a estos. La información que se maneja en una entidad ya sea privada publica, o incluso nuestro ámbito personal es de carácter confidencial y así como no queremos que un extraño husmee en nuestras cosas privadas, tampoco se desea que alguien que no esté autorizado a ver, almacenar o dar uso de la información de una empresa.
Basados en la premisa anterior se empezaron a implementar mecanismos que permitieran hacer una gestión de la información más segura, protegiéndola de posibles ataques, filtraciones o usos no autorizados de la misma, desde firewalls, uso de medios encriptados, antivirus etc.…

Estos mecanismos son implementados y diseñados en función de las necesidades básicas y específicas de cada entidad, adicionalmente debido a que este mercado es muy amplio existen un sinfín de herramientas y mecanismos que se permitirán la correcta elección para el cumplimiento de las necesidades de cada empresa.

“informática y comunicaciones en la empresa (carme de pablos, José Joaquín López-hermoso, editorial Esic-2014) “

4.2 DEFINICION DE CONCEPTOS

Análisis de riesgos: Es el proceso que ayuda a comprender la naturaleza del riesgo y determinar su nivel, clasificarlo y realizar priorización.

Evaluación de riesgo: Proceso que identifica, analiza y evalúa el riesgo.

Estimación o apetito de riesgo: Es el proceso que ayuda a comprender los resultados de análisis de riesgo con los criterios definidos para determinar si el riesgo y/o su impacto son aceptados o tolerados para la organización. “De aquí se desprende el componente de continuidad de negocio”

Gestión de riesgos: Son actividades planificadas con el objetivo de orientar y controlar a una empresa u organización con su mapa de riesgos.

Tratamiento de riesgos: Proceso que modifica el riesgo, tener presente que si un control es mal implementado este podría representar o transformarse en otro riesgo.

Control: Es el mecanismo por el cual se contrarresta una amenaza y se reduce la probabilidad o impacto de la materialización de un riesgo.

Riesgo residual: Resultado “Riesgo” que queda luego de haber tomado medidas de control.

Riesgo aceptado: Este puede ser tomado como aceptado cuando el apetito de riesgo lo permite y se pueda contrarrestar un posible impacto de manera positiva o si este llegase a impactar de manera negativa lograr sobrevivir al evento.

Vulnerabilidad: Es la debilidad/falencia de un activo “físico/digital” o de un control que puede ser aprovechado por una amenaza para ser explotado.

Amenaza: Es el potencial de hacer daño a los activos, este se asocia con el aspecto negativo de riesgo; de aquí también se desprender los agentes de amenaza como persona o grupo que tienen una motivación o interés para hacer daño.

Comprendiendo estas definiciones podemos apoyarnos de estándares técnicos de seguridad de la información como los de la **ISO 27000,** los cuales contienen las buenas prácticas y cada serie cuenta con un marco de énfasis y enfoque que apoya a la gestión de seguridad de la información. Este contempla funciones como la de garantizar la selección de controles de seguridad adecuados y proporcionales las mejores prácticas para proteger la información. Sus características son las de establecer una metodología de gestión de seguridad

visible, precisa y estructurada apoyando a la reducción y/o probabilidad ante la materialización del riesgo de robo, perdida o corrupción de información. **La norma ISO/IEC ISO27001** Es el estándar internacional que especifica los requisitos de seguridad de la información para la implementación del modelo de “SGSI” sistema de gestión de seguridad de la información, este estándar con el transcurso de los años ha venido mejorando e incluyendo su énfasis en gestión de riesgos como la **ISO 31000** y apoya a la mejora continua del sistema. Estos modelos contemplan dominios, objetivos de control y controles, esto define el plan para la implementación adecuada y acorde a la organización; donde se debe tener presente el alcance, la política de seguridad y la metodología de gestión de riesgos para su identificación, evaluación y tratamiento del riesgo.

El modelo de gestión de seguridad de la información (SGSI) suele estructurarse bajo la norma ISO/IEC 27001:2013 “Requerimientos de un sistema de gestión de seguridad de la información e ISO/IEC 27002:2013 “ Código de buenas prácticas para la gestión de la seguridad de la información, cuyo propósito fundamental es preservar la confidencialidad, disponibilidad, no repudio e integridad de la información a través de la aplicación de un proceso y buenas prácticas de gestión de riesgos que garantice que los riesgos de la información están siendo debidamente manejados.
El valor agregado de implementar y realizar un adecuado levantamiento, análisis y gestión de riesgos informáticos se derivan en mejorar la imagen corporativa y del negocio, mejorar la competitividad, ayuda al cumplimiento legal y regulatorio, mejora la protección y continuidad del negocio para optimizar los recursos e inversión de tecnología.

4.3 MARCO CONCEPTUAL

Las metodologías a utilizar en este proyecto son:

La metodología a utilizar por parte de la empresa Zero Day Ltda. Está basada en OSSTMM la cual ofrece una forma ordenada de todo el trabajo a ejecutar.

Metodología "OWASP"[4]- Aplicaciones web, el objetivo de esta es recopilar todas las técnicas probables de intrusión, explicarlas y estar actualizadas, esta metodología nos permite realizar pruebas con un enfoque de caja negra, esto con la finalidad de simular los ataques materializados.

Figura 1 Metodología OSSTMM

Fuente: Tomada de www.isecom.org

Cuando el ataque busca desestabilizar a la empresa lo más probable es que ataque los sistemas informáticos con el fin de ocasionar una tragedia.

Encontramos diferentes vulnerabilidades es por esto que se hará uso de mecanismos/herramientas para detectar y explotar vulnerabilidades.

"OSSTMM es un proyecto mantenido por ISECOM - Institute for Security and open methodologies, desarrollado por una comunidad abierta, y sujeto a revisión interdisciplinaria entre pares"[5]
En esta etapa se homologa una ejecución de test de intrusión, este tiene un carácter intrusivo y se encuentra orientado a identificar y explotar las

[4] Open Web Application Security Project. Obtenido 03, 2017, [En línea]. Bogotá: Disponible en http://www.isecom.org/mirror/OSSTMM.3.pdf

[5] Open Web Application Security Project. Obtenido 03, 2017, [En línea]. Bogotá: Disponible en http://www.isecom.org/mirror/OSSTMM.3.pdf

vulnerabilidades en un entorno controlado. Dentro de la metodología a implementar para este proyecto se divide en diferentes fases.

1 Planeación y especificación: Reunión de apertura y socialización con la empresa para determinar fechas de inicio y fin, alcance del proyecto, tipos de pruebas, definición de ambientes, entornos de pruebas y aspectos relevantes que lleven a la finalización efectiva y eficaz del proyecto.

2. Alcance y riesgos: Se evaluará con la empresa los posibles riesgos que estos ataques pueden conllevar e informar al cliente que si estos servidores están comprometidos se puede ofrecer el servicio de peritaje informático.

3. Levantamiento de información: Como primera instancia de un ataque es la taxonomía donde se realizará una recolección de información ya sea pública o privada de la compañía, con la finalidad de identificar posibles vectores de ataque que se ejecutaron en fases posteriores.

4. Escaneos: Se procederá a realizar una revisión exhaustiva de los servidores comprometidos, con el objetivo de descubrir puertos, servicios, vulnerabilidades y demás causas que conllevaron al ataque efectivo.

5. Revisión de vectores de ataque: Trabajo de campo con los especialistas para planear y preparar los entornos controlados basados en la información recolectada en las fases anteriores para determinar el vector de ataque utilizado y ruta del delincuente. “Posiblemente se identifique fraude interno, cómplices”.

6. Explotación: Se procede a realizar la explotación de las vulnerabilidades evidenciados en las etapas anteriores en un entorno controlado, dejando evidencia del paso a paso del atacante y como entregable para un red team o blue team de la compañía.

7. Análisis de resultados: Se validaron posibles falsos positivos, amenazas nuevas y/o alguna inconformidad del cliente.

8. Generación de informe: Se realiza la entrega de un informe ejecutivo y técnico de las actividades antes mencionadas, sin olvidar la respectiva evidencia fílmica y digital de cada simulación, como valor agregado se entregará un concepto técnico acerca de la seguridad global de la compañía y plan de capacitación y sensibilización para los empleados.

Esta metodología tendrá tarea, entregables y reuniones pactadas con la empresa NOSTRADAMUS S.A.S.

4.4 MARCO LEGAL

En Colombia existe leyes, como la “ley 1273 del 2008 ley de delitos informáticos”[8], la “Ley 1581 de 2012”[9] se dictan disposiciones para la protección de datos personales. Es el marco legal que desarrolla el derecho que tienen las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, el régimen probatorio en el Derecho Colombiano se encuentra consagrado en el Código de Procedimiento Civil, Sección tercera, Título XIII y estándares internacionales como las de la IOCE, la Convención de Cibercrimen expuesta por la Comunidad Europea, el Digital Forensic Research Workshop-DFRWS 2001, etc., donde establecen lineamientos o frameworks para identificar los delitos informáticos, recolección de evidencia digital, atención de incidentes y protección de datos personales, Sin embargo, en Colombia no tenemos normatividad puntual para la realización de pruebas de penetración, nos basamos en buenas prácticas.
Los delitos informáticos en Colombia y Latinoamérica han tenido un crecimiento exponencial y en el transcurso del 2019 según las estadísticas del caí virtual se obtiene un resultado mayor que el del 2018.

Figura 2 Ciberdelitos en Colombia 2019

Delito	Artículo	ene-19	feb-19	mar-19	Total
Uso software malicioso	269E	518	477	366	1361
Violación datos personales	269F	148	180	182	510
Acceso abusivo sistema informático	269A	115	86	128	329
Obstaculizar sistema informático	269B	53	20	35	108
Interceptación datos informáticos	269C	49	31	35	115
Daño informático	269D	30	75	35	140
Transferencia no consentida activos	269J	30	36	35	101
Estafa	246	166	614	491	1271
Extorsión	244	78	37	99	214
Hurto	269I	129	104	117	350
Pornografía infantil	218	71	20	72	163
Injuria	220	188	20	138	346
Calumnia	221	30	20	60	110
Amenazas	347	30	56	52	138
Total delitos ->		**1635**	**1776**	**1845**	**5256**

Delitos informáticos reportados en el CAI Virtual de la Policía durante los meses enero, febrero y marzo de 2019. Fuente propia.

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

[8] Congreso de la República de Colombia. (2009). *Diario Oficial. Ley 1273 de 2009*. *Diario Oficial LEY*. Bogotá D.C. Recuperado a partir de http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

[8] Congreso de la República de Colombia. (2009). *Diario Oficial. Ley 1273 de 2009*. *Diario Oficial LEY*. Bogotá D.C. Recuperado a partir de http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

4.5 MARCO ESPACIAL

Este trabajo se desarrolla en la ciudad de Bogotá D.C. Colombia, en la cual existen leyes, normatividades, frameworks, tanto nacionales como internaciones que permiten el desarrollo de este trabajo.

Este trabajo debe mejorar de manera significativa el impacto social a través del conocimiento que se plasmara para que cualquier persona que lea este trabajo, comprenda y tenga bases para lograr realizar unas pruebas de seguridad cumpliendo con los requerimientos mínimos que establece las buenas practicas del mercado apoyando la mitigación de fraudes y alinearse con la normatividad legal colombiana para el manejo de atención de incidentes y custodia de los datos.

4.6 MARCO METODOLOGICO

Para alcanzar los objetivos, se utilizará los conceptos de Investigación Aplicada.

Esto se basará en la realización de nuevas investigaciones en la empresa, identificando las áreas responsables del tratamiento de la información, categorizando el nivel de seguridad de acuerdo al tipo de dato/información que se maneja.

Se estima una fase de planificación inicial de 1 mes de duración, en donde el equipo identificara los métodos de investigación necesarios para la ejecución del proyecto. Se realizarán reuniones con las áreas interesadas y establecerá las autorizaciones necesarias para concluir el proyecto.

El proyecto tendrá 1 duración de 1 año en todas sus fases hasta cumplir con el objetivo principal.

Técnicas de recolección de Información:

- Las técnicas que se utilizaran son las siguientes:
- Encuesta
- Entrevista estructurada
- Sondeo de Opinión
- Observación
- Análisis de documentos

Se presentan los diseños generales a partir de los objetivos propuestos:

Objetivo 1: Establecer la metodología a implementar de acuerdo a la norma ISO27001:2013 contemplando todos los activos de la empresa para generar el análisis de riesgos.

Diseño general
Para el cumplimiento de este objetivo se recolectará toda la información de activos de la compañía y se realizará la matriz de riesgo a través de la metodología Margerit.
Se realizarán reuniones con el área de Infraestructura, Soporte, Recursos Humanos, Área de Desarrollo para establecer el inventario inicial de todos los activos de la compañía. Se evaluará la norma ISO27001:2013 para garantizar el cumplimiento de la matriz de riesgos se encuentra bajo la norma. Se analizará la información recolectada y será categorizada, identificando vulnerabilidades y riesgos inherentes, así como se cuantificará el nivel de riego de cada activo con su posible acción para la prevención de este.

Análisis de Documentos:
Se analizarán toda la documentación disponible (Inventarios de equipos, informes de Nomina, Informes de activos) para establecer todos los activos reales de la organización.

Objetivo 2: Analizar el nivel de madurez del SGSI de la compañía identificando su estructura y descripción del proceso de aplicación con alcance a la infraestructura crítica y a la definición de nuevos protocolos de seguridad.

Diseño general
El objetivo se cumple con la realización de entrevistas a los dueños del proceso de la información incluyendo a los oficiales de seguridad, así como el análisis de la política, instructivos y procedimientos de seguridad existentes, se redefinirá un nuevo alcance que contemple el aseguramiento de la información a través de nuevos protocolos de la seguridad de la información.
Para este punto es indispensable ya tener el primer objetivo logrado, para poder analizar el riesgo de la información en los cuales se debe centrar. En paralelo se realizarán entrevistas a los oficiales de seguridad con preguntas acerca de cuáles son los protocolos de seguridad de la información que actualmente manejan para mitigar los riesgos arrojados en el primer objetivo. Así mismo, se llevarán a cabo entrevistas con las personas del área de Infraestructura para identificar el correcto uso de los activos (Servidores, software, protocolos de red, etc.) y el cumplimiento de las políticas existentes.

Análisis de Documentos:
Se analizarán toda la documentación existente de las reglas, políticas y protocolos que existen actualmente para el manejo de la información en la compañía.

Entrevistas:
Se realizarán entrevistas programadas de mínimo 2 horas con los oficiales de seguridad, para interactuar con ellos acerca los procedimientos, políticas,

instructivos y protocolos de seguridad de la información que actualmente implementan.
Se realizarán entrevistas programadas de mínimo 2 horas con los administradores de Servidores, Administradores de Redes, Administrador del Domino para interactuar con ellos acerca de cómo se están implementando los protocolos de seguridad de la información existentes y el cumplimiento de los procesos para el manejo de la información.

Observación:
Durante el tiempo de estadía en la compañía, se recolectará información por medio de la observación de cómo se llevan los procesos internos, si se cumplen realmente el uso de las políticas de seguridad.

Objetivo 3: Determinar mediante el uso de herramientas de hacking, las posibles vulnerabilidades que posee el sistema de seguridad de la empresa implicada.

Diseño general
El objetivo se cumple utilizando software para la infiltración en diferentes sistemas de la compañía, la decodificación de contraseñas para validar las políticas de seguridad implementadas en las contraseñas y métodos que simulen robos de información. Basándose en la matriz de riesgos ya generada, se planea un plan de trabajo de simuladores de hackeo de la información, para evidenciar las vulnerabilidades existentes con los protocolos de seguridad actuales y de este mismo modo, servir como base documental para generar nuevas políticas de seguridad que se ajusten a la infraestructura actual.

Análisis de Documentos:
Se analizará la información de manuales de usuario, manuales técnicos de aplicaciones de software para entender su funcionamiento de negocio e planificar un plan de trabajo para la generación de los simuladores.
Se analizarán el diseño arquitectónico de las redes para identificar los posibles ataques a simular.

Encuestas:
Se realizarán encuestas a los usuarios funcionales con preguntas acerca del funcionamiento de los diferentes aplicativos que manejan (Tipos de Login, bloqueos del aplicativo, permisos y roles sobre la información).

Observación:
Durante el tiempo de estadía en la compañía, se recolectará información por medio de la observación de cómo los usuarios finales utilizan los diferentes sistemas de información.

Objetivo 4: Documentar un plan de mejoramiento en temas de normatividad y protocolos de seguridad implementados en la empresa implicada para disminuir el riesgo de sufrir ATAQUES CIBERNETICOS u otros riesgos que afecten la seguridad de los sistemas informáticos de la empresa.

Diseño general
Para el cumplimiento de este objetivo, se realizará la documentación necesaria incluyendo los riesgos encontrados en el tratamiento de la información, así como sus respectivas correcciones incluyendo las mejores a nivel de recursos de infraestructura, metodologías de desarrollo de software.
Esta fase se contempla que se realizara en paralelo, es decir, desde el inicio de la recolección de la información para cumplir el primer objetivo, se empezara a documentar el plan de mejoramiento basado en los hallazgos identificados en cada una de las actividades que se desarrollan para el cumplimiento de los objetivos propuestos en el proyecto.

Análisis de Documentos:
Se analizará la información acerca de la normativa legal y de calidad para garantizar el marco actualizado de trabajo.
Toda la documentación existente acerca de los procesos de la compañía.
Todos los manuales y documentación acerca de los protocolos y políticas de seguridad existentes.
Documentación acerca de últimos ataques a nivel mundial en empresas del sector.

Entrevistas:
Para entender mejor el proceso, se programarán reuniones para la recopilación de la información de los procesos con las áreas interesadas.

Observación:
Durante el tiempo de estadía en la compañía, se recolectará información por medio de la observación de cómo se manejan los procesos en la compañía a nivel general.

Sondeo de Opinión:
Se enviarán por correo electrónico, pequeñas encuestas para generar debate de cuáles pueden ser posibilidades de mejores en los sistemas de información.

MÉTODOS Y MODELOS DE ANÁLISIS DE LOS DATOS:

Análisis de Escenarios: Se van a simular diferentes ataques en donde se analizará cada uno de ellos identificando los diferentes resultados para determinar las vulnerabilidades y/o fallos en los sistemas de información y ejecutar la mejor decisión para la implementación del plan de mejoramiento.

PROGRAMAS A UTILIZAR PARA ANÁLISIS DE LOS SISTEMAS

Encontramos diferentes vulnerabilidades es por esto que se hará uso de mecanismos/herramientas para detectar y explotar vulnerabilidades, serán utilizadas las siguientes herramientas:

- **Distribución Kali Linux:** Nueva generación de herramientas de intrusión y auditoría de seguridad, anteriormente llamada backtrack, esta contiene más de 600 herramientas de pruebas.
- **MetaSploit Framework:** Es una plataforma de explotación de vulnerabilidades ejecución de exploits que contiene varias herramientas que permiten realizar pruebas de vulnerabilidades.
- **Analizador de vulnerabilidades Nessus**: Programa de escaneo de vulnerabilidades.
- **Analizador de vulnerabilidades Openvas**: Programa de escaneo de vulnerabilidades.
- **SQLMAP**: herramienta de pruebas de penetración para inyección de SQL.
- **Lazagne**: herramienta que permite extraer información de autenticación guardad sobre los equipos “Sam y navegadores”.

4.7 RECURSOS

Tabla 1 Recurso necesario para proyecto

RECURSO	DESCRIPCIÓN	PRESUPUESTO
1. **Equipo Humano**	1 Oficial de seguridad. 1 Analista de pruebas de seguridad. 1 consultor de seguridad e infraestructura.	$30.000.000 Propio, el consultor apoyo UNAD.
2.**Equipos y Software**	2 Computadores portátiles (Windows y Mac) • RAM de 16 GB, Procesador I5, Almacenamiento 1 TB. RAM de 8 Gb DDR3, procesador Core i5 de almacenamiento de 500 Gb–Sistema de virtualización (VirtualBox y VMWARE) Máquinas virtuales “Windows, y linux"	$7.000.000 Propio
3. **Viajes y Salidas de Campo**	Acompañamientos, reuniones en sitio, transporte	$400.000 Propio
4. **Materiales y suministros**	Acceso a las instalaciones de NOSTRADAMUS SAS “Tarjeta de acceso”	No aplica

5. **Bibliografía**	Autoestudio	No aplica
TOTAL $37.400.000		

4.8 CRONOGRAMA

1. Tabla 2 Cronograma de actividades

10. **CRONOGRAMA DE ACTIVIDADES**												
ACTIVIDAD	**MES 1**	**MES 2**	**MES 3**	**MES 4**	**MES 5**	**MES 6**	**MES 7**	**MES 8**	**MES 9**	**MES 10**	**MES 11**	**MES 12**
Análisis e identificación de activos de información.	x											
Análisis e identificación de riesgos "Inherente"	x											
Análisis de los protocolos de seguridad existentes para manejo de la información	x											
Implementación de entornos controlados (Instalación de máquinas virtuales)	x											
Implementación de herramientas hacking		x										
Ejecución de plan de pruebas para determinar vulnerabilidades		x										
Simulación de ataque del sistema operativo W7 haciendo uso de la **ingeniería social**		x										
Simulación de ataque **elevación de privilegios** en el sistema operativo windows		x	x									
Simulación de ataque **denegación de servicios** en el sistema operativo windows			x	x								
Simulación de ataque **Ransomware** en el sistema operativo windows				x	x	x						
Generación de informe de simulación de ataques						x	x					
Diseño de soluciones de metodologías y procedimientos de protocolos de seguridad.						x	x					
Generación de propuesta de aseguramiento de la información							x	x	x			
Generacion de informe de plan de mejoramiento en los protocolos de seguridad de la información							x	x	x			
Entrega y capacitación de personal aplicando la solución de la nueva propuesta.		x		x		x		x	x			
Soporte y acompañamiento a la nueva implementación								x	x	x	x	x

Fuente: planeación con equipo de trabajo.

5.RESULTADOS

CUMPLIMIENTO DE OBJETIVOS

i. Establecer la metodología a implementar de acuerdo a la norma ISO27001:2013 contemplando todos los activos de la empresa para generar el análisis de riesgos.

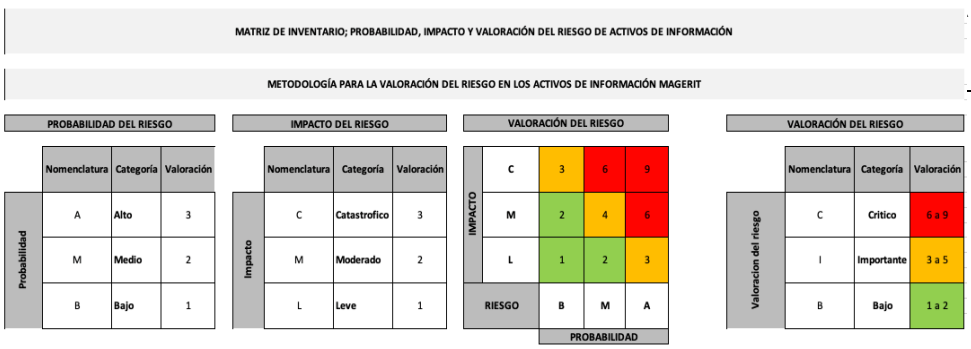
ANALISIS DE RIESGOS E IDENTIFICACION DE ACTIVOS

Tabla 3 Análisis de riesgos e identificación de activos NOSTRADAMUS

OBJETIVO	Realizar la identificación, análisis y evaluación de los activos y riesgos de seguridad de la información.
ALCANCE	Aplica para los activos dela Empresa
Nombre de la Empresa:	**NOSTRADAMUS S.A.S**
Sitio web:	**PAGINA WEB ALOJADA EN UN TERCERO**
Descripción de la empresa:	una empresa del sector tecnológico que brinda servicios a los sectores: educativo, corporativo y gubernamental en temas relacionados con proyectos de educación y capacitación a través del uso de TIC desde la implementación y configuración de plataformas de aprendizaje brindando capacitación y soporte 24/7
CONTEXTO LEGAL	NTC ISO/IEC 27001 - NTC ISO/IEC 27005 - NTC ISO/IEC 31000
ENFOQUE METODOLOGICO	El enfoque de gestión de riesgos a aplicar está basado en la metodología **MAGERIT**
TRATAMIENTO	Se tratarán los riesgos cuyos niveles sean:
	CRITICO Eje. CRITICO
	Se aceptarán los riesgos cuyo resultado después de la valoración de riesgos sean:
	BAJO (1 – 2) **IMPORTANTE** (3 – 5)
	Niveles de aceptación del riesgo (1 a 2 aceptable (A), 3 a 5 moderado (M), 6 a 9 inaceptable(I))
	Una vez aplicados los controles se acepta un riesgo de residual

en niveles **BAJO** o **IMPORTANTE**

Criticidad residual (1 a 2 aceptable (A), 3 a 5 moderado (M), 6 a



METODOLOGIA

Figura 3 Metodología

Fuente: gestión de activos ISO 19001

IDENTIFICACION DE ACTIVOS

Tabla 4 Identificación de activos de información

No.	DATOS DEL ACTIVO DE INFORMACIÓN			TIPO									
	Nombre del activo de información	Proceso propietario del activo	Responsable	[D] DATOS	[K] CLAVES CRIPTOGRÁFICAS	[S] SERVICIOS	[SW] SOFTWARE	[HW] EQUIPAMIENTO INFORMÁTICO	[COM] REDES DE COMUNICACIONES	[Media] SOPORTE DE INFORMACIÓN	[AUX] EQUIPAMIENTO AUXILIAR	[L] INSTALACIONES	[P] PERSONAL
1	[www] Página Web http://104.236.31.57/Test_SQLInj/	Departamento de Sistemas	Jefe tecnología-plataforma			X							
2	[print] medios de impresión	Oficina de dirección	Jefe tecnología-servicios					X					
3	[print] medios de impresión	Oficina de contabilidad	Jefe tecnología-servicios					X					
4	[app] servidor de intranet server 2008	Datacenter I	Jefe tecnología-plataforma				X						
5	[app] servidor de aplicaciones server 2008	Datacenter I	Jefe tecnología-plataforma				X						
6	[app] servidor de aplicaciones server 2016	Datacenter I	Jefe tecnología-plataforma				X						
7	[File] servidor de archivos	Datacenter I	Jefe tecnología-plataforma	X									

8	[Firewall] Cortafuegos	Departamento de Sistemas	Jefe tecnología-Seguridad informática					X					
9	[SW] SOFTWARE ANTIVIRUS – McAfee	Departamento de Sistemas	Jefe tecnología-Seguridad informática				X						
10	[host] Equipo de cómputo w7	Oficina de Contabilidad	auxiliar contable					X					
11	[host] Equipo de cómputo w7	Oficina de Contabilidad	auxiliar contable	X				X					
12	[host] Equipo de cómputo w7	Oficina de Contabilidad	jefe contable					X					
13	[host] Equipo de cómputo w7	Oficina recursos humanos	Psicóloga					X					
14	[host] Equipo de cómputo w7	Oficina recursos humanos	jefe de contratación	X				X					
15	[host] Equipo de cómputo w7	Oficina recursos humanos	jefe recursos humanos					X					
16	[host] Equipo de cómputo w10	Oficina recursos compras	negociador compras					X					
17	[host] Equipo de cómputo w10	Oficina tecnología - plataforma	jefe de área					X					
18	[host] Equipo de cómputo w10	Oficina tecnología - Servicios	jefe de área					X					
19	[host] Equipo de cómputo w10	Oficina tecnología - Seguridad informática	jefe de área					X					
20	[host] Equipo de cómputo w10	Oficina tecnología - Mesa de ayuda	técnico soporte					X					
21	[host] Equipo de cómputo w10	Oficina tecnología - soporte	técnico soporte					X					
22	[host] Equipo de cómputo w10	Oficina tecnología - soporte	técnico soporte								X		
23	[hub] CONCENTRADORES – Principal	red de datos	Administrador de la red					X					
24	[hub] CONCENTRADORES – Principal	red de datos	Administrador de la red					X					
25	[hub] CONCENTRADORES - Secundario	red de datos	Administrador de la red					X					
26	[SWITCH] CONMUTADORES	red de datos	sala de Contabilidad					X					
2	[SWITCH]	red de datos	Departamento de					X					

7	CONMUTADORES		Sistemas										
28	[SWITCH] CONMUTADORES	red de datos	Recursos humanos					X					
29	[SWITCH] CONMUTADORES	red de datos	compras					X					
30	[IPPHONE] TELÉFONO IP	oficina de contabilidad	sala de Contabilidad					X					
31	[IPPHONE] TELÉFONO IP	departamento de Sistemas	Departamento de Sistemas					X					
32	[IPPHONE] TELÉFONO IP	Oficina recursos humanos	Recursos humanos					X					
33	[IPPHONE] TELÉFONO IP	dependencias del centro	compras					X					
34	[IPPHONE] TELÉFONO IP	dependencias del centro	técnico soporte					X					
35	[IPPHONE] TELÉFONO IP	dependencias del centro	técnico soporte					X					
36	[wap] PUNTO DE ACCESO INALÁMBRICO	Departamento de Sistemas	Recursos humanos					X					
37	[wap] PUNTO DE ACCESO INALÁMBRICO	Departamento de Sistemas	sala de Contabilidad					X					
38	[wap] PUNTO DE ACCESO INALÁMBRICO	Sala de Sistemas	Departamento de Sistemas					X					
39	[wap] PUNTO DE ACCESO INALÁMBRICO	Sala de Sistemas	técnico soporte					X					
40	UPS	Sala de Sistemas	Administrador mantenimiento					X					
41	Software RH	Departamento de Sistemas	Recursos humanos			X							
42	Software Contable	Departamento de Sistemas	sala de Contabilidad	X									
43	Software ERP	Sala de Sistemas	Departamento de Sistemas			X							
44	Software utilitarios	Sala de Sistemas	técnico soporte										X

VALORACION DEL RIESGO

ACTIVOS CRITICOS

Tabla 5 Activos Críticos

Nombre	Riesgo
[www] Página Web http://104.236.31.57/Test_SQLInj/	CRITICO
[print] medios de impresión	CRITICO
[print] medios de impresión	CRITICO
[app] servidor de intranet server 2008	CRITICO
[app] servidor de aplicaciones server 2008	CRITICO
[app] servidor de aplicaciones server 2016	CRITICO
[File] servidor de archivos	CRITICO
[Firewall] Cortafuegos	CRITICO
[host] Equipo de cómputo w10_Srv	CRITICO
[SWITCH] CONMUTADORES PRINCIPAL	CRITICO
[host] Software ilegal violación de derechos de autor	CRITICO

ACTIVOS IMPORTANTES

Tabla 6 Activos Importantes

Nombre	Riesgo
[SW] SOFTWARE ANTIVIRUS - McAfee	IMPORTANTE
[hub] CONCENTRADORES - Principal	IMPORTANTE
[hub] CONCENTRADORES - Principal	IMPORTANTE
[hub] CONCENTRADORES - Secundario	IMPORTANTE
[wap] PUNTO DE ACCESO INALÁMBRICO	IMPORTANTE
[wap] PUNTO DE ACCESO INALÁMBRICO	IMPORTANTE
UPS	IMPORTANTE

ACTIVOS BAJOS

Tabla 7 Activos Bajos

Nombre	Riesgo
[IPPHONE] TELÉFONO IP	BAJO
[IPPHONE] TELÉFONO IP	BAJO
[IPPHONE] TELÉFONO IP	BAJO
[host] Equipo de cómputo w7	BAJO
[host] Equipo de cómputo w7	BAJO
[host] Equipo de cómputo w7	BAJO
[host] Equipo de cómputo w7	BAJO
[host] Equipo de cómputo w7	BAJO
[host] Equipo de cómputo w7	BAJO
[host] Equipo de cómputo w10	BAJO
[host] Equipo de cómputo w10	BAJO

[host] Equipo de cómputo w10	BAJO
[host] Equipo de cómputo w10	BAJO
[host] Equipo de cómputo w10	BAJO
[host] Equipo de cómputo w10	BAJO
[SWITCH] CONMUTADORES SECUNDARIO	BAJO
[SWITCH] CONMUTADORES SECUNDARIO	BAJO
[IPPHONE] TELÉFONO IP	BAJO
[IPPHONE] TELÉFONO IP	BAJO
[IPPHONE] TELÉFONO IP	BAJO

AMENAZA Y VULNERABILIDADES

Frecuencia de amenazas:

Tabla 8 Frecuencia de Amenaza

Valor			Criterio
4	Muy frecuente	MF	A diario
3	Frecuente	F	Mensualmente
2	Normal	N	Una vez al año
1	Poco frecuente	PF	Cada varios años

Degradación de las amenazas:

Tabla 9 Degradación de Amenaza

Valor		Criterio
100%	MA	Degradación MUY ALTA del activo
80%	A	Degradación ALTA considerable del activo
50%	M	Degradación MEDIANA del activo
10%	B	Degradación BAJA del activo
1%	MB	Degradación MUY BAJA del activo

La identificación de las amenazas la realizaremos con el uso de la Metodología MAGERIT, que en resumen nos permite es medir el riesgo que pueden presentarse o están expuestos los diferentes activos. También nos permite medir los criterios de afectación de la confidencialidad, disponibilidad e integridad de la información.

ii. Analizar el nivel de madurez del sistema de gestión de seguridad de la compañía identificando su estructura y descripción del proceso de aplicación con alcance a la infraestructura crítica y a la definición de nuevos protocolos de seguridad

La ISO/IEC 27002:2013 habla de los controles que se establecen para garantizar la adecuada gestión de la seguridad de la información, pero hay que tener presente que algún control es o no aplicable, es necesario documentar y justificar y aquí es donde entra la Matriz SOA "declaración de aplicabilidad".

A continuación, se detallan los requisitos de norma de la ISO/IEC 27001:2013 adicional su relación con el ciclo de calidad y gestión.

Figura 4 Requisitos ISO/IEC 27001:2013

ISO/IEC 27001:2013	Ciclo PHVA
Introducción	
1.Objetivo y campo de aplicación	
2.Referencias Normativas	
3.Terminos y definiciones	
4.Contexto de la organización	PLANEAR
5.Liderazgo	
6.Planificacion	
7.Soporte	
8.Operaciones	HACER
9.Evaluacion del desempeño	VERIFICAR
10.Mejora	ACTUAR

Fuente: el Autor

Contexto de la organización: Las entidades deben determinar los aspectos internos y externos que son requeridos para su objetivo y que pudiesen afectar el cumplimiento de sus objetivos, esta posible afectación impactaría los resultados previstos al sistema de Gestión de la Seguridad de la Información – SGSI.

Liderazgo: La alta dirección deberá demostrar y apoyar el compromiso y liderazgo con todo lo relacionado al Sistema de Gestión de la Seguridad de la Información – SGSI, de aquí se desprenden responsabilidades frente a: se establezcan políticas y objetivos de seguridad los cuales se encuentren alienados a la estrategia de la organización, adicional su apalancamiento con el resto de los procesos y sistemas de la empresa, sin olvidar los recursos requeridos para su control.

Planificación: La organización tiene que considerar los requisitos, riesgos y oportunidades a tratar durante su implementación y mejora, de aquí se desprende una adecuada gestión de riesgos y velar por los criterios y componentes de seguridad.

Soporte: Este requerimiento suele ser el más olvidado ya que es necesario que la organización determine y proporcione los recursos requeridos para la gestión y mejora del sistema, esto está en paralelo con la planificación y liderazgo luego de realizarse un adecuado presupuesto deberán tenerse presente los riesgos y mecanismos de control a implementar. La competencia del equipo de seguridad de la información o seguridad informática deben ser competentes basándose en su experiencia laboral y educativa.

Operación: La compañía debe planear e implementar los requerimientos requeridos para cumplir con los requisitos del SGSI, esto está encaminado a las acciones preventivas o correctivas que se implementen basado y contemplando los objetivos del sistema.

Evaluación del Desempeño: Se debe realizar una evaluación y monitoreo continuo del sistema, dentro de esta evaluación se debe medir su eficacia y eficiencia, de aquí se desprende la toma de decisión frente a que metodologías escoger e implementar. Este ítem es muy importante ya que se desprende un actor importante para los sistemas de gestión y mejora continua “la auditoria” este ente control y línea de defensa ayudara a la medición del sistema siendo enfático, transparente y bajo un alcance identificado.

Mejora: La mejora continua de cualquier entidad es muy importante de aquí se desprenden los errores o falencias identificadas en auditorías internas o externas; estas no conformidades o acciones correctivas permitirán a la organización a continuar con una mejora continua sin olvidar su estrategia y ayudando a disminuir la probabilidad de que se materialice algún riesgo.

Objetivo del SGSI

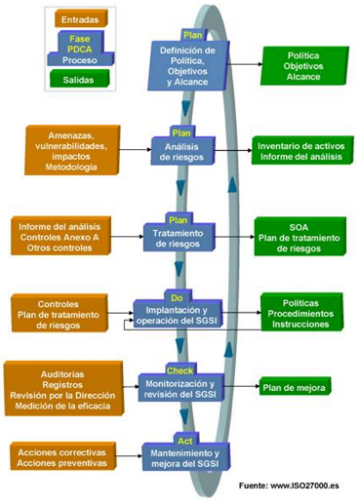
Garantizar y propender la integridad, confidencialidad y disponibilidad, de la seguridad de los sistemas de información y de los datos, definido con base en las directrices y políticas de la Dirección y los requisitos normativos actuales y que son aplicables a la empresa de acuerdo a su necesidad.

Establecer alcance que abarque (procesos involucrados, ubicaciones incluidas, etc.) y de esta forma justificar el SGSI en la empresa.
Todos los activos de información relacionados con las actividades, procesos y áreas de NOSTRADAMUS S.A.S son de mucho valor para la organización, por lo tanto, requiere una protección del uso no adecuado, de su publicación no autorizada, de robo, alteración o destrucción y de futuras amenazas del ciberespacio. Una gestión de seguridad de la información efectiva garantiza que pueda ser compartida, tratada y custodiada mientras se minimiza su exposición al riesgo.

Cualquier que sea la forma que este tome “Física o Digital” o el medio por el cual es almacenada o transferida, está siempre debe ser apropiadamente protegida, con las medidas de control vigente y efectivo.
El modelo de Gestión de Seguridad de la Información “SGSI” definido en NOSTRADAMUS S.A.S , está estructurado y bajo las buenas prácticas de las normas ISO/IEC 27001:2013 Sistema de Gestión de Seguridad de Información: Requerimientos Tecnología de Información Técnicas de Seguridad e ISO/IEC 27002:2013 Código de buenas prácticas para la Gestión de la Seguridad de la Información, cuyo propósito fundamental es garantizar y propender por la integridad, confidencialidad y disponibilidad, de la seguridad de los sistemas de información y de los datos, definido con base en las directrices y políticas de la Dirección y los requisitos normativos.

Figura 5 Componentes del SGSI

Actividades para la implementación del SGSI



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

COMPROMISO DE LA DIRECCIÓN GENERAL

Mantener y mejorar el sistema de gestión de la Seguridad de la Información que garantice el cumplimiento de los objetivos de seguridad requerido para ejecutar los planes y objetivos estratégicos y aumentar la mejora a los procesos y áreas de negocio de NOSTRADAMUS S.A.S

Garantizar y motivar la participación de todos los empleados de NOSTRADAMUS S.A.S, proveedores y socios de negocios en el desarrollo del SGSI.
Mantener un nivel de protección sobre los riesgos que puedan afectar la seguridad de la información que crea, procesa y resguarda la empresa como parte de la debida diligencia de la Dirección.

Proveer los recursos pertinentes para garantizar el debido cuidado de la información que crea, procesa o resguarda la Organización.

ALINEACIÓN POLÍTICA DE GESTION, OBJETIVOS ESTRATEGICOS PARA EL SGSI

Tabla 10 Alineación compromisos específicos de SGSI

COMPROMISOS	OBJETIVO ESTRATEGICO
• Proteger la privacidad de la información de clientes. • Proteger los procesos de creación, procesamiento y resguardo de la información. • Garantizar que el acceso, intercambio o procesamiento de la información por parte de terceros. • Asegurarse que la información esté disponible en el momento que los usuarios la requieran. • Mejorar el costo-eficiencia de los controles de seguridad y su contribución a la rentabilidad del negocio. • Sensibilizar a los usuarios para garantizar la ejecución y cumplir con las políticas de seguridad.	• Contribuir al mejoramiento de la calidad de vida de los clientes y la comunidad • Lograr desarrollo armónico de infraestructura • Consolidar una red de (socios, aliados y proveedores) • Alcanzar la excelencia en la gestión • Generar un crecimiento sólido de los negocios

REVISION POR LA DIRECCION PARA EL SGSI

La GERENCIA general ha establecido los criterios para la evaluación anual del SGSI y seguimientos semestrales, para asegurarse de su conveniencia, alcance y mejora. La dirección para el SGSI la conforma el Comité de Riesgos, Auditoría y Cumplimiento. Los resultados de la Revisión por la dirección contienen las salidas descritas en el modelo ISO 27001 y las decisiones y acciones relacionadas con:

- La mejora de la eficacia del sistema del SGSI.
- La actualización de la evaluación de riesgos y el plan de tratamiento.

Como un elemento constitutivo y de apoyo para todo el Sistema de gestión de seguridad de la información “SGSI”, se ha desarrollado la Declaración de aplicabilidad*. Este documento describe los objetivos de control y los controles pertinentes y aplicables para el SGSI de NOSTRADAMUS S.A.S, y sus responsables

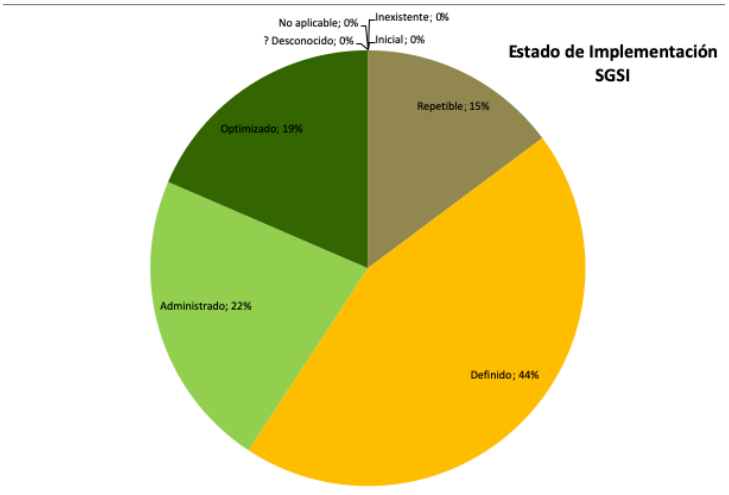
6.GAP

Figura 6 GAP

En la siguiente figura se evidencia el estado de madurez.

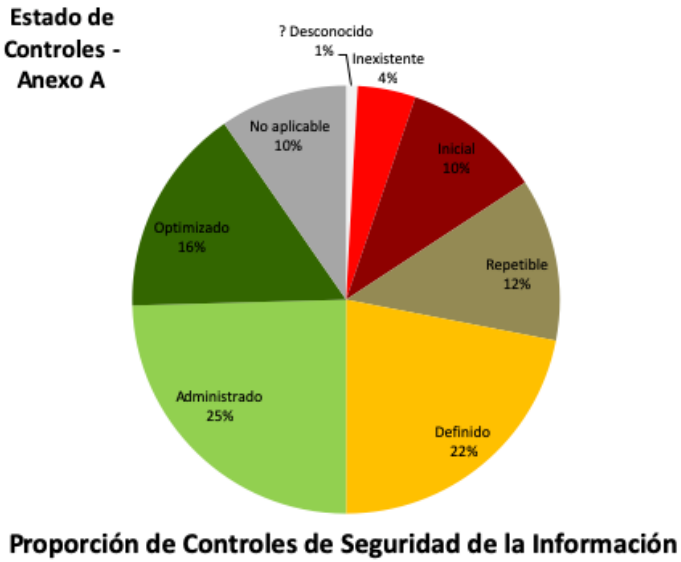
Estado	Significado	Proporción de requerimientos SGSI	Proporción de Controles de Seguridad de la Información
? Desconocido	No ha sido verificado	0%	1%
Inexistente	No se lleva a cabo el control de seguridad en los sistemas de información.	0%	4%
Inicial	Las salvaguardas existen, pero no se gestionan, no existe un proceso formal para realizarlas. Su éxito depende de la buena suerte y de tener personal de la alta calidad.	0%	11%
Repetible	La medida de seguridad se realiza de un modo totalmente informal (con procedimientos propios, informales). La responsabilidad es individual. No hay formación.	15%	12%
Definido	El control se aplica conforme a un procedimiento documentado, pero no ha sido aprobado ni por el Responsable de Seguridad ni el Comité de Dirección.	44%	22%
Administrado	El control se lleva a cabo de acuerdo a un procedimiento documentado, aprobado y formalizado.	22%	25%
Optimizado	El control se aplica de acuerdo a un procedimiento documentado, aprobado y formalizado, y su eficacia se mide periódicamente mediante indicadores.	19%	16%
No aplicable	A fin de certificar un SGSI ,todos los requerimientos principales de ISO/IEC 27001 son obligatorios. De otro modo, pueden ser ignorados por la Administración.	0%	10%
	Total	100%	100%

Fuente: Modelo de madurez de proyectos.



7.SOA

Figura 7 Estado de controles SOA



Fuente: recolección de datos.

Tabla 11 SOA

Tabla SOA se evidencian los controles del anexo A de la ISO 27001:2013 vs el análisis de la entidad NOSTRADAMUS su estado de implementación.

Sección	Controles de Seguridad de la Información	Estado	Comentarios
A5	**Políticas de seguridad de la información**		
A5.1	**Directrices de gestión de la seguridad de la información**		
A5.1.1	Políticas para la seguridad de la información	Administrado	Se cuenta con la Política de Seguridad de la Información, que define un conjunto de políticas de Seguridad de la información aprobadas por la

			dirección. Está política se encuentra publicada en el repositorio de gestión documental definido por la organización.
A5.1.2	Revisión de las políticas para la seguridad de la información	Optimizado	La Política de Seguridad de la Información es revisada de manera periódica para garantizar la conveniencia y de su contenido.
A6	**Organización de la seguridad de la información**		
A6.1	**Organización interna**		
A6.1.1	Roles y responsabilidades en seguridad de la información	Repetible	Los roles del SGSI se encuentran en la matriz RACI en el capítulo de Seguridad de la Información en el Manual Sistema de Gestión la organización. Los roles propios del subproceso de Seguridad de la Información se están documentando en los descriptivos del cargo.
A6.1.2	Segregación de tareas	Inicial	La organización cuenta con un proceso de negocio segmentado por equipos de trabajo,

			se inicia trabajo de segregación
A6.1.3	Contacto con las autoridades	Optimizado	La sede La organización cuenta con un plan de emergencias, el cual detalla los contactos con las diferentes autoridades ver formato de Plan de emergencias - Formato 5 directorio telefónico de emergencias. El contacto con la autoridades de policía es manejado de forma centralizada por el equipo de seguridad física quien a través del establecimiento de un comité evalúa y toma la determinación de contactar a esta entidad, la notificación de temas de seguridad de la información y fraude o delito informático es trabajado coordinadamente con las áreas de Seguridad de la Información y Seguridad Física.
A6.1.4	Contacto con grupos de interés especial	Optimizado	la organización pertenece a los

			grupos especiales: Segurinfo, Gartner, ISACA.
A6.1.5	Seguridad de la información en la gestión de proyectos	Inexistente	
A6.2	**Los dispositivos móviles y el teletrabajo**		
A6.2.1	Política de dispositivos móviles	No aplicable	
A6.2.2	Teletrabajo	No aplicable	
A7	**Seguridad relativa a los recursos humanos**		
A7.1	**Antes del empleo**		
A7.1.1	Investigación de antecedentes	Optimizado	El estudio de seguridad está a cargo de contratistas especializados y será ordenado según los lineamientos del servicio de selección, contemplando, visita domiciliaria, verificación de la historia laboral de los últimos dos años, validación de títulos y desempeño académico, validación de antecedentes disciplinarios, financieros y referenciación de personal.
A7.1.2	Términos y condiciones del empleo	Optimizado	el acuerdo de confidencialidad de colaboradores se

			incluyen las responsabilidades para el tratamiento de los datos personales. Es obligación que cada colaborador conozca, acepte y se comprometa a cumplir con los lineamientos declarados.
A7.2	**Durante el empleo**		
A7.2.1	Responsabilidades de gestión	Administrado	En el Manual Sistema de Gestión la organización se mencionan las responsabilidades y compromisos de la dirección frente a la seguridad de la información.
A7.2.2	Concienciación, educación y capacitación en seguridad de la información	Administrado	la organización cuenta con programas de concienciación y formación en temas de Seguridad de la Información a través de capacitaciones y divulgación de información en medios como: la Intranet, red social corporativa, cursos en temas: seguridad de información, protección de datos personales, riesgos, entre

			otros.
A7.2.3	Proceso disciplinario	Optimizado	Depende del grado de responsabilidad o del impacto de daño que se le pueda hacer a la organización, se analizan los casos y se ejerce la facultad disciplinaria por parte de la organización; de acuerdo con el procedimiento de talento humano.
A7.3	**Finalización del empleo o cambio en el puesto de trabajo**		
A7.3.1	Responsabilidades ante la finalización o cambio	Optimizado	En el formato de Acuerdo de Confidencialidad Colaboradores, se mencionan las obligaciones de los empleados ante la desvinculación relacionadas con la entrega de información o medios de almacenamiento que posean, no retener copias, extractos o cualquier otro tipo de reproducción, total o parcial, de la información confidencial.
A8	**Gestión de activos**		
A8.1	**Responsabilidad sobre los activos**		
A8.1.1	Inventario de activos	Administrado	Los activos de

			información identificados se encuentran documentados en la herramienta organizacional bajo los lineamientos definidos en el procedimiento de Inventario Activos de Información.
A8.1.2	Propiedad de los activos	Administrado	Los activos de información identificados se encuentran documentados en la herramienta organizacional bajo los lineamientos definidos en el procedimiento de Inventario Activos de Información.
A8.1.3	Uso aceptable de los activos	Definido	la organización tiene la Política de Seguridad de la Información, que habla sobre el uso adecuado de los activos de información.
A8.1.4	Devolución de activos	Repetible	Dentro del procedimiento, de Desvinculación de Colaboradores, el empleado debe gestionar el Paz y Salvo de Retiro para dejar constancia de su desvinculación de la organización y la entrega de activos, ausencia de

			control efectivo, se retiran colaboradores sin paz y salvo
A8.2	**Clasificación de la información**		
A8.2.1	Clasificación de la información	Administrado	Se tiene definido el Estándar de Clasificación de la información y Datos, en el cual se definen las directrices para generar la clasificación de la información.
A8.2.2	Etiquetado de la información	Repetible	Las directrices de clasificación y las formas de etiquetado de la información se encuentran documentados en el Estándar de Clasificación de la información y Datos, falta software o ayuda automática para su etiquetado
A8.2.3	Manipulado de la información	Definido	De acuerdo a los lineamientos definidos en el procedimiento de Inventario Activos de Información, los activos de información son ingresados en la herramienta colaborativa, desde allí se revisan y actualizan los

			activos del proceso.
A8.3	**Manipulación de los soportes**		
A8.3.1	Gestión de soportes extraíbles	Optimizado	En la Política de Seguridad de la Información, se tiene el capítulo de uso de controles criptográficos. Adicional, existe el Formato de Autorización del uso de dispositivos para solicitar la autorización del uso de memorias USB o medios de almacenamiento.
A8.3.2	Eliminación de soportes	Optimizado	Se cuenta con un proveedor externo para la destrucción de medios, los seguimientos son generados por el proceso de Tecnología.
A8.3.3	Soportes físicos en tránsito	Repetible	
A9	**Control de acceso**		
A9.1	**Requisitos de negocio para el control de acceso**		
A9.1.1	Política de control de acceso	Definido	En la Política de Seguridad de la Información, se establecen los lineamientos frente al control de acceso lógico y la gestión del control de acceso físico se encuentra a cargo del proceso de

			Seguridad Física.
A9.1.2	Acceso a las redes y a los servicios de red	Repetible	En la Política de Seguridad de la Información personales, se tienen documentados los capítulos relacionados con directrices de uso de los servicios de red: internet, red interna, intranet, correo electrónico.
A9.2	**Gestión de acceso de usuario**		
A9.2.1	Registro y baja de usuario	Inicial	Gestión de identidad es el encargado de la asignación y mantenimiento de los derechos de acceso a usuarios. se cuenta con los siguientes documentos de apoyo:
A9.2.2	Provisión de acceso de usuario	Inicial	Gestión de Identidad o el proceso de TI son quienes crean los usuarios en el directorio activo, tomando como base la matriz de perfilamiento de accesos, la autorización del jefe inmediato o seguridad de la información.
A9.2.3	Gestión de privilegios de acceso	Inicial	Los privilegios de acceso son administrados

			desde Gestión de Identidad de acuerdo a lo documentado en el Estándar de Administración de usuarios.
A9.2.4	Gestión de la información secreta de autenticación de los usuarios	Optimizado	se definen los lineamientos contemplados para la estructura y administración de contraseñas en los sistemas de información.
A9.2.5	Revisión de los derechos de acceso de usuario	Repetible	Gestión de identidad de manera periódica la revisión e inactivación de acceso de los colaboradores retirados, y se realiza eliminación de las cuentas del directorio activo con más de 3 meses de inactividad de acuerdo a los lineamientos definidos, se evidencia que el control es manual y es necesario automatizar e implementar un monitoreo no se cumple a cabalidad.
A9.2.6	Retirada o reasignación de los derechos de acceso	Definido	El grupo de Gestión de Identidad se encarga de retirar

			los accesos del personal retirado.
A9.3	**Responsabilidades del usuario**		
A9.3.1	Uso de la información secreta de autenticación	Optimizado	En la Política de Seguridad de la Información, Autogestión y Parámetros de Contraseñas se establecen los lineamientos para la creación y mantenimiento de contraseñas seguras, se definen los lineamientos contemplados para la estructura y administración de contraseñas en los sistemas de información.
A9.4	**Control de acceso a sistemas y aplicaciones**		
A9.4.1	Restricción del acceso a la información	Definido	Los accesos y los permisos en las aplicaciones son manejados por Gestión de Identidad, cada proceso tiene a disposición un recurso de almacenamiento para los documentos del mismo proceso.
A9.4.2	Procedimientos seguros de inicio de sesión	Administrado	En la Política de Seguridad de la Información, Autogestión y

			Parámetros de Contraseñas se establecen los lineamientos para la creación y mantenimiento de contraseñas seguras.
A9.4.3	Sistema de gestión de contraseñas	Administrado	En la Política de Seguridad de la Información, Autogestión y Parámetros de Contraseñas se establecen los lineamientos para la creación y mantenimiento de contraseñas seguras.
A9.4.4	Uso de utilidades con privilegios del sistema	Inicial	En la Política de Seguridad de la Información, se hace referencia a la utilización del software en la organización está basado en las leyes de derechos de autor
A9.4.5	Control de acceso al código fuente de los programas	Inicial	En la organización el proceso de administración de la configuración es el encargado de gestionar el control de acceso a código fuente.
A10	**Criptografía**		
A10.1	**Controles criptográficos**		
A10.1.1	Política de uso de los controles criptográficos	Optimizado	Los lineamientos de cifrado de datos se encuentran

			definidos en la Política de Seguridad de la Información en el numeral de controles criptográficos y contempla que sea aplicada para aquella información que sea clasificada como confidencial. Adicional, se cuenta con el estándar de Criptografía, en el cual se definen los lineamientos para la administración y uso de llaves criptográficas en la organización.
A10.1.2	Gestión de claves	Optimizado	la organización cuenta con una solución de criptografía que permite guardar y controlar las llaves desde un repositorio central, esta solución es administrada por el grupo de seguridad informática del proceso de operaciones de tecnología. El manejo y administración de los certificados digitales es realizado por el mismo grupo de

			seguridad informática. Las directrices sobre el manejo de las llaves criptográficas se encuentra Política de Seguridad de la Información, adicional se tiene definido el estándar de criptografía.
A11	**Seguridad física y del entorno**		
A11.1	**Áreas seguras**		
A11.1.1	Perímetro de seguridad física	Optimizado	Se cuenta con el Instructivo para el ingreso a las instalaciones de la organización. La organización cuenta con monitoreo remoto de las 10 cámaras CCTV dispuesta en todo el edificio. Adicionalmente se cuenta con los siguientes controles: Servicio de Guía Canino, Patrullajes Policía Nacional. Cámara de vigilancia externa la cual tiene cobertura sobre el frente del edificio (Plazoleta Principal), cámara de vigilancia al ingreso de las instalaciones

			(única opción de ingreso y salida del edificio) y son monitoreadas las 24 horas del día, desde la consola de seguridad ubicada en la sede principal.
A11.1.2	Controles físicos de entrada	Optimizado	Se cuenta con Instructivo para el ingreso a las instalaciones de la organización. Según el plan de vigilancia dispuesto, se tienen los siguientes controles: -Inspección física mediante la verificación de Bolsos, maletas, bolsas, etc, por vigilancia humana. -Registro de visitantes en el libro dispuesto por la vigilancia, al ingreso de las instalaciones a través del documento de identidad del mismo. -Verificación del número de requerimiento para ingreso de contratistas a laborar a las instalaciones. -Revistas

			vigilancia humana (recorredor). -Control del porte del carné de identificación institucional (identificación a la vista). -Para el personal visitante, se han dispuesto de 30 tarjetas con cordón institucional, las cuales se entregan al momento de ingreso del visitante y debe ser devuelta en el momento de su retiro. -El vigilante del ingreso peatonal cuenta con un sistema de alarma (botón de pánico) con conexión a la consola de seguridad, el cual permite reportar situaciones y que por situaciones de intimidación le impidan utilizar los medios de comunicación establecidos (Avantel, celular, etc).
A11.1.3	Seguridad de oficinas, despachos y recursos	Administrado	la organización tiene definido el procedimiento Solicitud de Carne, Tarjeta-Carne y Administración de

			Accesos establece como se controla el acceso a las oficinas de la organización mediante el uso de tarjeta de control de acceso para así restringir el acceso no autorizado.
A11.1.4	Protección contra las amenazas externas y ambientales	Definido	Adicional a los planes de emergencias, se tienen implementadas una serie de controles como: Los sistemas de extinción, provisión de extintores de incendios, planes de evacuación, alertas para evacuación, monitoreo de las cámaras de seguridad y se generan ejercicios prácticos de simulacro de evacuación una vez al año, entre otros. La organización ha dispuesto para la atención de emergencias al Sistema Comando de Incidentes .
A11.1.5	El trabajo en áreas seguras	Administrado	El acceso a las instalaciones de La organización es restringido desde la recepción y

			cuando un visitante ingresa a las instalaciones, siempre debe estar acompañado por el colaborador responsable de la atención del visitante hasta el momento de su retiro. Se manejan tarjetas de proximidad para el control de acceso. Este lugar cuenta con cámaras de vigilancia las cuales son monitoreadas las 24 horas del día desde la consola de seguridad de la sede principal.
A11.1.6	Áreas de carga y descarga	? Desconocido	
A11.2	**Seguridad de los equipos**		
A11.2.1	Emplazamiento y protección de equipos	Inicial	El retiro de equipos se realiza previo requerimiento y llega una solicitud de traslado autorizada por el líder o autorizador designado del proceso, cuando el activo va a ser retirado el vigilante debe reportar a la consola, donde se validara si el equipo tiene la respectiva autorización.

A11.2.2	Instalaciones de suministro	Inicial	Relativo al soporte eléctrico: El edificio cuenta con planta eléctrica y se realizan rutinas periódicas de mantenimiento para garantizar su adecuada operación, estas rutinas periódicas no están siendo revisadas por auditoria, se identifica brecha
A11.2.3	Seguridad del cableado	Inicial	Los centros de cableado son terminados en rack o gabinetes que son con acceso restringido, con llave manejada por el guarda de seguridad. Falencias en el control de acceso
A11.2.4	Mantenimiento de los equipos	Definido	Existe un cronograma establecido para llevar a cabo el mantenimiento preventivo de equipos de Cómputo.
A11.2.5	Retirada de materiales propiedad de la empresa	Repetible	El retiro de equipos se realiza previo requerimiento a través del aplicativo y debe llegar una solicitud de traslado autorizada por el líder o autorizador designado del

			proceso, cuando el activo va a ser retirado el vigilante debe reportar .
A11.2.6	Seguridad de los equipos fuera de las instalaciones	Inexistente	
A11.2.7	Reutilización o eliminación segura de equipos	Repetible	Los equipos que van a ser dados de baja por fin de vida útil o devolución al Leasing ingresan a bodega de TI en donde se realiza procedimiento de Borrado seguro sobre los medios con la herramienta FS2A suministrada por el prestador de servicios y avalada por seguridad de la información.
A11.2.8	Equipo de usuario desatendido	Optimizado	Seguridad para el Desarrollo de Aplicaciones, se definen los parámetros de bloqueo automático (3 minutos de inactividad), adicional, se han realizado campañas de sensibilización en grupos primarios, intranet, cursos prisma, entre otros.
A11.2.9	Política de puesto de trabajo despejado y pantalla limpia	Administrado	En la Política de Seguridad de la información, Escritorios y pantallas limpias,

			se definen éstos lineamientos. Adicional, se han realizado campañas de sensibilización en grupos primarios, intranet, cursos prisma, entre otros, frente al conocimiento de ésta política.
A12	**Seguridad de las operaciones**		
A12.1	**Procedimientos y responsabilidades operacionales**		
A12.1.1	Documentación de procedimientos operacionales	No aplicable	
A12.1.2	Gestión de cambios	No aplicable	
A12.1.3	Gestión de capacidades	No aplicable	
A12.1.4	Separación de los recursos de desarrollo, prueba y operación	No aplicable	
A12.2	**Protección contra el software malicioso (malware)**		
A12.2.1	Controles contra el código malicioso	Definido	La solución de FW adquirida por la organización permite la búsqueda de código malicioso y amenazas de nueva generación, haciendo una inspección más elaborada para detectar software malicioso, adicional, la organización tiene

			un sistema de antivirus para todos los equipos y servidores;
A12.3	**Copias de seguridad**		
A12.3.1	Copias de seguridad de la información	Repetible	la organización tiene contratado con un tercero los servicios de Backup y restauración, los cuales se realizan bajo una programación que se acuerda con el proveedor para garantizar que se realicen las actividades de backup.
A12.4	**Registros y supervisión**		
A12.4.1	Registro de eventos	Inexistente	
A12.4.2	Protección de la información del registro	Inicial	En la organización los logs son respaldados dentro de las rutinas periódicas de backups de los sistemas y cuando sean requeridos se deben solicitar bajo el procedimiento definido por el grupo de operaciones de tecnología.
A12.4.3	Registros de administración y operación	Definido	Se tiene implementado un procedimiento de gestión de LOGs, en el cual la responsabilidad de la revisión de las

			actividades realizadas por el administrador y los operadores está en cabeza del CISO
A12.4.4	Sincronización del reloj	Optimizado	La sincronización es tomada de la SIC- Superintendencia de Industria y Comercio - adicional Procesamiento de Datos (la organización) realiza monitoreo semanal, confrontando el margen del tiempo, no mayor a 3 segundos.
A12.5	**Control del software en explotación**		
A12.5.1	Instalación del software en explotación	Definido	Por medio de la existencia de la herramienta de antivirus existe un control de descargas de software no reconocido. En la Política de Seguridad de la Información, se hace referencia a la Instalación y Uso de Software.
A12.6	**Gestión de la vulnerabilidad técnica**		
A12.6.1	Gestión de las vulnerabilidades técnicas	Inexistente	
A12.6.2	Restricción en la instalación de software	Definido	En la Política de Seguridad de la

			Información, Instalación y uso de Software se establece que los usuarios no podrán realizar ninguna instalación de software en los equipos de la organización, tecnología y seguridad de la información son los únicos facultados para dar autorizaciones.
A12.7	**Consideraciones sobre la auditoria de sistemas de información**		
A12.7.1	Controles de auditoría de sistemas de información	Definido	Las auditorías llevadas a cabo al interior con los lineamientos definidos en el procedimiento de auditorías internas. Para la ejecución de auditorías a los sistemas de información se revisa el plan de auditoría y se acuerda con los líderes de los diferentes procesos las fechas y horarios, los accesos requeridos y ambientes en los cuales se realizarán las pruebas.

A13	**Seguridad de las comunicaciones**		
A13.1	**Gestión de la seguridad de las redes**		
A13.1.1	Controles de red	Definido	Las sedes cuentan con segmentación propia manejada por switches (VLANS L3) y para el caso del centro de cómputo se manejan VLANS con switches, el enrutamiento y las políticas de control de acceso entre ellas es realizado por el FW.
A13.1.2	Seguridad de los servicios de red	Definido	La red es monitoreada, el acceso a la red es controlado a través de la herramienta CISCO Los equipos activos L3 realizan el control y los permisos de tráfico a través de ACLs. Otras capas de servicios de red, se protegen a través del Firewall, Directorio Activo y Antivirus.
A13.1.3	Segregación en redes	Definido	Las sedes cuentan con segmentación propia manejada por switches (VLANS L3) y para el caso del centro de cómputo se manejan VLANS

			con switches pero el enrutamiento entre ellas es realizado por el FW.
A13.2	**Intercambio de información**		
A13.2.1	Políticas y procedimientos de intercambio de información	Administrado	En la Política de Seguridad de la Información. Transferencia de Información, se hace referencia a los controles a ser aplicados en la transferencia de información, adicional el nivel de clasificación de la información que se va a enviar. En el acuerdo de confidencialidad se menciona que la información de la organización es de tipo confidencial y por lo tanto el empleado se obliga a no copiarla, distribuirla, reproducirla, revelarla o transmitirla.
A13.2.2	Acuerdos de intercambio de información	Administrado	Se tienen acuerdos de envío de información con los diferentes bancos, siguiendo lineamientos definidos por estos para garantizar la transferencia

			segura de información.
A13.2.3	Mensajería electrónica	Administrado	El servicio de mensajería está contratado con un tercero (Microsoft) quien mediante un contrato de servicios garantiza la seguridad y disponibilidad del correo.
A13.2.4	Acuerdos de confidencialidad o no revelación	Administrado	El departamento de compras maneja los acuerdos de confidencialidad que son informados y aceptados por los proveedores y estos hacen a su vez parte del contrato establecido entre las partes. En los contratos son mandatarias las cláusulas de confidencialidad y el anexo de riesgos. Talento Humano maneja los acuerdos de confidencialidad que pertenecen a los colaboradores de la organización, este acuerdo es firmado por el colaborador cuando ingresa a la empresa.

A14	**Adquisición, desarrollo y mantenimiento de los sistemas de información**		
A14.1	**Requisitos de seguridad en los sistemas de información**		
A14.1.1	Análisis de requisitos y especificaciones de seguridad de la información	Administrado	la organización cuenta con el Estándar de Seguridad para el desarrollo de APPS donde se encuentran los requisitos de seguridad para la autenticación, contraseñas, cifrado, aplicaciones, Exige el uso de certificados digitales, considera algunos lineamientos de la ley de protección de datos personales, Controles de aplicación y procedimiento, en este último se mencionan los aspectos de seguridad que se deben cumplir en relación al Anexo A de ISO/IEC 27001.
A14.1.2	Asegurar los servicios de aplicaciones en redes públicas	Administrado	Se cuenta con certificados digitales para exposición de los

			sitios públicos y reglas a través de firewall, donde se controla el acceso de una manera más específica a los usuarios. Para el acceso a usuarios del sitio admin, se tienen dispuestos certificados digitales y reglas de firewall limitadas a usuarios de la redes de la organización.
A14.1.3	Protección de las transacciones de servicios de aplicaciones	Administrado	Se utiliza un esquema de cifrado por medio de tokens, PKI y ftps, para evitar los riesgos de interceptación y manipulación con las diferentes entidades bancarias para las transacciones de información confidencial, para ello se cuenta con autenticación secreta de usuarios.
A14.2	**Seguridad en el desarrollo y en los procesos de soporte**		
A14.2.1	Política de desarrollo seguro	Administrado	la organización cuenta con el Estándar de Seguridad para el desarrollo de

			APPS, en donde se encuentran los requisitos de seguridad para la autenticación, contraseñas, cifrado, aplicaciones, Exige el uso de certificados digitales, considera algunos lineamientos de la ley de protección de datos personales, Controles de aplicación y procedimiento, en este último se mencionan los aspectos de seguridad que se deben cumplir en relación al Anexo A de ISO/IEC 27001.
A14.2.2	Procedimiento de control de cambios en sistemas	Definido	A través de su procedimiento de gestión de cambios vela por los cambios requeridos en cada uno de los servidores y aplicaciones donde se encuentran los servicios.
A14.2.3	Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo	Administrado	Se tiene definido el procedimiento de gestión de cambios, en el cual se incluye la ejecución de pruebas a la

			versión previa a la instalación de la misma en el ambiente de producción.
A14.2.4	Restricciones a los cambios en los paquetes de software	Administrado	Se tiene implementado una política de desarrollo, donde se definen los roles que existen en el área de desarrollo con sus responsabilidades y así mismo restricciones.
A14.2.5	Principios de ingeniería de sistemas seguros	Administrado	Se tiene políticas de desarrollo seguro para garantizar la seguridad durante el proceso de diseño y desarrollo de aplicaciones, se deben seguir las recomendaciones, mejores prácticas y patrones de diseños señalados en el instructivo .
A14.2.6	Entorno de desarrollo seguro	Administrado	Se cuenta con diferentes ambientes para desarrollo, pruebas y producción, así como controles de acceso a los mismos por medio de la asignación de permisos por parte de los líderes de área, igualmente se tiene establecido que

			para el acceso a los diferentes ambientes y plataformas se debe realizar por medio de autenticación con usuario y contraseña.
A14.2.7	Externalización del desarrollo de software	Administrado	El proceso parte del negocio quien expone la necesidad diligenciando un formato SRQ para solicitudes puntuales y ficha de iniciativa para solicitudes nuevas.
A14.2.8	Pruebas funcionales de seguridad de sistemas	Administrado	Se tiene implementado Script de pruebas, en el cual se validan pruebas de seguridad correspondientes a verificación de cifrado de contraseñas, conexión segura mediante protocolo https y ejecución correcta de cambios de contraseñas.
A14.2.9	Pruebas de aceptación de sistemas	Administrado	Se encuentran documentadas a través del procedimiento de gestión de cambios y producto no conforme. Se cuenta con ambiente de

			pruebas en el cual se ejecutan las pruebas funcionales y de seguridad a las versiones, antes de ser instaladas en producción.
A14.3	**Datos de prueba**		
A14.3.1	Protección de los datos de prueba	Definido	El ambiente de pruebas está totalmente separado del ambiente de producción, y los datos que se manejan en el ambiente de pruebas no son reales.
A15	**Relación con proveedores**		
A15.1	**Seguridad en las relaciones con proveedores**		
A15.1.1	Política de seguridad de la información en las relaciones con los proveedores	No aplicable	
A15.1.2	Requisitos de seguridad en contratos con terceros	No aplicable	
A15.1.3	Cadena de suministro de tecnología de la información y de las comunicaciones	No aplicable	
A15.2	**Gestión de la provisión de servicios del proveedor**		
A15.2.1	Control y revisión de la provisión de servicios del proveedor	No aplicable	
A15.2.2	Gestión de cambios en	No aplicable	

	la provisión del servicio del proveedor		
A16	**Gestión de incidentes de seguridad de la información**		
A16.1	**Gestión de incidentes de seguridad de la información y mejoras**		
A16.1.1	Responsabilidades y procedimientos	Repetible	Se tiene definido el Procedimiento de Gestión de Incidentes de Seguridad de la Información en el cual se definen las responsabilidades,.
A16.1.2	Notificación de los eventos de seguridad de la información	Repetible	Dentro de los lineamientos para reportar los incidentes de seguridad de la información, existen los siguientes canales s: - Herramienta de gestión de solicitudes - Correo electrónico. Una vez reportado se procede con la creación de incidente de seguridad de la información para continuar con la gestión y seguimiento del caso, el cual es realizado por el equipo de respuesta a

			incidentes de Seguridad de la Información.
A16.1.3	Notificación de puntos débiles de la seguridad	Repetible	El modelo definido contempla el registro y reporte de eventos, incidentes y vulnerabilidades de seguridad de la información, se pretende que los procesos de negocios reporten cualquier situación presentada sin que tengan que establecer si es un evento, incidente o vulnerabilidad.
A16.1.4	Evaluación y decisión sobre los eventos de seguridad de información	Repetible	
A16.1.5	Respuesta a incidentes de seguridad de la información	Repetible	Se crea un grupo de respuesta de incidentes, quienes realizan el respectivo análisis apoyándose con el colaborador de la organización quien genera el incidente y el equipo de gestión a fin de determinar que sucedió y que se afectó, generando la correspondiente gestión y documentación de todas las acciones realizadas en el respectivo registro.

A16.1.6	Aprendizaje de los incidentes de seguridad de la información	Inicial	Una vez se gestiona y analiza el incidente entre seguridad de la información junto con las partes interesadas, se identifican las causas que lo originaron y se determinan las acciones que permiten reducir la posibilidad o el impacto de incidentes futuros.
A16.1.7	Recopilación de evidencias	Inexistente	
A17	**Aspectos de seguridad de la información para la gestión de la continuidad de negocio**		
A17.1	**Continuidad de la seguridad de la información**		
A17.1.1	Planificación de la continuidad de la seguridad de la información	Definido	Se tiene definido el estándar de requerimientos de Seguridad de la Información para Continuidad de Negocio, en el cual se definen los lineamientos de seguridad que se deben contemplar y que deben estar operativos ante una situación adversa dentro de continuidad de negocio.

A17.1.2	Implementar la continuidad de la seguridad de la información	Definido	Se tiene definido el estándar de requerimientos de Seguridad de la Información para Continuidad de Negocio, en el cual se definen los lineamientos de seguridad que se deben contemplar y que deben estar operativos ante una situación adversa dentro de continuidad de negocio.
A17.1.3	Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Definido	Se tiene definido el estándar de requerimientos de Seguridad de la Información para Continuidad de Negocio, en el cual se definen los lineamientos de seguridad que se deben contemplar y que deben estar operativos ante una situación adversa dentro de continuidad de negocio.
A17.2	**Redundancias**		
A17.2.1	Disponibilidad de los recursos de tratamiento de la información	Optimizado	La plataforma tecnológica de la organización se encuentra alojada en dos centros de procesamiento de datos "CPDs",
A18	**Cumplimiento**		
A18.1	**Cumplimiento de los**		

	requisitos legales y contractuales		
A18.1.1	Identificación de la legislación aplicable y de los requisitos contractuales	Definido	El área de jurídica de la organización, realiza actualización normativa de acuerdo con lo señalado por el Instructivo, es así que se remite la información que se considera relevante para los proceso por medio de correo electrónico dirigido a Directores, lideres.
A18.1.2	Derechos de Propiedad Intelectual (DPI)	Definido	En la política Seguridad de la Información, se tiene el capítulo de Uso de Internet e Instalación y uso de software.
A18.1.3	Protección de los registros de la organización	Definido	El proceso de gestión documental es el encargado de administrar las tablas de retención documental; estas tablas son construidas con los diferentes procesos de la organización. Esta tabla menciona entre otras cosas el tiempo de retención de la documentación para cumplir con

			las prácticas de conservación, custodia y disposición de la información.
A18.1.4	Protección y privacidad de la información de carácter personal	Definido	En la Política de Seguridad de la Información se tiene el capítulo de protección de datos personales.
A18.1.5	Regulación de los controles criptográficos	Administrado	Se tiene definida una política para el uso de controles criptográficos, donde se tienen los siguientes lineamientos: - El área de operaciones consulta la información solicitada, esta es encriptada utilizando el algoritmo de encriptación AES-256 y una contraseña que cumple con la política de contraseñas a través de la aplicación 7Zip. - La información encriptada debe enviarse en un medio magnético, cifrada y protegida por contraseña. Para el intercambio de información con las diferentes entidades

			bancarias, se cuenta con tokens y PKI's que garantizan la identificación plena de los usuarios, así como la integridad y confidencialidad de la información, los cuales están soportados por convenio administrativo con los bancos aplicando la normatividad vigente. - Se cuenta con una política de gestión de llaves criptográficas en la cual se define su uso, protección, retiro y tiempo de vida.
A18.2	**Revisiones de la seguridad de la información**		
A18.2.1	Revisión independiente de la seguridad de la información	Administrado	Auditoria realiza auditorías periódicas a la plataforma tecnológica de la organización, con el objetivo de validar el cumplimiento de los requisitos, de acuerdo a los lineamientos definidos en la política de declaración de auditoria y el

			procedimiento de Auditorías Internas del Sistemas de Gestión.
A18.2.2	Cumplimiento de las políticas y normas de seguridad	Definido	En las auditorías internas se realiza la verificación de cumplimiento de las políticas y las directrices de seguridad de la información, esto hace parte de los criterios de auditoría.
A18.2.3	Comprobación del cumplimiento técnico	Inicial	

8.EJECUCION DE LOS ATAQUES

Teniendo presente lo ocurrido a la empresa NOSTRADAMUS S.A.S; se ha solicitado a la empresa Zero Day, recrear los ataques informáticos con el fin de poder establecer las causas que originaron los incidentes. Para esto se le ha designado como parte del equipo de pruebas de penetración con el fin de dar inicio al proceso de simulación de los escenarios presentados y para que presente a las Directivas de Nostradamus S.A.S.

Ejecución de cada uno de los ataques: presentar un video donde se realice cada una de las simulaciones utilizando laboratorios controlados a partir de máquinas virtuales y el uso de sistemas operativos de auditorías como Kali Linux.

1. Ataque a sistemas operativos Windows 7 a través de navegadores web haciendo uso de técnicas de ingeniería social con metasploit.
   URL VIDEO: https://youtu.be/AEMROjTeE2U

2. Acceso indebido, Ataque de elevación de privilegios y robo de información a sistemas operativos Windows, dejando huella del uso de un exe denominado lazange
   URL VIDEO: https://youtu.be/-j8yrpqqFXQ

3. 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)

URL VIDEO: https://youtu.be/CLlnaR1w1U0

4. 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
   URL VIDEO: https://youtu.be/xTpb7kZ6xtA

5. El Sitio web de NOSTRADAMUS S.A.S fue vulnerado posiblemente con un ataque de inyección de sql. Para para esta simulación Ud. 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
   URL VIDEO: https://youtu.be/CezI49IJfyI

9.PROPUESTA DE ASEGURAMIENTO

Como estrategia para realizar un seguimiento al tráfico de red, se presentan dos propuestas para la implementación de un administrador unificado de amenazas (UTM de código abierto) que permita realizar:

• Prevención de intrusiones en línea
• Medir el tráfico de la red
• Monitorear de flujo de red
• Que incorpore un sistema de detección de intrusiones (IDS)

Se presentan dos opciones de administradores unificado de amenazas “PfSense y Untangle.

9.1 CUADRO COMPARATIVO

realizando un cuadro comparativo, mostrando sus ventajas y desventajas, sus Características e indicar cual sería el apropiado para su implantación.

Tabla 12 UTM

pfSense		Untangle	
Ventajas	Desventajas	Ventajas	Desventajas
Un factor importante que no se puede ignorar es que se necesita contenido actualizado para que un dispositivo UTM haga su trabajo. Sin actualizaciones periódicas de las reglas de	• La última versión estable de la aplicación pfsense 24 de septiembre	Dentro de las ventajas Que posee esta propuesta Recae en la facilidad de Implementación y	•El software cuenta Con diversas aplicaciones Para la protección de ataques, pero no cuenta con mecanismos

IDS, listas de hosts y firmas de malware, la gestión de amenazas no es mejor que un firewall. • La propuesta de valor de pfSense es significativa. Es gratuito, abierto y no se necesitan suscripciones costosas para proteger la red. • Instalación en cualquier equipo “Desktop o servidor” • Requerimientos mínimos de software. • No se requiere tener conocimientos de Unix para su instalación. • Gestor de paquetes que le permite incluir o retirar módulos de herramientas como Snort, IMSpector, Squid.	de 2018 (1 año y 10 días). • Se requieren constantes actualizacion es periódicas - patchwork • Soporte y asistencia limitada en el mercado. • Tener conocimient os técnicos al instalar o usar módulos de terceros “Snort, IMSpector, Squid etc..” • Ausencia de documentaci ón técnica.	Configuración del software. •utiliza programas de software Abierto. • bajos requisitos de Hardware • permite de manera inmediata La protección a diversas Amenazas que atentan A la red. • sistema implementado en Forma modular que permita La activación o desactivación De niveles de seguridad a Gusto de la empresa. •	Para eliminar amenazas ya existentes • la herramienta está orientada A ejecutar mecanismos de protección, así que esta Limitado en términos Operacionales •se requiere usar un software adicional para eliminar amenazas que ya posea la red. • esta herramienta cuenta con aplicaciones de uso libre y código abierto Sin embargo, existen Aplicaciones extra que Requieren de pago
• Cortafuegos: Filtrado de IP / puerto, conexiones limitantes, capacidad de capa 2, depuración. • State table: De forma predeterminada, todas las reglas tienen estado, hay varias configuraciones disponibles para el manejo del estado, permite administración con segregación de funciones por perfiles. • Balanceador de carga: LB incorporado para distribuir la carga entre varios		No requiere de la instalación De un sistema operativo Operacional adicional Donde se aloje Ya que este cuenta con una Distribución de debian. •contiene una gran cantidad De equipos compatibles. •costos bajos para	Ya que las aplicaciones Que añaden protección extra son de pago se transforma en un impedimento para entornos de red complejos y grandes.

servidores. • NAT: Reenvío de puertos. • HA (alta disponibilidad): activa el secundario si falla el primario. • Multi-WAN (Wide Area network): Permite usar más de una conexión de internet. • VPN (red privada virtual): Admite IPsec y OpenVPN. • Informes: Plantillas personalizadas y permite guardar históricos. • Monitoreo: Monitoreo en tiempo real • DNS dinámico: Se incluyen varios clientes DNS • DHCP: Se incluye el servidor DHCP • Relay: Se incluye el Relay. • Portal Cautivo: Contiene la funcionalidad de desplegar un portal cautivo. Untangle		la implementación	

• Dentro de las ventajas que posee esta propuesta recae en la facilidad de implementación y configuración del software, adicionalmente de utilizar programas de código abierto y de bajos requisitos de hardware. • Permite de manera inmediata la protección a diversas amenazas que atenten a la misma. • Un sistema implementado de forma modular que permitirá la activación o desactivación de niveles de seguridad a gusto de las exigencias de la empresa. • No requiere de la instalación de un sistema operativo adicional donde se alojará ya que este viene montado en una distribución de debian Linux. • Contiene una gran cantidad de equipos compatibles para el uso del mismo y sus requisitos son bajos que son óptimos en sistemas de bajo consumo energético. • Costos bajos para la implementación del mismo.			

El UTM más apropiado para implementar en NOSTRADAMUS ES: PfSense

10.SIMULACION UTM

A partir del seleccionado realice una simulación en un laboratorio controlado (máquina virtual), configurando las políticas que usted como futuro especialista considere necesarias y pertinentes para reducir el riesgo.

Video: https://www.youtube.com/watch?v=Aa-oUfsl234

Instalación:

Se procede a descargar la última versión disponible en el sitio: https://www.pfsense.org/download/ se debe seleccionar la arquitectura e instalador, para este proyecto será utilizado un servidor virtual y utilizaremos una imagen AMD64bits y formato ISO para su descarga.

Se procede a crear la máquina virtual en el entorno virtual vmware o virtualbox.

En los requerimientos de la maquina dejamos 1 gb de ram y se crea un disco duro virtual con espacio reservado dinámicamente.

Es importante parametrizar y tener listas las interfaces de red según la topología de la red.

Políticas:

1. Alta disponibilidad de la solución “primario y master”.
2. VPNs
3. Traffic Shaper
4. Instalación y configuración de los paquetes Squid
5. Proxy server
6. DHCP
7. DMZ

El siguiente texto corresponde a la guía de instalación de pfsense , se recomienda ver el video a la par de que se realiza la lectura de la guía, muchas gracias.

“El sistema pfsense es un sistema de la familia BSD , damos click en esta opción y continuación seleccionaremos la versión FreeBSD de 64 que corresponde a la arquitectura de este equipo en particular, damos click en siguiente , seleccionaremos la memoria ram que deseemos , y damos click en siguiente. Creamos un disco virtual con el espacio que deseemos y finalizamos dando click en crear. un vez creado la máquina virtual buscamos la opción de “configuración” y damos click en ella, aquí se nos abrirá un menú, buscamos la sección de red , y crearemos inicialmente 3 redes , una que configuraremos en modo puente y la nombramos como deseemos , la segunda como red interna que esta será nuestra red lan le colocamos un nombre y una tercera para establecer una posible configuración con DMZ , una realizada la configuración de las redes, añadiremos la imagen ISO del sistema pfsense para ello accedemos a la opción “almacenamiento” y buscamos nuestra imagen dentro de nuestro directorio . iniciamos la máquina virtual aquí se iniciara el proceso de instalación, una vez

finalizado oprimimos aceptar, buscamos la distribución de teclado latinoamericano y continuamos, esperamos que termine la instalación una vez finalizada se nos mostrara un mensaje indicándonos que acabo la instalación , en este menú damos en NO , le amos en reiniciar y extraemos la unidad virtual, ahora iniciara directamente el sistema operativo. Esperamos que cargue los módulos necesarios para el inicio. una vez cargados se nos mostrara un menú, aquí procederemos a asignar el nombre de nuestras interfaces digitamos el número 1 , damos enter , aquí digitamos la tecla n , no configuraremos las Vlans , asignamos nuestra interfaz wan le asignamos a em0 , ahora nuestra LAN la nombramos em1 y para finalizar nuestra red opcional Em2 que sería el dmz , aplicamos los cambios , escribimos la tecla "y" y damos enter, esperamos a que apliquen los cambios.

Ahora procederemos a configurar las ips de nuestras interfaces, opción 2 y enter , comenzaremos con la red wan , configuramos con el DHCP de nuestro modem para ello digitamos la tecla "y" , la siguiente opción damos en "n" no configuremos las ipv6 , y aplicamos los cambios , esperamos a que finalice.

Procederemos a configurar la siguiente interfaz , opción 2 y luego digitamos el número 2 de nuevo aquí se nos solicita la dirección ip que deseemos, en esta opción introduciremos la dirección de puerta de enlace de nuestra red, para ello podemos conocerla usando el código cmd y el comando Ipconfig en nuestro sistema anfitrión , en este caso nuestra puerta de enlace es 192.168.56.1 , , digitamos esta dirección en Pfsense y damos enter , elegimos la máscara de subred que utilizaremos, en este caso la opción "24" que corresponde a 255.255.255.0 , y damos enter , damos entre dos veces mas para omitir las opciones , una vez se no pida habilitar el servidor DHCP damos si, digitamos "y" , ahora se nos pide definir un rango de direcciones para esto , así que podemos iniciar desde la dirección 192.168.56.2 hasta 192.168.56.100 , aplicamos los cambios .

Ahora configuraremos la opción 3 , seguiremos los mismos pasos anteriores asignamos otra dirección ip , por ejemplo 10.15.0.1 repetimos los pasos y asignamos un rango desde 10.5.0.2 hasta 10.5.0.100 , aplicamos los cambios .
A continuación habilitamos el sshd , opción 14 , una vez realizado lo anterior iremos a nuestro sistema operativo , aquí nos conectaremos a la red 1 que es la que configuramos como red interna, procederemos a revisar que ip se le asignó a este sistema, utilizando el comando ipconfig en el cmd-
Ahora en cualquier explorador web digitamos la dirección de puesta de enlace 192.168.56.1 aquí se nos mostrara un menú de pfsense, se nos pide un nombre de usuario y contraseña , por defecto el usuario es admin y la contraseña es pfsense una vez dentro se nos muestra un menú, damos click en next, de nuevo next aquí cambiamos el nombre del dominio por el que deseemos y escribimos un servidor dns , aquí escribimos el servidor de google para fines académicos y aplicamos cambios , damos click en next si deseamos realizar cambios en la wan aqu podemos hacerlos pero no haremos cambios, damos click en next, y luego en

next , si deseamos cambiar la contraseña aquí podemos hacerlo , y aplicamos los cambios.
Un buen método para conocer si está operando pfsense seria acceder al servidor utilizando por ejemplo Putty , entramos al software y digitamos nuestra puerta de enlace 192.168.56.1 y damos click en open , como vemos se encuentra bloqueado , se nos pide nombre de usuario y contraseña , comprábamos que podemos acceder con esta información y vemos como pudimos acceder al servidor . ahora podemos efectuar reglas de bloqueo para bloquear diversas páginas, aquí intentaremos bloquear facebook, como observamos entra común y corriente, entonces crearemos un alias atreves de la opción de firewall, buscamos la opción de alias, usamos un nombre de alias y se nos pide la ip de la página, digitamos la ip , y agregamos, inmediatamente buscamos la opción de reglas , buscamos nuestra red lan , añadimos, seleccionamos la opción bloquear y en la opción destino escribimos el alias que creamos, y habilitamos Log , guardamos y aplicamos cambios. Vamos a la pestaña de youtube y recargamos como vemos, aun carga la página esto es porque la dirección ip no es la correcta entonces , tomaremos un camino diferente, crearemos una lista negra atreves de un servidor proxy , buscaremos un paquete en la opción Packcage manager llamado squid, procedemos a instalarlo esperamos que finalice, una vez finalizamos buscamos la opción servicios y opion squid proxy server, habilitamos el servicio , elegimos la interfaz lan observamos que puerto usara, y habilitamos un proxy transparente, podemos deshabilitar la opción de modo offline en el menú local cache para que el disco duro no se llene de información excesiva, crearemos nuestra lsita negra en la opción Alcs , escribimos nuestra puerta de enlace y buscamos la opción de lista negra , ahí escribimos los dominios y damos click en aceptar, aun se peude acceder a youube, debemos acceder y conectarnos al proxy, para ello buscamos a opciones de red , en nuestro sistema win 8.1 opción conexiones , opción configuración de red de área local, aquí digitamos la dirección ip del servidor y del puerto 3128 , y aceptamos , vamos a la pestaña donde se encuentra facebook y como observamos hay un error en el proxy, regresamos a la configuración de pfsense y notamos que no habíamos aplicado correctamente los cambios, modificamos los datos aplicamos y comprobamos de nuevo de que ahora si se encuentra bloqueado este dominio de esta forma podemos establecer políticas de seguridad de red en nuestra redes y proteger asi nuestra información de posibles ataques muchas gracias.” -

11.ENTREVISTAS

Acta entrevistas empresa NOSTRADAMUS S.A.S

Parte 1. Oficiales de seguridad

PRESENTACION

En el siguiente documento se recompila la información obtenida al ejecutar diversas entrevistas al personal capacitado para dar uso de la información de la empresa.
Se tuvieron en cuenta preguntas en el ámbito personal como técnico para poder comprender el modo en el que operan dichas personas al ejecutar sus labores diarias.

Se entrevistará a diversos oficiales de seguridad informática dando como resultado la siguiente información.

INICIO

Nombre de la Persona entrevistada: Jesús García
Empresa donde labora: NOSTRADAMUS S.A.S
Cargo: Oficial de seguridad informática.
Experiencia en el cargo: 2 años y 4 meses
Número de personas a cargo: 2
Edad: 34 años
Funciones: Gestionar y planificar todo lo referente al mejoramiento de las políticas de seguridad informática en la empresa.

PRIMERA ETAPA: ANALISIS DE LOS PROCEDIMIENTOS INTERNOS.

Preguntas formuladas durante la entrevista:

Entrevistadora: Buenas tardes mi nombre es Alejandra un gusto en conocerlo, soy planeadora y desarrolladora de proyectos enfocados a la seguridad y manejo de la información de ámbito informático, cuento con una trayectoria de más de 2 años de experiencia en la ejecución de proyectos, ¿Puede indicarme cuál es su nombre y a que se dedica?

Entrevistado: Buenas tardes, es un gusto conocerla señorita Alejandra, mi nombre es Jesús García y mi labor es ser oficial de seguridad informática en esta compañía.

Entrevistadora: podría indicarme si es tan gentil ¿qué funciones cumple en ser un oficial de seguridad informática y que lo hace diferente a otros con el mismo cargo?

Entrevistado: Claro que si¡, entre mis funciones destaca el definir la política de seguridad informática que manejara la empresa y por su puesto definir los procedimientos para aplicarla, adicionalmente de desarrollar, planificar, gestionar y ejecutar actividades y proyectos referentes a la seguridad informática dentro de la empresa.

Establecer una meta con los directivos de la empresa en términos de seguridad de la información. Apoyar la implementación segura de sistemas de información en función del modelo se seguridad que se nos plantee, realizar la gestión de incidentes de seguridad y realizar las respectivas investigaciones de estos hechos para determinar sus causas, responsables y posteriormente plantear recomendaciones y mejoras para los sistemas afectados. Incentivar a la empresa a la ejecución de auditorías que se enfoquen en el tema de seguridad en la seguridad para de esta forma evaluar las prácticas enfocadas a la seguridad en nuestra empresa.

Además, también el crear un grupo de respuesta de incidentes de seguridad de esta forma se puede manejar de una manera más eficiente y rápida los incidentes, fallas errores etc.… que ocurran en la empresa en materia de seguridad informática.

Lo que me hace diferente de otras personas es la capacidad de poder implementar mecanismos robustos que permiten detectar vulnerabilidades que posea una red, adicionalmente de proteger y aislarlas con gran rapidez.

Entrevistadora: interesantes labores que desempeñan, me pregunto cómo es que ponen en ejecución estas labores, podría contarme ¿qué estándar o estándares de seguridad informática implementan para el cumplimiento de sus funciones y desarrollo de proyectos?

Entrevistado: es esta empresa implementamos el estándar ISO 17799 , con este estándar recopilamos información en los procedimientos que se ejecutan día a día esto nos ayuda a mantener un control más detallado sobre el cómo y el por qué se ejecuta una tarea , por ejemplo suponga usted señorita que el día de hoy ocurre una falla a uno de nuestros equipos, se procede primeramente a notificar de la falla a los encargados directos de dichos equipos , se examinan el estado del equipo y la naturaleza de la falla, y se ejecuta la solución consignada dentro de nuestro manual de procedimientos en la sección de fallas y soluciones, posteriormente se realiza la actividad pertinente y al solucionar la falla se consignara en un formato que diseñamos para cuando ocurren estas fallas. Esta información señorita nos ayuda como empresa a contar con un buen manejo de los incidentes que ocurren en el día a día ayudándonos a mantener nuestra empresa e operación continua.

Entrevistadora: muy interesante todo esto que me plantea, le agradezco el ejemplo de cómo ejecutan el estándar en su empresa, con lo que me acaba de decir se me formulo una pregunta que me gustaría que me ayudara a resolver ¿qué recomendaciones podría darme sobre la implementación de ungís?

Entrevistado: por supuesto que puedo darle unas cuantas recomendaciones, en nuestra empresa a hora de implementar por primera vez el estándar ISO 17799 , debíamos primeramente contar el aval y el patrocinio de los directores y gerentes de la empresa , mostrándoles las grandes ventajas que tenía la implementación para que se ejecutara en la empresa , le recomiendo que a la hora de que desee mostrar esto a los gerentes de una empresa les haga ver el cómo se pueden mejorar en gran manera los procedimientos internos sobre el manejo de la información y que esto a la vez se traduce directamente en dinero y bienestar . El segundo paso es que debe de dejar muy en claro una estructura de toma de decisiones y por su puesto una jerarquía para la misma, si usted sabe que para tomar una decisión importante en su empresa también debe tener en claro quien o quienes deben de aprobar o desaprobar la misma, y por su puesto en caso de requerir que uno de ellos tome una decisión que esta persona o personas sea o sean las indicadas para lo tomarla, ¿esto en que ayudaría? Se podría preguntar, piénselo de este modo, si en caso de una eventualidad usted sabe a quién recurrir esto facilitara el resolver dicha eventualidad, pero si esto no es claro o no se ha establecido en la empresa, la decisión podría tomarla una persona no idónea para la misma ocasionándole más problemas. El siguiente paso es realizar un estudio de como su empresa se desempeña en materia de seguridad, este paso es muy importante porque aquí es donde se conocerá el cómo la empresa realiza sus procedimientos en términos de seguridad, en este paso podemos no solo conocer el cómo realizan las tareas sino también ayudar a mejorarlas o corregir posibles errores que se realizan en las mismas, es aquí donde definimos nuestros estándares , las normas y todo aquello que nos permita mejorar en el cómo manejamos la información en el día a día. El siguiente paso es el que yo llamaría el paso crítico, porque como usted sabe la vida es muy incierta y cosas inesperadas pasan en el día a día, no podemos saber que pasara mañana, pero si podemos tener un plan sobre qué hacer si algo critico nos ocurre, piénselo así que haría usted si en un momento del día su empresa se prende en llamas? Cosas así pueden pasar y tener un plan de acción sobre como operar, así que debemos identificar cuáles de todos los procesos que se realizan en la empresa son de carácter crítico y priorizar estos mismos en caso de algo inesperado, se podría decir que se jerarquizan los procedimientos y a la vez se establecen prioridades en los mismos en casos de que algo malo ocurra. El siguiente paso que debe tomar es establecer tiempos de ejecución en los procedimientos asignar personal idóneo para desempeñar las tareas y tener un presupuesto claro de cómo usara. Y como un último paso podría realizar una revisión de los estándares de seguridad para así poder implementar y mejorar lo que ya se ejecutó anteriormente.

Entrevistadora: Puede contarme brevemente que políticas de seguridad emplean para el manejo de la información y ¿qué procedimientos realizan para la ejecución de estas políticas?

Entrevistado: Dentro de la organización contamos con un comité de planeación en la cual evaluamos los requisitos de la organización, los activos que se poseen, el presupuesto que se asigna para la ejecución de proyectos, dentro de este comité se plantean diversas ideas que tengan las personas directamente relacionadas con el tema del manejo y seguridad de la información, en este comité se han logrado definir políticas como las siguientes.
Una de ellas establece reglas en el uso de los activos de información por parte del personal responsable, tales como el modo de usarlo, hasta el cómo es almacenada la información en ellos, por ejemplo, la información no debe de ser enviada desde los activos a correos electrónicos personales o ajenos a la organización, tampoco se permite la descarga de archivos ejecutables de fuentes no autorizadas o desconocidas en los activos de la organización.
Otra de las políticas establece el nivel de privilegios asignados a cada persona que maneje dicha información, no se le permite el acceso a la información a ninguna persona aprobada por el comité, de ser aprobada se asignaran el nivel de privilegios según requiera su cargo y sus funciones.

También se estableció una política en el uso de medios de almacenamiento externos, se implementó un mecanismo de encriptación que no permite el copiado de la información a medios externos no autorizados.

Políticas como estas son las que rigen el cómo se realizan los procedimientos en esta empresa.

Entrevistadora: Muy interesante, puede contarme un poco sobre ¿a qué amenazas informáticas se ha enfrentado desde que labora en esta empresa?

Entrevistado: desde que laboro en esta empresa hemos sido atacados de varias formas, cuando tenía apenas unos cuantos días de trabajar en la empresa detectamos un Caballo de Troya que venía contenido dentro de un mensaje de correo electrónico dirigido a la empresa. A causa de este se filtró información importante sobre un proyecto que se iba a ejecutar en los siguientes días.

También hace poco tiempo tuvimos un ataque dirigido por un hacker que deseaba filtrar información vital de nuestros usuarios para extorsionarlos para obtener dinero a causa de la información que deseaba obtener.

Adicionalmente debido a una falla que poseían algunos equipos y a medios de almacenamiento extraíbles no autorizados, diversos equipos fueron infectados con Spywares que afortunadamente no lograron obtener información de estos gracias a una temprana detección por parte de mi equipo.

Entrevistadora: ¿ya que me ha mencionado los spyware me nace una duda, podría decirme que antivirus emplean en esta empresa y por qué lo usan?
Entrevistado: En esta empresa se tiene implemento el uso del antivirus Bitdefender GravityZone Business Security , este antivirus tiene muchas ventajas entre las cuales está el que es simple de usar , no afecta el rendimiento de los equipos donde se implementa, ayuda a protegerlos de amenazas desconocidas que podría afectarlos , además cuenta con un sistema de detección de comportamientos que bloquea amenazas en tiempo real, este antivirus lo tenemos implementado en 10 de nuestros equipos, tanto cups como servidores, usamos una consola de gestión para administrar los dispositivos conectados en nuestra red, aquí es donde configuramos el firewall de dos vías y establecemos un protocolo de transmisión de datos para proteger de amenazas a los dispositivos de nuestra red. De esta forma gestionamos cada dispositivo conectado a nuestra red, bloqueando páginas que podrían ser maliciosas, evitando que se transmita información sensible a otro dispositivo no autorizado para el manejo de la misma, es una buena herramienta que nos permite el mejoramiento del uso de la información en nuestra empresa.

Entrevistadora: Por lo que puede contarme es una muy buena ayuda este antivirus que manejan además es Increíble que hayan sufrido estos ataques a la fecha de hoy, me causa curiosidad el saber qué mecanismos utilizaron para poder evitar que posibles ataques como estos se presenten de nuevo, ¿podría indicarme alguno de ellos?

Entrevistado: Para responderle esa pregunta puedo decirle que esta empresa toma muy enserio la privacidad y seguridad de la información de todos sus usuarios así que tiene políticas estrictas sobre el manejo de ella, para proteger la información de los diversos usuarios se tomaron medidas tales como
El uso de credenciales y privilegios asignados a cada persona para el manejo o visualización de información dentro de la empresa, esto mediante software de autentificación y validación mediante contraseñas y lectores biométricos para la identificación del usuario.
Bloqueo de descargas directamente desde el equipo o el encriptado mediante el propio sistema operativo para el acceso a el almacenamiento de los equipos.
Acceso a las bases de datos únicamente por protocolos de red seguros y por tiempos limitados para el manejo de la información.
Generación, actualización y gestión de claves encriptadas usando protocolos de 3 envíos.

Estos y más mecanismos empleamos para poder proteger la información de la empresa de posibles ataques o fallas que posea.

Entrevistadora: muy interesantes y buenos mecanismos poseen para la protección de la información, por último, podría contarme a brevedad que proyectos planea ejecutar próximamente en la empresa.

Entrevistado: dentro de los planes que deseamos implementar próximamente es la mejora de la infraestructura física de nuestra red, para mejorar la velocidad de envío y recepción de datos dentro de la misma.

También implementaremos un mecanismo de software que permita el visualizar mediante un entorno grafico que permita mostrar todos los usuarios dentro de la red, que actividad se encuentra realizando y permitir el acceso o bloqueo de los mismos de forma rápida y efectiva.

Esos proyectos son los que se encuentran próximos a ejecutar.

Entrevistadora: proyectos muy buenos para el desarrollo y crecimiento de la empresa, le agradezco mucho su tiempo y continuaremos en contacto para ayudarle a desarrollar sus proyectos de una forma más rápida y efectiva, muchas gracias.

Entrevistado: a usted por su tiempo buenas tardes.

Parte 2.

INICIO

Nombre de la Persona entrevistada: Antonio Torres
Empresa donde labora: NOSTRADAMUS S.A.S
Cargo: Gerente financiero
Experiencia en el cargo: 5 años
Número de personas a cargo: 15
Edad: 56 años
Funciones: supervisa y se encarga del flujo de dinero y los activos que entran y salen de una empresa

Entrevistadora: Buenas tardes mi nombre es Alejandra un gusto en conocerlo, soy planeadora y desarrolladora de proyectos enfocados a la seguridad y manejo de la información de ámbito informático, cuento con más de 2 años de experiencia en la ejecución de proyectos, ¿Puede indicarme cuál es su nombre y a que se dedica?

Entrevistado: Buenas tardes mi nombre es Antonio torres y soy el gerente financiero de esta empresa, podría extenderme en funciones, pero podría resumírselas en que me encargo de todo lo que tenga que ver con el flujo del dinero y los activos de esta empresa, si desea saber algo sobre el tema yo soy la persona indicada para ayudarle.

Entrevistadora: Encantada de conocerlo, muchas gracias por ser tan claro, mi área de trabajo es la del desarrollo de proyectos como ya le mención el día de hoy estoy aquí con el ánimo de preguntarle sobre, que conoce sobre la implementación del SGSI en su empresa, coménteme que conoce sobre ello.

Entrevistado: soy una persona que maneja activos en esta empresa y claro que conozco de este tema, hace un tiempo hablaron conmigo nuestro personal encargado de la parte informática, me comentaron que deseaban implementar un proyecto para el m anejo de la información, yo como persona capacitado en finanzas no comprendo mucho sobre el tema informático así que les pedí me resumieran claramente para que serviría esto.
Me comentaron que la información que manejamos en nuestra empresa y es mas en cualquier empresa negocio o casa, es vulnerable a ataques , robos filtraciones , manipulaciones entre otras , así que debíamos de establecer unos mecanismos que nos ayudaran a que esa información importante se manejara de la mejor forma , porque imagínese usted me preguntaron sobre si tenía algún familiar enfermo a lo que respondí que sí, mi madre , me preguntaron además que problema médico tenia, les respondí que era privado porque es algo de mi familia, a lo que ellos respondieron y si le dijéramos que podríamos lograr saber no solo de que sufría mi madre sino además que tratamientos se le han hecho, donde está internada, que medicamentos toma, su nombre su historia clínica y todo lo referente a ella , me dijeron ¡qué haría¡ a los que respondí claramente, pues estaría asustado y buscaría a las autoridades para que los metieran presos porque esa información no es algo que ellos debían saber, a lo que respondieron EXACTO ese es el punto, si así pasa con la información que usted maneja diario imagínese con lo que pasaría si algo así le pasara a la empresa, a lo cual me dejaron preocupado, ¡imagínese¡ si eso pasara con la información que manejamos de nuestros clientes, que pasaría con nuestro negocio y qué pensarían ellos de nosotros, que no servimos como empresa y dejarían de usar nuestros servicios , a lo que la empresaria entraría en banca rota¡.
Luego de todas esas preguntas me dijeron que existía una forma de proteger nuestra información, a través de mecanismos procedimientos y políticas que ayudaran a evitar cosas así. A lo cual respondí que hay que hacer, ellos me expusieron un proyecto donde definían cada procedimiento, actor y activos de la empresa el que debían hacer y el cómo, realmente no entendía mucho, pero me ilustraron mediante ejemplos el cómo operaban los antivirus, firewall y el cómo poder detectar amenazas, así que cuando llego la hora de la verdad les pregunte ¿y bueno cuánto cuesta esto? , a lo que ellos me mostraron un presupuesto y tiempos de ejecución, lo analizamos con cuidado y la rentabilidad de este proyecto era alta, el costo era bajo y el beneficio altísimo, a lo cual aprobé este presupuesto para la ejecución.
Esto es lo que puedo contarle sobre el tema es todo lo que se.

Entrevistadora: le encaminaron muy bien y se ve que lo entendió muy bien le agradezco me contara sobre esa experiencia en su trabajo, mucha gracias.

Parte 3

Nombre de la Persona entrevistada: María Rodríguez
Empresa donde labora: NOSTRADAMUS S.A.S
Cargo: Asesora comercial.
Experiencia en el cargo: 2 años
Número de personas a cargo: 0
Edad: 29 años
Funciones: servicio al cliente, ventas de productos y agendado de citas

Entrevistadora: Buenas tardes mi nombre es Alejandra un gusto en conocerlo, soy planeadora y desarrolladora de proyectos enfocados a la seguridad y manejo de la información de ámbito informático, cuento con más de 2 años de experiencia en la ejecución de proyectos, ¿Puede indicarme cuál es su nombre y a que se dedica?

Entrevistada: Buenas tardes mi nombre es maría soy una asesora comercial de esta empresa, mi labor es brindar servicio al cliente, promuevo la compra de servicios para la empresa y realizado agendado de citas que requieran los usuarios de la misma.

Entrevistadora: ¿es una labor muy importante, el día de hoy me encuentro realizando unas preguntas sobre el tema de gestión de la información, usted señorita maría como una persona que opera un equipo personal de la empresa puede contarme que conoce sobre este tema?

Entrevistada: claro que sí, mira cada día al iniciar mi jornada laboral a la hora de encender mi computadora me solicita una clave, esta clave nos la suministran cada dos semanas , además de realizar un escaneo de un código de barras de mi carnet empresarial, y un escaneo de mi huellas digitales para iniciar el equipo, una vez hecho esto puedo iniciar mi equipo, luego inicio el software de llamadas de la empresa y sale un mensaje que dice “ encriptando comunicación” se queda allí unos 30 o 40 segundos e inicia, tan pronto recibo llamadas y deseo consultar algo en la base de datos se me pide diligenciar un formato breve sobre que deseo consultar, a lo cual lo relleno con la información que solicito y procede a hacer una verificación de mis credenciales, algunas veces la información que solicito no logro acceder a ella debido a que no tengo los permisos en ese caso me contacto con mis superiores o líder de seguridad informática para que pueda suministrar la información , de poder acceder a la información se lo comunicó al usuario y diligencio un formato donde consigno que información suministre, al finalizar la llamada procedo a enviar un correo electrónico al usuario con el cual me comunique haciéndole un resumen de las solicitudes que requirió, el cual es

revisado por un superior y posteriormente enviado al usuario . Mi superior me dice que lo revisa y encripta realmente no entiendo mucho sobre el tema, pero creo que lo hace para que solo lo pueda ver el usuario con el que hable, esto es lo que puedo contarle sobre el tema no domino mucho el tema informático.

Entrevistadora: te agradezco mucho tu tiempo, te puedo contar que en horas de la noche realizare un foro tratando sobre estos temas y así podemos comunicar el cómo la empresa maneja estos temas, el foro se llama “seguridad informática un tema de todos” estas invitadas, te estaré esperando, buenas tardes.

Resultados de las entrevistas

Como resultados de estas entrevistas, se planteó la implementación inmediata de una auditoria externa, con la necesidad de poder establecer mecanismos que permitan identificar el funcionamiento de los diversos procedimientos que se ejecutan en la organización.

12.PLAN DE AUDITORIA

Se propone implementar esta misma en un plazo de 3 semanas posteriores a la finalización de estas mismas, se abordarán los procesos básicos, intermedios y avanzados en los cuales se haga uso de la informática, como se muestra a continuación:

- **Análisis detallado sobre la recolección de la información**: orientada principalmente a todo proceso por el cual la organización recolecta información ya sea de formas verbales como lo son los call center, mediante correos electrónicos, directamente en las plataformas web de la empresa etc.
- **Tiempo estimado:** 1 semana.

- **Estudio de los procedimientos de seguridad que implementa la organización**: orientados hacia el área de seguridad informática, se establecerá un estudio profundo sobre los procedimientos que realizan los encargados designados por la empresa, partiendo desde los protocolos ya implementados por la organización.
  Tiempo estimado: 2 semanas.

- Recolección de información sobre el almacenaje de información: este ítem estar orientado principalmente a como la organización lleva a cabo el almacenaje de la información que posee, ya sea en modos físicos como

discos extraíbles, servidores físicos en las instalaciones de la organización, hasta las bases de datos que se manejan en la misma.
Con esto se pretende recopilar información importante que permitirá no solo establecer normas para el mejoramiento de los procesos internos y externos de la organización en materia de seguridad informática sino además la inserción de este proyecto orientado a cumplir las necesidades de esta.
Tiempo estimado: 3 semanas

13.ESTADO ACTUAL DEL PROYECTO

La siguiente tabla describe las metas alcanzadas por el Proyecto en función del desarrollo actual del proyecto, esto sirve como una guía para establecer mecanismos que permitan una orientación correcta para el desarrollo del mismo.

Objetivos del Proyecto	Contenido del Proyecto
-Establecer la metodología a implementar de acuerdo a la norma ISO27001:2013 contemplando todos los activos de la empresa para generar el análisis de riesgos	Mediante el transcurso del proyecto, y en función del desarrollo de entrevistas y auditorias se ha logrado generar un listado de los activos que posee la empresa para poder así asignar los niveles de riesgos a los cuales están comprometidos. ✓
-Analizar el nivel de madurez del sistema de gestión de seguridad de la compañía identificando su estructura y descripción del proceso de aplicación con alcance a la infraestructura crítica y a la definición de nuevos protocolos de seguridad	Sumado al numeral anterior el plan de auditorías permitirá establecer un análisis profundo de los protocolos implementados por la organización y de esta forma llevar a cabo la implementación de un plan de mejoramiento suministrado por este proyecto para aumentar la robustez de los sistemas informáticos de la empresa. ✓.
Determinar mediante el uso de herramientas de seguridad y penetración, las posibles vulnerabilidades que posee el sistema de seguridad de la empresa implicada.	Se llevó al cabo mediante el uso de diversas soluciones de software la detección de vulnerabilidades que posee la red de la empresa, se realizaron la simulacion de los ataques generados en la compañía evidenciando las vulnerabilidades y practicas inadecuadas que permitieron explotar dichas vulnerabilidades, adicionalmente mediante estas herramientas se puede determinar el nivel de seguridad que posee la misma, llevando a cabo procesos de penetración para así llevar a cabo la implementación

	del plan de mejoramiento. ✓
Documentar un plan de mejoramiento en temas de normatividad y protocolos de seguridad implementados en la empresa implicada para disminuir el riesgo de sufrir ATAQUES CIBERNETICOS u otros RIESGOS que afecten la seguridad de los sistemas informáticos de la empresa	Sumado al proceso de auditoria propuesto en este proyecto se pretende poder recopilar la información necesaria para poder llevar a cabo una correcta implementación de medidas y políticas en seguridad de red, una vez reunida esta información se llevara a cabo la mejor solución para la necesidades de la organización ✓

14.PLAN DE MEJORAMIENTO

El siguiente plan de mejoramiento se construye en función de la información recopilada en la realización de las pruebas de robustez de los sistemas, para ello dividiremos la propuesta en los siguientes ítems:

- Mejoramiento en la gestión interna: Realizar correctas configuraciones a los sistemas informáticos en términos de seguridad, facilitando mecanismos de recopilación de fallas y corrección de errores, documentaciones día a día que permitan evaluar la eficiencia de los sistemas en tiempo real.
- Organización corporativa en materia de seguridad: establecer una organización jerárquica que permita poder establecer roles y actores en el proceso del manejo de la información en los sistemas de la organización, adicionalmente en consecuencia de las entrevistas realizadas anteriormente establecer métodos de concientización sobre el uso de la información y su valor como un bien corporativo.
- Propuestas adicionales: implementación de diversos mecanismos que permitan mejorar la robustez de los sistemas de gestión de información, haciéndolos más eficientes en el cumplimiento de su misión.

Una vez definidos los ítems que se trabajarán en el plan de mejoramiento, procederemos a especificar las acciones y alcance que tendrán para el proyecto, de la siguiente manera:

14.1 MEJORAMIENTO EN LA GESTIÓN INTERNA

Contenida de las siguientes propuestas, divididas en diversas acciones a tomar para llevar a cabo:

1. Cada responsable implicado en el manejo, intervención o mantenimiento de los sistemas de seguridad en redes , deberá comprometerse a estar en una constante mejoría de los aplicativos de seguridad en las redes , en todas y en cada una de las capas de seguridad en las redes, desde ya sean los diversos cortafuegos hasta métodos de filtrado de información en aplicaciones, esta acción cumple un énfasis principal orientado hacia la parte de software , como un mecanismo inicial para el mejoramiento de los mecanismos de seguridad en la red.

2. Cada responsable implicado en el manejo intervención o mantenimiento de los sistemas de seguridad en redes enfocados hacia la parte de hardware, debe de comprometerse a mantener un rendimiento óptimo en los diversos dispositivos implicados en el sistema de seguridad en redes. Implementando mecanismos de mantenimiento preventivo y correctivo en un intervalo de tiempo mínimo de 1 mes, asegurando así y minimizando los riesgos que puedan sufrir estos dispositivos a fallas de índole eléctrica o fallas de índole electrónico.

3. Se debe establecer una herramienta universal para el manejo de incidentes de seguridad informática, para de esta manera recopilar información que permita establecer mecanismos eficaces para posibles fallas o ataques informáticos en el futuro.

4. Todo responsable directo del uso gestión, administración, mantenimiento de los sistemas informáticos, debe de proponer nuevos mecanismos que ayuden a definir nuevos procesos (o redefinir los que ya se están implementando) para complementar la gestión de cambios, procesos como lo son la detección, actualización y tratamiento de vulnerabilidades, o procesos enfocados hacia el monitoreo de la seguridad de redes. Este ítem tiene como propósito involucrar a todo el personal que participa en los sistemas para mantener un proceso incluyente, para integrar a todos en este proceso de mejoría.

5. Una vez establecido el orden jerárquico en la organización, el director de seguridad deberá crear un documento que especifique la arquitectura de seguridad implementada en la organización.

6. Realizar un cronograma de pruebas de seguridad, periódicamente, aproximadamente cada 2 meses, para así poder establecer la rigidez de los esquemas de seguridad implementados.

7. Establecer procedimientos que permitan revisar los resultados obtenidos tras la ejecución de recopilación de datos y ejecución de pruebas para de esta manera poder implementar acciones que permitan mejorar los sistemas informáticos en temas de seguridad, adicionalmente ayudar a construir un documento recopilatorio para evaluar el progreso de las acciones tomadas cada cierto tiempo, tiempo sugerido cada 6 meses.

8. Crear mecanismos y protocolos que permitan la implementación rápida y efectiva de actualizaciones a los sistemas informáticos, ayudando así a la reducción de costos en tiempos de implementación. Reduciendo así los tiempos de mantenimiento de los sistemas.

A continuación, se describen las acciones a tomar en temas de organización corporativa y jerarquización organizacional para los procesos informáticos de la organización.

1. Se debe de formar un grupo de personas capacitadas para la ejecución de actividades orientadas al mejoramiento de la seguridad informática y de la informacion en la organización, y estas personas deben de ser designadas por la directiva administrativa de la organización.

2. Se debe de implementar una política orientada hacia la calificación y calidad de la información , estableciendo así las pautas y normas CLARAS sobre el alcance que tiene la misma, el uso que se le puede dar y así mismo las personas implicadas para el manejo de la misma, clasificando la información en grupos tales como el grado de confidencialidad, requisitos sobre la transmisión de información en los diversos medios informáticos de la corporación , restricción de acceso a la información, entre otras.

3. Establecer la normativa operativa sobre los tiempos máximos y mínimos para la ejecución de medidas implicadas en temas de seguridad en las redes.

4. Crear un plan de concientización en seguridad de redes para todas aquellas personas que pertenezcan a la corporación.

5. Crear un plan de formación y capacitación constante sobre los temas relacionados a la seguridad en redes.

6. Crear y establecer los diversos perfiles de usuario y como como consecuente, sus privilegios para el acceso a la información. “Segregacion de funciones”

7. La gerencia de la organización en conjunto con el equipo creado anteriormente deben crear y establecer una política de medidas de acceso en conjunto con un grupo de contraseñas seguras y llaves de acceso para el uso de la información.

8.Implementar un SOC o monitoreo continuo sobre los usuarios e infraestructura de la compañía. “podria validarse un coutsoursing o adquirir el servicio de SOC”.

El objetivo de ejecutar las acciones anteriores es el de poder crear un conjunto de protocolos y normas que permita esclarecer claramente los responsables del uso de la información en la corporación, para a partir de ello poder establecer

mecanismos que permitan la mejoría constante de los procesos llevados por la corporación.

Las siguientes acciones son complemento de las anteriores y como consecuencia ayudan a la mejoría de procesos que se realizan en la corporación:

Otras medidas:

1. Creación de un correo electrónico institucional, con sus debidas políticas de acceso y circulación de información.

2. Creación de copias de seguridad, y posteriormente realización de pruebas de seguridad en las mismas.

3. Creación de sistema de acceso remoto.

4. Implementación de protocolos de seguridad frente a ataques de tipo DDoS.
5. Implementar y garantizar la gestion de vulnerabilidades sobre la infraestructura de la compañía.

Con este plan de mejoramiento se busca el lograr optimizar todos los procesos referentes a la gestión de la información informática de la corporación, cabe resaltar que toda aquella propuesta de mejoramiento, ideas proyectos deberán ser expuestos al comité de seguridad para su debida aprobación.

15.CONCLUSIONES

- Se logro Implementar una propuesta sólida que cumple con los requisitos establecidos por la empresa NOSTRADAMUS. La propuesta cumple de manera óptima, eficaz y eficientemente con el objetivo mayor de mejorar la seguridad informática de la misma.

- Basados en las buenas prácticas a nivel mundial y tomando como referencia la ISO/IEC 27000, se apoya a la organización para guiarlos en la mejora continua del SGSI e identificar su nivel de madurez. El planteamiento y esquema de seguridad de la información fue trabajado baso la ISO/IEC 27001 y 27002 Anexo A, le fue entregado la matriz de aplicabilidad “SOA” y Plan de tratamiento de riesgos sobre los activos identificados y clasificados como críticos

- Se logró demostrar de una manera rápida y eficiente la configuración e implementación de herramientas de software que ayudan a él complimiento de políticas de seguridad en redes, para este proyecto se utilizaron herramientas como pfsense que permitieron la creación de un servidor proxy entre otras configuraciones. Mediante el uso de Pfsense se logra cumplir con una infraestructura de red básica. Adicionalmente de que es un sistema de bajo consumo, es económico y portable, una opción muy viable para optar por un sistema firewall de alta fidelidad.

- Mediante la metodología Magerit se logró recopilar información vital sobre los activos de la empresa para de esta manera lograr tomar las acciones correctas sobre cómo se manejarían para el proyecto.

BIBLIOGRAFIA

1. Barceló, O. J. M, Íñigo, G. J., Y Llorente, V. S. Protocolos y aplicaciones Internet. Barcelona, ES: Editorial UOC. (2008). Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10646241&p00=protocolo+http

2. Cardador, C. A. L. Implantación de aplicaciones web en entornos internet, intranet y extranet (MF0493_3). Madrid, ESPAÑA: IC Editorial. (2014). Disponible en: http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=190&docID=11126348&tm=1481044080162

3. Chicano, T. E. Auditoría de seguridad informática (MF0487_3). Madrid, ESPAÑA: IC Editorial.(2014).Disponible en http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=215&docID=11126290&tm=1481044220050

4. Contreras Castañeda, Miguel Ángel. Desarrollo de aplicaciones web multiplataforma. Madrid, ESPAÑA: Ministerio de Educación de España, (2016). ProQuest ebrary. Web. Disponible en http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=11216901&p00=inyecci%C3%B3n+archivos

5. Hernández, D. L. R. Un modelo para la implementación de la seguridad de una aplicación Web con el uso de la programación orientada a aspectos. La Habana, CU: D - Instituto Superior Politécnico José Antonio Echeverría. CUJAE. (2012) Disponible en http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/reader.action?ppg=108&docID=10624371&tm=1481119226186.

6. Howard, M., & Leblanc, D. 19 puntos críticos sobre seguridad de software: fallas de programación y cómo corregirlas. México, D.F., MX: McGraw-Hill Interamericana. (2007). Disponible en http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=10433796&p00=vulnerabilidades+web

7. Lázaro, D. Ataques SQL Injection en PHP.(2016, 04). Obtenido 03, 2017, de https://diego.com.es/ataques-sql-injection-en-php

8. E. (2014, 04). Cómo funciona SQL Injection, seguro eres vulnerable. Obtenido 03, 2017, de http://www.cristalab.com/tutoriales/como-funciona-sql-injection-seguro-eres-vulnerable-c113268l/

9. (2013, 12). Ataques de inyección SQL: qué son y cómo protegerse. Hostalia.com. Obtenido 03, 2017, de http://pressroom.hostalia.com/white-papers/ataques-inyeccion-sql

10. (2012, 12). Inyección SQL. owasp. Obtenido 03, 2017, de https://www.owasp.org/index.php/Inyecci%C3%B3n_SQL

11. (2016, 06). Open Web Application Security Project. Obtenido 03, 2017, de https://www.owasp.org/index.php/

12. Rengarajan, A., Sugumar, R., & Jayakumar, C. Secure Verification Technique for Defending IP Spoofing Attacks. International Arab Journal Of Information Technology (IAJIT), 13(2), 302-309. (2016). Obtenido de http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aci&AN=114270555&lang=es&site=ehost-live

13. Pandey, A. a., & Saini, J. s. Comprehensive Security Mechanism for Defending Cyber Attacks based upon Spoofing and Poisoning.BVICAM's International Journal Of Information Technology, 8(2), 1011-1016. (2016). Disponible en http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aci&AN=122681957&lang=es&site=ehost-live

14. Bijral, R. K., Gupta, A., & Sharma, L. S. Study of Vulnerabilities of ARP Spoofing and its detection using SNORT. International Journal Of Advanced Research In Computer Science, 8(5), 2074-2077. (2017). Disponible en http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=aci&AN=124636718&lang=es&site=ehost-live

15. Gutierrez, F. (2011, 02). El Modelado de Amenazas de Seguridad. SEGURIDAD Y AUDITORIA DE SISTEMAS. Obtenido 05, 2018, de http://seguridadenlanube.blogspot.com.co/2011/02/el-modelado-de-amenazas-de-seguridad-es.html

16. Costas, J. Mantenimiento de la seguridad en sistemas informáticos. (2014) .Disponible en http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=11046692

17. Fernández, C. M., Piattini, M. (2012). Gómez, Á. (2014). Auditoría de seguridad informática. Recuperado de http://bibliotecavirtual.unad.edu.co:2077/lib/unadsp/detail.action?docID=110

46412

18. Gómez, L., Álvarez, A. Guía de aplicación de la Norma UNE-ISO/IEC 27001 sobre seguridad en sistemas de información para pymes. (2012). Disponible en http://bibliotecavirtual.unad.edu.co:2162/openurl?sid=EBSCO%3aedsebk&genre=book&issn=&ISBN=9788481437492&volume=&issue=&date=20120101&spage=&pages=&title=Gu%c3%ada+de+aplicaci%c3%b3n+de+la+Norma+UNE-ISO%2fIEC+27001+sobre+seguridad+en+sistemas+de+informaci%c3%b3n+para+pymes&atitle=Gu%c3%ada+de+aplicaci%c3%b3n+de+la+Norma+UNE-ISO%2fIEC+27001+sobre+seguridad+en+sistemas+de+informaci%c3%b3n+para+pymes&aulast=&id=DOI%3a&site=ftf-live

19. Berná Galiano, J. A., Pérez Polo, M., & Crespo Martínez, L. M.Redes de computadores para ingenieros en informática. [Alicante]: Digitalia. (2002). Recuperado de HYP

20. Borja Merino F. Febrero. Análisis de Tráfico en Wireshark, (1-52), (2011). Disponible en https://www.incibe.es/extfrontinteco/img/File/intecocert/EstudiosInformes/cert_inf_seguridad_analisis_trafico_wireshark.pdf

21. Bustamante, R.,SEGURIDAD EN REDES. Capítulos 1 - 4,(2014). Disponible en http://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Seguridad%20en%20redes.pdf

22. Dostálek, L., & Kabelová, A. Understanding TCP/IP: A Clear and Comprehensive Guide to TCP/IP Protocols. Birmingham, England: Packt Publishing.(2006) Disponible de Http://bibliotecavirtual.unad.edu.co:2048/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=e000xww&AN=267885&lang=es&site=ehost-live

23. Herzberg, A., & Shulman, H.Cipher-Suite Negotiation for DNSSEC: Hop-by-Hop or End-to-End?. IEEE Internet Computing, 19(1), 80-84.(2015). Disponible en http://search.ebscohost.com/login.aspx?direct=true&db=aci&AN=100949176&lang=es&site=ehost-live

24. México, U. N. (s.f.). Nota de Seguridad UNAM-CERT-2008-006 Vulnerabilidad en SQL Server podría permitir la ejecución remota de código. Recuperado el 04 de 03 de 2017, de

https://www.seguridad.unam.mx/vulnerabilidadesDB/?vulne=5691

25. TechNet, M. (s.f.). Reduciento explotación de fallas de seguridad con EMET - (es-ES). Recuperado el 04 de 03 de 2017, de https://social.technet.microsoft.com/wiki/contents/articles/25003.reduciento-explotacion-de-fallas-de-seguridad-con-emet-es-es.aspx

26. TICbead, «Las 10 grandes amenazas de seguridad en las bases de datos,» se. Ticbead, 17 abril 2013. [En línea]. Available: ttp://www.ticbeat.com/tecnologias/10-grandes-amenazas-seguridad- bases-datos/. [Último acceso: 24 mayo 2017].

27. «Seguridad en las bases de datos,» [En línea]. Available: ttp://gplsi.dlsi.ua.es/bbdd/bd1/lib/exe/fetch.php?media=bd1:0910:trabajos:seguridadbd.pdf. [Último acceso: 20 05 2017].

28. Tarazona T., C. H. Amenazas informáticas y seguridad de la información. Derecho Penal y Criminología: Revista Del Instituto de Ciencias Penales y Criminológicas, (. 84), 137. (2007). Disponible en http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsdnp&AN=edsdnp.3311853ART&lang=es&site=eds-live&scope=site

29. Parra Correa, C. A. Las amenazas informáticas: peligro latente para las organizaciones actuales. Gerencia Tecnológica Informática, (. 16), 85. (2007). Disponible en http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsdnp&AN=edsdnp.2659667ART&lang=es&site=eds-live&scope=site

30. Espín Mena, B. S. Auditoría de seguridad informática a la red de la entidad Cyber Xpress detectando sus fortalezas y deficiencias. (2013) disponible en http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.DD6A8ADE&lang=es&site=eds-live&scope=site

31. Romero Mestre, H. A. Ciberseguridad en sistemas de control industrial o ICSs. (2018). Disponible en http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.5428EE55&lang=es&site=eds-live&scope=site

32. Acosta Zambrano, J. A. Protocolo de seguridad informática para usuarios en la Universidad Regional Autónoma de Los Andes Uniandes. (2018). Disponible en http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.11C2A972&lang=es&site=eds-live&scope=site

33. Eterovic, J., & Cipriano, M. Aproximación a la seguridad de las comunicaciones en Internet de las Cosas.(2017). Disponible en http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.EDE37DA9&lang=es&site=eds-live&scope=site

34. Gutiérrez Vera, F., Ortega González, C. C., & Torres Yépez, M. D. MalWare, más allá de los virus informáticos. (2018). Disponible en http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.10DBB855&lang=es&site=eds-live&scope=site

35. Ficarra, F. Informática: Los virus informáticos. (2017). Disponible en http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.39426159&lang=es&site=eds-live&scope=site

36. Dulce María Canes Fauces, Yaimet Pérez Infante, & Sureima Callis Fernández. Acerca de los virus informáticos: una amenaza persistente About computer virus: a persistent threat. (2011). Disponible en http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.E0348018&lang=es&site=eds-live&scope=site

37. OWASP, Education Project. Ingeniería social [en línea], 2007. Disponible en url: http://osl.ugr.es/descargas/OWAND11/OWAND11%20Granada%__20-%20Ingenier%C3%ADa%20social.pdf

38. PENAGOS BERMUDEZ, Edilberto. INGENIERÍA SOCIAL, UN FACTOR DE RIESGO INFORMÁTICO INMINENTE EN. Neiva: Tesis de grado Especialización, 2015.

39. Seguridad y privacidad de la información. [En línea] mayo 03 de 2017. [Revisado 1 Septiembre 2017]. Disponible en: Https://www.mintic.gov.co/gestionti/615/articles-5482_G3_Procedimiento_de_Seguridad.pdf

40. Técnicas de ingeniería Social, [En línea] [Revisado 5 octubre 2017]. Disponible en:https://www.welivesecurity.com/la- es/2014/05/21/tecnicas-ingenieria-social-evolucionaron-presta- atencion/

41. WEBSECURITY. 2017. La Ingeniería social [En línea] abril de 2017. [Revisado 17 Septiembre 2017]. Disponible en Http://www.websecurity.es/ingenier-social-introduccion

42. CORPORACIÓN COLOMBIA DIGITAL. Violaciones de seguridad cuestan a las empresas hasta US$500,000 por ataque [2015]. [en línea] [citado el 1 de noviembre, 2018]. Disponible en internet:https://colombiadigital.net/actualidad/noticias/item/8559-violaciones-de-seguridad-cuestan-a-las-empresas-hasta-us-500-000-por-ataque.html

43. Ministerio de Tecnologías de la Información y Comunicaciones. Seguridad y privacidad de la información. Guia No. 13. [En línea]. Bogotá: Mintic. Disponible en http://www.mintic.gov.co/gestionti/615/articles-5482_G13_Evidencia_Digital.pdf

44. REDACCION PASSWORD. ACIS. Colombia. Aumenta en 30% la inversión de las Pymes en ciberseguridad [Internet]. (2018). Disponible en ttp://acis.org.co/portal/content/NoticiaDelSector/aumenta-en-30-la-inversi%C3%B3n-de-las-pymes-en-ciberseguridad

45. Equipo técnico de OEA. Oportunidades y desafíos para las Pymes en el contexto de una mayor adopción de las TIC. [2018]. [en linea]. Disponible en internet: ttp://www.oas.org/es/sms/cicte/docs/white-papers/ESP_Digital_-_white_paper_3.pdf

46. BKF. (2017). Las pymes son las más vulnerables a ataques cibernéticos. [Internet]. Disponible en http://bkf.com.co/pymes-vulnerables-a-ataques-ciberneticos/

47. REPUBLICA DE COLOMBIA. LEY 1273 DE 2009. [2009]. [en línea] [citado el 15 de octubre, 2018]. Disponible en internet: http://www.sic.gov.co/recursos_user/documentos/normatividad/Ley_1273_2009.pdf

48. Hosny Bermeo.Amenaza mundial: de los virus informáticos a los virus biológicos. . (2017). Disponible en http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.8EFEEC8D&lang=es&site=eds-live&scope=site

49. Vilches, L. La construcción del virus informático. (2000). Disponible en http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsbas&AN=edsbas.DF95FE54&lang=es&site=eds-live&scope=site

50. Mazuelos Coello, J. Consideraciones sobre el delito de daños informáticos, en especial sobre la difusión de virus informáticos. Derecho Penal y Criminología: Revista Del Instituto de Ciencias Penales y Criminológicas, (. 85), 29. (2007). Disponible en http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsdnp&AN=edsdnp.3313822ART&lang=es&site=eds-live&scope=site

51. Rodríguez, L. Integración de un sistema de detección de intrusos y un escáner de vulnerabilidades para la detección efectiva de ataques informáticos. (2016). Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.E2AAEA5&lang=es&site=eds-live&scope=site

52. Plaza Torres, P. J. Métodos de ataques informáticos. (2014). Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.759126D2&lang=es&site=eds-live&scope=site

53. Pazmiño Gómez, L. A. Diseño de una metodología para la detección de ataques a infraestructuras informáticas basada en la correlación de eventos. (2017). Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.60845047&lang=es&site=eds-live&scope=site

54. Chávez Zapata, J. P. Simulación y análisis de mecanismos de defensa ante los ataques de denegación de servicios (DoS) en redes de área local convergentes. (2011). Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.5F214F35&lang=es&site=eds-live&scope=site

55. Echaiz, J., & Ardenghi, J. R. Detección spoofing en paquetes IP. (2004). Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.409AA853&lang=es&site=eds-live&scope=site

56. Echaiz, J., & Ardenghi, J. R. Detección spoofing en paquetes IP. (2004). Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.409AA853&lang=es&site=eds-live&scope=site

57. Gómez Vieites, Á. *Seguridad en equipos informáticos*. (2015). Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edselb&AN=edselb.3229330&lang=es&site=eds-live&scope=site

58. Gómez Vieites, Á. *Sistemas seguros de acceso y transmisión de datos*. (2015).Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edselb&AN=edselb.3229662&lang=es&site=eds-live&scope=site

59. GABALDÓN, L. G., & PEREIRA, W. Usurpación de identidad y certificación digital: propuestas para el control del fraude electrónico. (Spanish). *Sociologias*, (20), 164. (2008). Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edo&AN=35781452&lang=es&site=eds-live&scope=site

60. Cabana, P. F. SUPLANTACIÓN DE IDENTIDAD Y USO DE NOMBRE SUPUESTO EN EL COMERCIO TRADICIONAL Y ELECTRÓNICO. (Spanish). *Revista de Derecho Penal y Criminologia*, *3*, 73. (2010). Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edb&AN=61996607&lang=es&site=eds-live&scope=site

61. Acero Martín, F. Los ataques cibernéticos. *Bit*, (. 183), 43. (2010). Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsdnp&AN=edsdnp.3440416ART&lang=es&site=eds-live&scope=site

62. Barros Barrios, P. M., & Aponte Díaz, J. D Sensibilización sobre la necesidad de tomar medidas contra las ciber amenazas. . (2018). Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.E59DFE8B&lang=es&site=eds-live&scope=site

63. Llorens, M. P. Los desafíos del uso de la fuerza en el ciberespacio. *Anuario Mexicano de Derecho Internacional*, *17*, 785–816. (2017). Disponiblee en

https://doi-org.bibliotecavirtual.unad.edu.co/10.22201/iij.24487872e.2017.17.11052

64. García García-Cervigón, D. J. El fraude informático en España e Italia. Tratamiento jurídico-penal y criminológico. (2012). Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.FA0D3072&lang=es&site=eds-live&scope=site

65. Pinsha Defaz, D. F., & Quevedo Zambonino, K. G. Fraude informático, análisis de vulnerabilidad en las empresas del sector industrial de la Provincia de Cotopaxi. (2017). Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.A02ABA6F&lang=es&site=eds-live&scope=site

66. Domaica Maroto, J. M., & Fundación MAPFRE Estudios. *El Control de riesgos en fraudes informáticos*. Spain, Europe: Fundación MAPFRE Estudios. (1997). Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.CFB4B274&lang=es&site=eds-live&scope=site

67. López Grande, C. E. Ingeniería social: el ataque silencioso. (2015).Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.3CA99214&lang=es&site=eds-live&scope=site

68. Caballero Velasco, M. Á., & MAPFRE Global Risks. Ciberdelincuentes: la gran amenaza. (2015). Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.9B3B6735&lang=es&site=eds-live&scope=site

69. Miren Begona Albizuri Romero. El Fraude y la Delincuencia Informática: Un Problema Jurídico y Etico. (2002). Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.85D25B60&lang=es&site=eds-live&scope=site

70. Nardi, J. L., & Maenza, R. R. Voto electrónico, vulnerabilidades y soluciones para evitar ataques. (2018). Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct

=true&db=edsbas&AN=edsbas.4CBDC365&lang=es&site=eds-live&scope=site

71. Análisis y gestión de vulnerabilidades de sistemas informáticos con software libre. (2018). Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.BC05EC5D&lang=es&site=eds-live&scope=site

72. Santos Castañeda, D. M. Análisis y diagnóstico de vulnerabilidades informáticas en la red de datos de la empresa YOUPHONE Cía. Ltda. Utilizando Hacking Ético. (2016). Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.411D4103&lang=es&site=eds-live&scope=site

73. Serrano Gómez, A. Criminología e informática. *Anuario de Derecho Penal y Ciencias Penales*, 437. (1971). Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsdnp&AN=edsdnp.2785116ART&lang=es&site=eds-live&scope=site

74. Faraldo Cabana, P. Los conceptos de manipulación informática y artificio semejante en el delito de estafa informática. *Eguzkilore: Cuaderno Del Instituto Vasco de Criminología*, (. 21), 33. (2007). Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsdnp&AN=edsdnp.3289403ART&lang=es&site=eds-live&scope=site

75. Castro Ospina, S. J. Algunos aspectos dogmáticos de la delincuencia informática. *Derecho Penal y Criminología: Revista Del Instituto de Ciencias Penales y Criminológicas*, (. 85), 107. (2007). Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsdnp&AN=edsdnp.3313831ART&lang=es&site=eds-live&scope=site

76. Tarazona T., C. H. Amenazas informáticas y seguridad de la información. *Derecho Penal y Criminología: Revista Del Instituto de Ciencias Penales y Criminológicas*, (. 84), 137. (2007). Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsdnp&AN=edsdnp.3311853ART&lang=es&site=eds-live&scope=site

RESUMEN ANALITICO ESPECIALIZADO

Información General	
1. Título	Aseguramiento de la seguridad de la información desde el análisis de vulnerabilidades en la infraestructura cibernética de la empresa NOSTRADAMUS S.A.S
2. Autor	MARIA ALEJANDRA HURTADO VANEGAS CHRISTIAN DAVID SIERRA BALCERO
3. Edición	Universidad Nacional Abierta y a Distancia - UNAD
4. Fecha	24 de mayo de 2020
5. Palabras clave	Autenticación, Vulnerabilidad, Amenaza, Delitos informáticos, Virus Informático, Controles de Seguridad, Ataques cibernéticos, Riesgos, Ethical Hacking.

6. Descripción.
Trabajo de grado para optar al título de especialista de seguridad informática de la universidad nacional abierta y a distancia. Se enfoca en realizar la aplicabilidad de un Sistema de gestión de seguridad de la información, identificación de riesgos y amenazas. La temática del trabajo aplicado tiene énfasis en la simulación de ataques y propuesta de aseguramiento. El crecimiento exponencial de amenazas presenta un panorama de riesgos muy elevado para entidades las cuales tengan un nivel bajo de seguridad.

7. 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. Se planeta desarrollar una propuesta y una solución al problema dado, sobre el tema de seguridad informática antes diversas metodologías y aplicativos desarrollados por la empresa Zero Day Ltda especialista en consultoría de soluciones de seguridad de la información.

8. Planteamiento Del Problema
La imagen corporativa de la empresa está siendo haciendo afecta debido a la vulnerabilidad de sus sistemas de información por causa de ataques informáticos que han generado inestabilidad, pérdida de información e impacto reputacional. Actualmente no existen procedimientos definidos de seguridad de la información como tampoco existen controles, políticas y planes de contingencia y continuidad que permitan mitigar un posible evento negativo y continuidad del negocio. A raíz de estos problemas la compañía decidido contratar una consultoría en Seguridad Informática con la empresa Zero Day Ltda, con el fin de recrear estos ataques bajo ambientes controlados simulando la explotación de vulnerabilidades, como primer reconocimiento se identificaron los siguientes ataques.

- Ransomware. “Secuestro de información”
- Denegación de Servicio.
- Infiltración de usuarios no permitidos por medio de elevación de privilegios. “robo de credenciales”
- Inyección SQL. “modificación del sistema”

9. Objetivo General

Presentar una propuesta que garantice el aseguramiento de la información partiendo del análisis de vulnerabilidades existentes en los protocolos de seguridad de la información actuales de la empresa Caso de estudio Nostradamus S.A.S

10. Objetivos Específicos

i. Establecer la metodología a implementar de acuerdo a la norma ISO27001 contemplando todos los activos de la empresa para generar el análisis de riesgos.
ii. Analizar el nivel de madurez del sistema de gestión de seguridad de la compañía identificando su estructura y descripción del proceso de aplicación con alcance a la infraestructura crítica y a la definición de nuevos protocolos de seguridad
iii. Determinar mediante el uso de herramientas de hacking, las posibles vulnerabilidades que posee el sistema de seguridad de la empresa implicada.
iv. Documentar un plan de mejoramiento en temas de normatividad y protocolos de seguridad implementados en la empresa implicada para disminuir el riesgo de sufrir ATAQUES CIBERNETICOS u otros RIESGOS que afecten la seguridad de los sistemas informáticos de la empresa

11. Marco Conceptual Y Teórico

Marco teórico: Existen los riesgos físicos que representan el daño que puede sufrir el hardware y en general las instalaciones del centro o área de cómputo de la empresa.
Por otra parte, todos los riesgos lógicos conocidos han sido creados y siguen siendo creados por personas que tienen de dañar o robar información de los sistemas informáticos empresariales o de los computadores personales de un hogar.

Colombia ataques cibernéticos(2017) informó “Los ataques por ransomware en América Latina han experimentado un aumento anual de 30% entre 2016 y 2017, con 57.512 detecciones en 2016 y 24.110 hasta la fecha en 2017”[4], reveló la compañía Kaspersky al hablar de esta modalidad de ataque, que comúnmente se conoce como un secuestro de información.

Marco conceptual: Las metodologías a utilizar en este proyecto son: La metodología a utilizar por parte de la empresa Zero Day Ltda. Está basada en OSSTMM la cual ofrece una forma ordenada de todo el trabajo a ejecutar. Metodología “OWASP”[8]- Aplicaciones web, el objetivo de esta es recopilar todas

las técnicas probables de intrusión, explicarlas y estar actualizadas, esta metodología nos permite realizar pruebas con un enfoque de caja negra, esto con la finalidad de simular los ataques materializados.

Cuando el ataque busca desestabilizar a la empresa lo más probable es que ataque los sistemas informáticos con el fin de ocasionar una tragedia. Encontramos diferentes vulnerabilidades es por esto que se hará uso de mecanismos/herramientas para detectar y explotar vulnerabilidades. “OSSTMM es un proyecto mantenido por ISECOM - Institute for Security and open methodologies, desarrollado por una comunidad abierta, y sujeto a revisión interdisciplinaria entre pares”8

En esta etapa se homologa una ejecución de test de intrusión, este tiene un carácter intrusivo y se encuentra orientado a identificar y explotar las vulnerabilidades en un entorno controlado. Dentro de la metodología a implementar para este proyecto se divide en diferentes fases.

1. Planeación y especificación.
2. Alcance y riesgos.
3. Levantamiento de información.

4. Escaneos.
5. Revisión de vectores de ataque.
6. Explotación.
7. Análisis de resultados.
8. Generación de informe.

12. Metodología

Para alcanzar los objetivos, se utilizará los conceptos de Investigación Aplicada.

Esto se basará en la realización de nuevas investigaciones en la empresa, identificando las áreas responsables del tratamiento de la información, categorizando el nivel de seguridad de acuerdo al tipo de información que se maneja. Se estima una fase de planificación inicial de 1 mes de duración, en donde el equipo identificara los métodos de investigación necesarios para la ejecución del proyecto. Se realizarán reuniones con las áreas interesadas y establecerá las autorizaciones necesarias para concluir el proyecto.

El proyecto tendrá 1 duración de 1 año en todas sus fases hasta cumplir con el objetivo principal.

Técnicas de recolección de Información:

- Las técnicas que se utilizaran son las siguientes:
- Encuesta
- Entrevista estructurada
- Sondeo de Opinión
- Observación

- Análisis de documentos.

13. Resultado.

Con este proyecto se busca dejar las herramientas suficientes y necesarias para que la empresa pueda hacer un correcto uso de la información que posee, adicionalmente de establecer mecanismos de defensa y fortalecimiento en procedimientos que estén relacionados en temas de información.

14. Fuentes.

a. **Gutiérrez, F. (2011, 02). El Modelado de Amenazas de Seguridad. SEGURIDAD Y AUDITORIA DE SISTEMAS. Obtenido 05, 2018, de http://seguridadenlanube.blogspot.com.co/2011/02/el-modelado-de-amenazas-de-seguridad-es.html**

b. **Bustamante, R., SEGURIDAD EN REDES. Capítulos 1 – 4,(2014) Disponible en http://www.uaeh.edu.mx/docencia/Tesis/icbi/licenciatura/documentos/Seguridad%20en%20redes.pdf**

c. **Tarazona T., C. H. Amenazas informáticas y seguridad de la información. Derecho Penal y Criminología: Revista Del Instituto de Ciencias Penales y Criminológicas, (. 84), 137. (2007). Disponible en http://bibliotecavirtual.unad.edu.co/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edsdnp&AN=edsdnp.3311853ART&lang=es&site=eds-live&scope=site**

d. **Análisis y gestión de vulnerabilidades de sistemas informáticos con software libre. (2018). Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.BC05EC5D&lang=es&site=eds-live&scope=site**

e. **Caballero Velasco, M. Á., & MAPFRE Global Risks. Ciberdelincuentes: la gran amenaza. (2015). Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.9B3B6735&lang=es&site=eds-live&scope=site**

f. **Domaica Maroto, J. M., & Fundación MAPFRE Estudios. *El Control de riesgos en fraudes informáticos*. Spain, Europe: Fundación MAPFRE Estudios. (1997). Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsbas&AN=edsbas.CFB4B274&lang=es&site=eds-live&scope=site**

g. **Acero Martín, F. Los ataques cibernéticos. *Bit*, (. 183), 43. (2010). Disponible en http://search.ebscohost.com.bibliotecavirtual.unad.edu.co/login.aspx?direct=true&db=edsdnp&AN=edsdnp.3440416ART&lang=es&site=eds-live&scope=site**

15. Contenidos.

Este trabajo de grado para optar al título de especialista de seguridad informática de la universidad nacional abierta y a distancia, está estructurado con 4 capítulos que hacen parte fundamental del desarrollo de este trabajo.

16. Conclusiones.

Basados en las buenas prácticas a nivel mundial y tomando como referencia la ISO/IEC 27000, se apoya a la organización para guiarlos en la mejora continua del SGSI e identificar su nivel de madurez. El planteamiento y esquema de seguridad de la información fue trabajado baso la ISO/IEC 27001 y 27002 Anexo A, le fue entregado la matriz de aplicabilidad “SOA” y Plan de tratamiento de riesgos sobre los activos identificados y clasificados como críticos.

Tras la ejecución de este proyecto aplicado se puede concluir que la infraestructura de red propuesta cumple con los objetivos que se diseñaron al inicio del proyecto. Se realiza la implementación del modelo de UTM en un entorno real probando diferentes ataques, monitoreando el tráfico y obteniendo insumos muy importantes para un monitoreo efectivo y que aporte a la seguridad de la compañía no solo a ser proactivos si no a tener un nivel de madurez que apoye a la automatización de los controles y ser reactivos frente a las múltiples amenazas del ciberespacio

Se logró demostrar de una manera rápida y eficiente la configuración e implementación de herramientas de software que ayudan a él complimiento de políticas de seguridad en redes, para este proyecto se utilizaron herramientas como pfsense que permitieron la creación de un servidor proxy entre otras configuraciones, Mediante el uso de Pfsense se logra cumplir con una infraestructura de red básica. Adicionalmente de que es un sistema de bajo consumo, es económico y portable, una opción muy viable para optar por un sistema firewall de alta fidelidad.

ANEXOS

Anexo 1 Propuesta # 1 PfSense Elaborada por Christian D. Sierra B.

Anexo 2 Propuesta # 2 Untangle Elaborada por María Alejandra Hurtado Vanegas.