ELABORACIÓN DE UN PLAN DIRECTOR DE SEGURIDAD (PDS) PARA LA COMPAÑÍA PRONAVICOLA S.A.

GERARDO CABAL ORTIZ

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEDE PALMIRA
AÑO 2023

ELABORACIÓN DE UN PLAN DIRECTOR DE SEGURIDAD (PDS) PARA LA COMPAÑÍA PRONAVICOLA S.A.

GERARDO CABAL ORTIZ

Proyecto de Grado – Proyecto Aplicado presentado para optar por el título de ESPECIALISTA EN SEGURIDAD INFORMATICA

Nombre Director
Joel Carroll

Nombre
Asesor

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA – UNAD
ESCUELA DE CIENCIAS BASICAS, TECNOLOGIA E INGENIERIA - ECBTI
ESPECIALIZACIÓN EN SEGURIDAD INFORMÁTICA
SEDE PALMIRA
AÑO 2023

NOTA DE ACEPTACIÒN

Firma del Presidente de Jurado

Firma del Jurado

Firma del Jurado

Guadalajara de Buga, 4 de agosto de 2023

DEDICATORIA

Dedico este proyecto a mi madre, abuela y abuelo maternos, ya que fueron ellos quienes me cuidaron y educaron para ser una persona con valores, integridad y ética.

A la Universidad Nacional Abierta y a Distancia (UNAD) sede Palmira; gracias a ella he podido prepararme profesionalmente y desarrollar competencias para el impulso y practica de mi carrera.

A todos los tutores y compañeros de estudio, ya que, gracias a su vocación, apoyo y esfuerzo, motivaron mi deseo de seguir adelante con mi elección profesional y su culminación, así como en esta especialización que se convierte en un ladrillo más de mi proyecto de vida[1].

[1] CARVAJAL ARTUNDUAGA, Juan Felipe, *et al.* Diseño de un plan de seguridad informática para el sistema de información del colegio Gimnasio los Pinos. Publicado en enero de 2021. Obtenido en: https://repository.ucc.edu.co/bitstream/20.500.12494/33277/2/2021_Dise%C3%B1o_plan_seguridad.pdf

AGRADECIMIENTOS

Como creyente agradezco primero a Dios por permitir que el camino de mi vida me encuentre en este punto y con todas mis capacidades físicas, emocionales e intelectuales intactas.

Agradezco a mi esposa, Angelica Aricapa, quien ha sido un apoyo fundamental e incondicional en todos los planes y proyectos que me he propuesto.

Agradezco también a Pronavicola S.A., compañía donde laboro hace más de 12 años, ya que, gracias a su confianza en mi trabajo, me han permitido acceder a los recursos y auxilios financieros que hoy se materializan en mi preparación profesional.

Finalmente agradezco a todos los familiares, amigos y colegas que directa o indirectamente siempre han apoyado mi decisión de prepararme profesionalmente[2].

[2] ARÉVALO PADILLA, Leandro Patricio. Plan Director de Ciberseguridad para el municipio de Tulcán – Ecuador. Publicado en 2019. Disponible en: http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2018-19/tfm_AREVALO_PADILLA_LEANDRO_PATRICIO_2018-19.pdf

CONTENIDO

pág.

LISTA DE TABLAS

pág.

LISTA DE FIGURAS

Pág.

LISTA DE CUADROS

pág.

LISTA DE ANEXOS

pág.

GLOSARIO

Términos y Definiciones:

Confidencialidad de la Información: Garantía de que la información estará protegida y no será divulgada sin consentimiento del propietario.

Confidencialidad de la Información: Ambiente sistemático en el cual los colaboradores de una compañía interactúan, intercambian información y colaboran entre sí.

Recurso Tecnológico: Medio que utiliza tecnología para brindar una utilidad, como computadoras, impresoras o también aplicaciones de software.

Trafico de Red: Todos los datos que se mueven dentro de una red.

Auditoria: Evaluación independiente del funcionamiento y actividades de un sistema, área o compañía para establecer su nivel de seguridad, integridad y confiabilidad.

Contraseña: Mecanismo de autenticación en base a caracteres que forman palabra secreta que permitirá acceso a determinados recursos.

Virus Informático: Software diseñado con la intención de dañar, o alterar el funcionamiento de cualquier dispositivo tecnológico sin el consentimiento del propietario.

Antivirus: Programa diseñado para la detección y eliminación de virus informático.

Archivo Adjunto: Archivo enviado de manera conjunta con un correo electrónico.

Unidad de Red: Espacio concedido por el administrador de la red para almacenar o compartir información.

Backup: Procedimiento de copia de respaldo de información relevante en caso de un daño físico o lógico de los datos.

Nube: Termino utilizado para referirse a servicios, espacios o información que se puede acceder o manipular desde internet o una red virtual especifica.

Data Center: Área tecnológica donde se concentra todo el procesamiento y recursos informáticos como servidores, firewall, switches, rack de cableado, rack eléctrico, entre otros.

Ciberseguridad: Hace referencia a todo aquello que involucre la prevención, protección y seguridad de la información, redes, o sistemas ante ataques informáticos o por virus.

RESUMEN

El desarrollo de este trabajo busca diseñar un plan director de ciberseguridad para la compañía Pronavicola S.A. utilizando como base las metodologías de estudio de caso y NIST CSF. Dicho plan consiste en analizar, dimensionar y gestionar el tratamiento de los recursos tecnológicos y los riesgos inherentes a ellos dentro y fuera de la organización.

Para dar inicio a dicho proyecto se debe comenzar con un inventario general a nivel tecnológico, como son los equipos de cómputo, información compartida y reservada, grupo de aplicaciones desarrolladas o contratadas, convenios, proveedores, infraestructura de red, personal, procedimientos o soportes informáticos existentes, sedes, entre otros. Una vez sea establecida dicha información se procede a evaluar en el marco de los pilares fundamentales de seguridad: Integridad, Disponibilidad, Confidencialidad, Autenticidad y Trazabilidad. Acto seguido, se determinan las posibles vulnerabilidades y amenazas que afectan a los recursos mencionados anteriormente junto a su grado de ocurrencia, labor que ayudara a establecer el impacto y riesgo latente sobre los mismos, esto apoyado en la utilización de las cinco áreas de estudio del marco de ciberseguridad NIST CSF: Identificación, protección, detección, respuesta y recuperación.

Haciendo uso del mencionado marco y en base a los pilares de la seguridad se lograran establecer los niveles de riesgo adecuados para definir claramente las acciones de mitigación, control o eliminación del riesgo por amenaza, consiguiendo así las mejoras y evolución de medidas existentes, el diseño y desarrollo de otras inexistentes, un procedimiento claro, sustentable y medible para la administración y

gestión TI y la elaboración de nuevos planes de seguridad puestos a disposición de la compañía Pronavicola S.A. para su futura implementación.[3]

.

[3] MONTERO VALENCIA, Jessica Alexandra. Desarrollo del Plan Director de Seguridad para la Asociación APSA. Publicado en septiembre de 2019. Disponible en: https://core.ac.uk/download/pdf/237118547.pdf

ABSTRACT

The development of this work seeks to design a cybersecurity master plan for the company Pronavicola S.A. using as a basis the case study methodologies and NIST CSF. This plan consists of analyzing, dimensioning and managing the treatment of technological resources and the risks inherent to them inside and outside the organization.

To start this project, a general inventory must be started at a technological level, such as computer equipment, shared and reserved information, group of applications developed or contracted, agreements, suppliers, network infrastructure, personnel, procedures or computer supports. existing offices, among others. Once this information is established, it is evaluated within the framework of the fundamental pillars of security: Integrity, Availability, Confidentiality, Authenticity and Traceability. Then, the possible vulnerabilities and threats that affect the aforementioned resources are determined along with their degree of occurrence, work that will help to establish the impact and latent risk on them, this supported by the use of the five study areas of the NIST CSF Cybersecurity Framework: Identification, Protection, Detection, Response, and Recovery.

Making use of the aforementioned framework and based on the security pillars, it will be possible to establish the appropriate risk levels to clearly define the mitigation, control or elimination actions of the risk by threat, thus achieving the improvements and evolution of existing measures, the design and development of other non-existent ones, a clear, sustainable and measurable procedure for IT administration and management and the elaboration of new security plans made available to the company Pronavicola SA for future implementation.

1. INTRODUCCIÓN

En toda compañía es importante tener un Sistema de Gestión de la Seguridad de la Información (SGSI) o en su defecto un Plan Director de Seguridad (PDS), el cual se resume en una serie de controles y políticas de administración y seguridad de la información, el cual se basa en estándares internacionales y marcos de referencia ampliamente probados y retroalimentados.

Debido a que las organizaciones cada día necesitan elevar los niveles de protección de sus datos, y activos informáticos, además las exigencias de tipo legal y regulatorio, es de vital importancia establecer planes de seguridad ajustados y acordes a las necesidades de las compañías para mantener los procesos que se gestionan al interior y exterior de las mismas bajo los pilares de la seguridad informática, integridad, confidencialidad y disponibilidad.

2. DEFINICIÓN DEL PROBLEMA

2.1. ANTECEDENTES DEL PROBLEMA

En años anteriores la compañía a logrado identificar varios ataques producto de ataques ***phishing***, el cual mediante correo electrónico fraudulento pretende redirigir a la víctima a portales web falsos donde pueda recopilar información sensible o también pidiendo responder a dichos correos diligenciando algún tipo de información para evitar sanciones.[4] También se han identificado infecciones de virus de tipo ***malware***, estos pueden ingresar provenientes de descargas o el uso de memorias USB infectadas, los cuales en su mayoría han sido contenidos y eliminados con el software antivirus Kaspersky, no sin antes afectar algunos archivos y entorpecer el correcto funcionamiento de los equipos.[5]

Recientemente el equipo IT de Pronavicola pudo identificar por medio de su firewall Fortigate y FortiMail y por las incidencias informadas por los usuarios que varias cuentas de correo de la compañía estaban enviando correo ***spam*** o ***phishing*** a otros remitentes, comportamiento que lógicamente puso en alerta al equipo informático, que luego de un par de días de investigación y seguimiento (acompañados de un experto en seguridad y Fortinet) pudo eliminar dicho virus y ajustar ciertas configuraciones.

A pesar de que el área IT en apoyo con soporte (en ocasiones contratado por las horas de soporte inmediato) ha logrado solucionar dichos inconvenientes sin mayores pérdidas, la importancia que revisten dichos ataques no son

[4] Panda. Phishing. Consultado el 30 de octubre de 2021. Obtenido de: https://www.pandasecurity.com/es/security-info/phishing/

[5] Malwarebyes. Malware. Consultado el 30 de octubre de 2021. Obtenido de: https://es.malwarebytes.com/malware/

documentados ni registrados para tener dichos antecedentes en consideración futura y, por lo tanto, tampoco han sido motivo de revisión de las políticas de seguridad establecidas para su afinamiento.

2.2. FORMULACIÓN DEL PROBLEMA

Según lo han establecido diferentes universidades, entre ellas el MIT, se han presentado muchos ataques y desastres de ciberseguridad una vez se reveló la existencia de problemas en miles de microchips, dichos dispositivos presentaron grandes volúmenes de filtración de información y ataques por virus que interrumpen el funcionamiento de las computadoras o el secuestro de las mismas, el famoso ataque Ransomware.

En vista de dichos descubrimientos y la llegada de la pandemia, el incremento exponencial de ataques no se hizo esperar, aprovechando el cambio a escenarios virtuales de trabajo producto del aislamiento preventivo, el desconocimiento de la mayoría de las personas en buenas prácticas de ciberseguridad y la ausencia de un PDS adecuado para mitigar dichas problemáticas.

Las estrategias de ciberseguridad pasaron a ser un objetivo de prioridad alta para las organizaciones y los equipos de TI o seguridad informática, ya que la mayoría de las compañías están colocando cada vez más su Core de comunicaciones, servidores, aplicaciones y contingencias en la web (nube), por lo tanto, es vital establecer estrategias para enfrentar los mencionados riesgos cibernéticos, además de otros mundialmente conocidos como dispositivos de consumo o el internet de las cosas.[6]

[6] CARVAJAL ARTUNDUAGA, Juan Felipe, *et al.* Diseño de un plan de seguridad informática para el sistema de información del colegio Gimnasio los Pinos. Publicado en enero de 2021. Disponible en: https://repository.ucc.edu.co/bitstream/20.500.12494/33277/2/2021_Dise%C3%B1o_plan_seguridad.pdf

En la actualidad la compañía Pronavicola S.A. requiere un análisis y auditoria del estado de sus políticas, procedimientos y Core de ciberseguridad, ya que dichas herramientas y el manejo de las mismas no llevan una correcta administración en términos de gestión y trazabilidad.

Existen ciertas políticas y procedimientos de las cuales no se tiene claridad y control adecuado ni medible, además de un sistema de seguridad perimetral (Fortigate, FortiMail, FortiAuthenticator y FortiVoice) los cuales garantizan un buen nivel de ciberseguridad y protección de la red corporativa, pero requieren de una reorganización en su configuración, procedimiento que el equipo TI desconoce pues no cuenta con personal experto en la solución.

2.3. PREGUNTA PROBLEMA DE INVESTIGACIÓN

¿Elaborar un Plan Director de Seguridad para la compañía Pronavicola S.A., garantizará la existencia de Integridad, Disponibilidad, Confidencialidad, Autenticidad y Trazabilidad de la información y recursos tecnológicos?[7]

[7] CARVAJAL ARTUNDUAGA, Juan Felipe, *et al.* Diseño de un plan de seguridad informática para el sistema de información del colegio Gimnasio los Pinos. Publicado en enero de 2021. Disponible en: https://repository.ucc.edu.co/bitstream/20.500.12494/33277/2/2021_Dise%C3%B1o_plan_seguridad.pdf

3. JUSTIFICACIÓN

Un área TI que no conozca ni aplique a plenitud medidas de ciberseguridad está expuesta a perdidas o daños significativos a la información.

Como es bien sabido en el campo de la seguridad informática en las empresas, es primordial garantizar los tres pilares fundamentales de la SI, integridad, disponibilidad y confidencialidad, tarea que solo se puede lograr implementando unas buenas prácticas en seguridad y estableciendo los límites y alcance de los recursos tecnológicos para tal fin.

Una buena práctica para cualquier CEO es establecer un PDS ceñido a las necesidades y acompañado de unas buenas políticas y proyectos de implementación que permitan una atmosfera de seguridad y monitoreo de la gestión del área TI y la ciberseguridad confiable, al igual que un plan de capacitación constante del equipo de ingenieros dispuesto a tan vital tarea.

La realización de este proyecto no busca otra cosa que no sea proponer y desarrollar estrategias que garanticen la protección de la información y los recursos tecnológicos mediante un plan que involucre a todos los colaboradores y brinde herramientas útiles a los profesionales en TI para una gestión soportada en marcos y metodologías plenamente respaldadas y corroboradas, además de el gran beneficio que traerá para la compañía Pronavicola S.A. pues podrá posteriormente implementar todos los proyectos y mejoras que se elaboren.[8]

[8] ALFARO VIANA, Ivan Andrés, *et al*. Diseño del plan de seguridad informática del sistema de seguridad misional de la procuraduría general de la nación. Publicado el 1 de marzo de 2016. Disponible en: http://polux.unipiloto.edu.co:8080/00003023.pdf

4. OBJETIVOS

4.1. OBJETIVOS GENERAL

Elaborar un Plan Director de Seguridad (PDS) en base a los pilares de la seguridad informática y que garantice la adecuada administración, gestión y mitigación de riesgos informáticos de la compañía.[9]

4.2. OBJETIVOS ESPECÍFICOS

- Examinar las políticas y prácticas actuales en busca de vulnerabilidades latentes utilizando como base el marco de metodología de NIST CSF.
- Establecer políticas de seguridad claras y renovadas que se adecuen a la infraestructura de red y los mecanismos de seguridad existentes, así como la reconfiguración de la solución Fortinet actual.
- Desarrollar proyectos de ciberseguridad y mecanismos de capacitación entre los colaboradores de la compañía para hacerles partícipes de la iniciativa.[10].

[9] VARGAS LEÓN, Edwin, *et al*. Diseño del plan de seguridad informática del sistema de seguridad misional de la procuraduría general de la nación. Publicado el 1 de marzo de 2016. Disponible en: http://polux.unipiloto.edu.co:8080/00003023.pdf

[10] ARÉVALO PADILLA, Leandro Patricio. Plan Director de Ciberseguridad para el municipio de Tulcán – Ecuador. Publicado en 2019. Disponible en: http://www.dit.upm.es/~posgrado/doc/TFM/TFMs2018-19/tfm_AREVALO_PADILLA_LEANDRO_PATRICIO_2018-19.pdf

5. MARCO REFERNCIAL

5.1. MARCO TEÓRICO

5.1.1. *Plan Director de Seguridad – PDS:*

Agrupación de proyectos encaminados a potenciar y garantizar la SI de cualquier compañía. Dicho plan estará acompañado de buenas prácticas de seguridad y un alcance proyectado, lo cual traerá beneficios significativos en el descubrimiento de áreas más vulnerables, riesgos de posible ocurrencia y guías de implementación de medidas para la SI.

Un PDS es entonces un grupo de proyectos técnicos, organizativos e incluso legales que serán llevados a cabo previo al análisis detallado del funcionamiento de la compañía, es por ello que un PDS de estar siempre alineado con los objetivos de la organización y contar con el respaldo y aprobación de la organización para concientizar a todos los colaboradores de los riesgos de ciberseguridad a los que se está expuesto todo el tiempo.

Las metas principales de un PDS deben ser:

- Evolución del ambiente actual, con lo cual se podrá observar posibles riesgos para la compañía.
- Identificar las áreas con mayor riesgo para establecer gravedad, impacto y probable ocurrencia.
- Implantación de proyectos y medias de ciberseguridad que mitiguen el riesgo aceptable y residual.
- Monitoreo y trazabilidad de las medidas implantadas y sus resultados para

determinar su nivel de éxito.

- Procesos de mejora continua, evaluando y analizando periódicamente la eficiencia y eficacia de las medidas.[11]

5.1.2. *¿Cómo se debe implementar un Plan Director de Seguridad?*

Se deben llevar a cabo seis fases cíclicas, esto debido a que el un PDS está diseñado bajo la premisa de mejora continua, por lo tanto, cuando cada fase se culmine se habrá regresado al inicio.

Teniendo en cuenta un análisis previo de la organización y sus características se establecerá el tiempo estimado para dicho ciclo.

- **Fase uno (Conocer la situación actual)**: Momento de mayor relevancia, ya que debe reunir a todos los actores que tendrán participación del plan, junto a las directivas que apoyaran y respaldaran el proyecto garantizando los recursos necesarios y su alineación con los objetivos estratégicos de la compañía.

  Se debe delimitar el alcance del PDS, responsables de gestionar activos, valoración general, análisis de cumplimiento, objetivos del plan y análisis de seguridad y riesgos.
- **Fase dos (Conocer la estrategia de la compañía)**: Conocer los proyectos que están en proceso en la compañía y los ya planificados hacia el futuro, sus alcances, cambios o mejoras que realizarían y también determinar cuál será la participación y futuro del área TI en dichas iniciativas, si crecerá o será divido.
- **Fase tres (Definición de proyectos e iniciativas)**: elaborar y determinar las

[11] Ayudaley. Plan director de seguridad ¿Cómo implantarlo en tu empresa?. Consultado el 15 de octubre de 2021. Disponible en: https://ayudaleyprotecciondatos.es/2020/10/30/plan-director-de-seguridad/

mejores medidas en busca del nivel y calidad esperados de seguridad informática.

- **Fase cuatro (Clasificacion y Priorización de proyectos para realizar)**: Determinar una clasificación y orden de los proyectos escogidos y que estarán incluidos en el PDS, estimando además su costo, tiempo de desarrollo y tiempo estimado de implementación, corto, mediano o largo plazo.
- **Fase cinco (Aprobación del PDS)**: Serán las directivas de la compañía quienes después de analizar y realizar las correcciones pertinentes darán visto bueno para su implementación.
- **Fase seis (Puesta en marcha)**: Se da inicio a la implementación.

Es importante resaltar que todos estos puntos llevan consigo una serie de actividades y tareas que serán presentadas y llevadas a cabo al momento de realizar el levantamiento de la información como tal.[12]

5.1.3. *Auditoria de Seguridad de la Información:*

Una auditoria o análisis interno de SI, permite descubrir y documentar vulnerabilidades existentes o con posibilidad de ocurrencia; dichas vulnerabilidades pueden estar presentes en diferentes tipos de dispositivos de la red corporativa, tales como servidores, equipos de usuarios, redes wifi, entre otros.

Una auditoria es beneficiosa para cualquier empresa ya que permite mejoras en los controles internos, descubre fallos y debilidades de la compañía en este aspecto, ya sea por omisión o desconocimiento. También puede detectar si se están realizando fraudes o robos de información al interior de la compañía, fortalece la

[12] RAMIREZ, Helena. ¿Qué es y como implantar un plan director de seguridad en una empresa?. Publicado el 23 de septiembre de 2020. Disponible en: https://protecciondatos-lopd.com/empresas/plan-director-de-seguridad/

seguridad en términos de comportamiento en la web, con el correo electrónico o demás conexiones externas y así mismo a controlar y monitorear accesos de tipo físico o virtual.[13]

Existen también diferentes tipos de auditorías como son:

- **Auditoría Interna o Externa**: realizadas por personal de la compañía o ajeno a ella, aunque también se pueden realizar en conjunto.
- **Auditoria Técnica**: Enfocadas en un punto, área o medidas específicas de las cuales se quiere determinar su rendimiento.
- **Auditoria por Objetivo**: Similares a las técnicas, enfocadas por lo general en: sitios web o eCommerce en busca de vulnerabilidades.
- **Auditorias Forenses**: Suelen darse posterior a un ataque para entender porque sucedido, su alcance y perpetrador, porque no se puedo evitar, entre otros.
- **Auditorias de Redes**: Se en el funcionamiento y seguridad de firewall, wifi, VPN, antivirus, etc.
- **Auditorias de Control de Acceso**: enfocadas en los dispositivos se acceso como lectores biométricos, cámaras de seguridad, etc.
- **Auditorias Ethical Hacking**: Fundamentales para realizar testing e intrusing, utilizando programas como Maltego y herramientas como Kali Linux permiten revelar diferentes tipos de vulnerabilidades que no suelen ser consideradas dentro de auditorías normales.

Por su naturaleza metodológica también se compone de fases para su ejecución, como son:

[13] Ealde. Consejos para hacer una auditoria de seguridad informática para evitar riesgos digitales. Publicado el 8 de abril de 2021. Disponible en: https://www.ealde.es/auditoria-de-seguridad-informatica/

- **Objetivos y Planificación**: Definir claramente el objetivo específico que se busca alcanzar y la manera como este se llevara a cabo paso a paso bajo un cronograma de actividades.
- **Recopilar información**: Se recolecta toda la información posible para determinar la operación de objetivo auditable y se procede a utilizar mecanismos como entrevistas, revisión documental de procedimientos, evaluación de software y hardware y pruebas tipo Pentest.
- **Análisis de información**: Con todo lo anteriormente recolectado se procede a revisar los resultados y vulnerabilidades en base al objetivo planteado.
- **Informe de Auditoría**: Por último, se realiza un informe al detalle, con los resultados de cada fase, resultados globales, recomendaciones y planes de acción, el estado previo y el estado actual luego de dicha auditoria.[14]

Cabe anotar que en el desarrollo de un PDS también existen técnicas de auditoría de seguridad informática, sin embargo, pueden ser apoyadas con técnicas de auditoría interna, por objetivo y de Ethical Hacking para expandir el panorama de evaluación.

5.1.4. *GAP 27001:*

También conocido como análisis de brecha, haciendo alusión al termino como la resolución de “donde se está” y “donde se quiere estar”.

Se trata de una metodología para determinar el rendimiento de las aplicaciones de software y establecer si cumplen con las necesidades de la compañía y el nivel de

[14] Ambit. ¿Qué es una auditoria de seguridad informática? Tipos y fases. Publicado el 9 de febrero de 2021. Disponible en: https://www.ambit-bst.com/blog/qu%C3%A9-es-una-auditor%C3%ADa-de-seguridad-inform%C3%A1tica-tipos-y-fases

madurez respecto a los controles de la norma. Es conocido también como análisis de necesidades y permite además entender cuáles son los recursos necesarios para alcanzar el rendimiento esperado.[15]

Existen diferentes herramientas y técnicas para realizar un análisis, como FODA y otras, pero como todo marco teórico, se requieren de ciertos pasos para realizar exitosamente dicho análisis:

- **Paso uno (Identificación del Área)**: Tener un enfoque claro es fundamental. Se debe ser especifico con el objeto a evaluar y lo que se pretende analizar.
- **Paso dos (Identificación de Metas)**: Con el pleno conocimiento del enfoque y área a evaluar, diseñar los objetivos que se persiguen, los cuales deben ser sumamente aterrizados y alineados con los objetivos estratégicos de la compañía.
- **Paso tres (Reconocer el estado actual)**: Revisión actual de la compañía, su momento en el mercado, actividades y todo aquello que presente un panorama claro.
- **Paso cuarto (Determinar proyección futura)**: Basado en las metas planteadas y la información recopilada se deben definir los parámetros que permitirán alcanzar victorias tempranas y planes futuros.
- **Paso cinco (Comprensión de brechas en ambos estados)**: Con la visión clara del estado actual y el esperado (futuro) se puede evidenciar la "brecha" que impide el cumplimiento de los objetivos.

  Para cerrar dicha brecha se debe entender las desventajas existentes con relación a lo esperado en el futuro, de esta forma hacerse preguntas sobre la

[15] asesorías. ¿Cómo hacer un análisis GAP o análisis de brechas? Con ejemplos. Consultado el 10 de octubre de octubre de 2021. Disponible en: https://asesorias.com/empresas/modelos-plantillas/analisis-gap/

forma como se está buscando alcanzar el éxito en los proyectos planificados, si se están utilizando las mejores estrategias y otros cuestionamientos que ayudaran a encontrar los mecanismos para disminuir las mencionadas brechas.[16]

5.1.5. *Política de Seguridad informática:*

Las políticas establecen el correcto uso y recomendaciones que todos los usuarios de una compañía deben tener sobre los recursos y activos tecnológicos de una organización, por ello es de vital importancia identificar cada aspecto relacionado con SI dentro de la red corporativa y la gestión del área TI para diseñar una política bien delimitada que involucre a todos los usuarios en cuanto a deberes y responsabilidades para mitigar al máximo cualquier vulnerabilidad o ciberataque.

Políticas se refiere a un conjunto de normas que garantizan la existencia de los tres pilares fundamentales de la SI y la mitigación de riesgos que puedan entorpecer las actividades de la organización.[17]

Algunas políticas y procedimientos:

- **Buenas Prácticas**: Documento anexo a la hoja de vida del empleado en el cual se estipulen el uso adecuado y esperado que se debe dar a los recursos tecnológicos, precauciones y recomendaciones respecto a contraseñas y uso en general.
- **Control de Acceso**: Medidas establecidas de permisos a determinados

[16] QuestionPro. ¿Qué es el análisis de brechas o GAP?. Consultado el 10 de octubre de 2021. Disponible en: https://www.questionpro.com/blog/es/analisis-de-brechas/

[17] Disete Comunicaciones. Qué son las políticas de seguridad informática y por que tu empresa debe tener una. Consultado el 10 de octubre de 2021. Disponible en: https://disete.com/que-son-las-politicas-de-seguridad-informatica-y-por-que-tu-empresa-debe-tener-una/

lugares y/o aplicaciones o información sensible, de esta forma se establecen controles físicos, los cuales establecen mecanismos de seguridad como son cámaras, alarmas, barreras, dispositivos de comprobación biométrica, facial, etc. Y los controles lógicos serian configuraciones sobre la información como tal, como por ejemplo limitar el acceso a un archivo para que solo sea de lectura en determinados usuarios.

- **Gestion de Usuarios**: procedimiento con instrucciones claras para la creación modificación o eliminación de los usuarios de la red, recopilación de los accesos, aplicaciones y permisos que posee, roles y responsabilidades.
- **Procedimiento para Clasificar y Tratar la Información**: Discriminar la información de acuerdo al valor, nivel de sensibilidad, características legales y criticidad, así como las medidas adoptadas para su manejo.
- **Gestion de Incidentes**: Procedimiento donde se indique la notificación, y respuesta de incidentes, un plan de contingencia que detalle los pasos a seguir en caso de ser detectada una incidencia.
- **Gestion de Activos**: Mecanismo por el cual se recopila y filtra dicha información.
- **Procedimientos de Backup**: Instructivo de cómo, dónde y con que aplicación se realiza copias de seguridad de la información, selección de los datos, periodicidad de la copia, pruebas de recuperación, responsables y tareas adicionales.[18]

5.2. MARCO CIENTÍFICO

Es bien sabido que toda investigación que tenga como objetivo medir, solucionar o plantear una estrategia resolutiva a cualquier problema debe construirse bajo el método científico, postulado que propende por el desarrollo del conocimiento y la

[18] Unir. Claves de las políticas de seguridad informática. Publicado el 14 de mayo de 2020. Disponible en: https://www.unir.net/ingenieria/revista/politicas-seguridad-informatica/

demostración irrefutable en base a las pruebas razonables generadas desde los principios naturales y lógicos de observar, experimentar, formular, analizar y replantear una hipótesis previa o derivada del objeto de estudio.[19]

Indudablemente la seguridad informática está ligada al método científico, ya que para sostener que una red corporativa o un equipo de cómputo son seguros es necesario confrontar mediante pruebas, análisis o software que dicha afirmación está basada en datos creíbles y medibles, es decir, la idea de que una infraestructura es segura por tener ciertos equipos, aplicaciones y políticas de seguridad debe ser corroborada para poder decir que dicha red es "segura", además de arrojar un porcentaje o nivel estimado de seguridad al someterse a cualquier auditoria o prueba de vulnerabilidades.

Ahora bien, para poder sustentar y hablar de hechos científicos concretos, el método científico utiliza dos pilares que son: Reproducibilidad y Refutabilidad; el primer pilar requiere de pruebas o experimentos que al ser realizados por otro analista o investigador le permitan ver información o comportamientos consecuentes con el objeto y problema de estudio y así verificar el estado del mismo en relación a lo que se pretende exponer y solucionar. En el caso del proyecto aplicado que aquí se presenta puede reflejarse y reproducirse mediante el método MAGERIT, vital para el análisis de riesgos y para establecer el Perfil Actual o estado de seguridad de la compañía y todos los recursos físicos y tecnológicos que están en peligro de sufrir un ciberataque severo.

El pilar de Refutabilidad por su parte es más directo y practico, ya que basa su legitimidad en un análisis deductivo que permita revelar la falsedad de una

[19] MONCAYO, Carolina. El método científico y el hacking ético. Publicado el 19 de septiembre de 2016. Obtenido de: https://incp.org.co/el-metodo-cientifico-y-el-hacking-etico/

proposición absoluta al demostrar por medio de la experimentación que una situación o tesis observada es falsa o equivocada.

Para entender mejor el anterior párrafo dentro del contexto del actual proyecto aplicado es importante recordar la pregunta problema de investigación planteada en la página 22 del presente documento, los resultados del análisis de riesgos (aplicación de los métodos MAGERIT y GAP), el estado actual del Appliance Fortinet y las políticas o procedimientos de seguridad establecidos para luego preguntarse *¿Si se toma al azar cualquier ordenador o dispositivo inteligente para ser utilizado dentro o hacia la red corporativa y se somete a un test de seguridad, pasará los análisis y estará libre de vulnerabilidades explotables*? Si al hacer dichas pruebas la respuesta es "NO" entonces la hipótesis de presunta seguridad es falsa y de este modo se demuestra la necesidad de correctivos y proyectos de ciberseguridad que luego de ser aplicados deberán responder afirmativamente a dicha pregunta, y además, establecer un estatus alto de seguridad y mitigación de vulnerabilidades así como la posibilidad de que el proyecto sea replicable en otras áreas de la compañía o en la consecución de otros objetivos, situación que estará siendo descrita, analizada, planteada y desarrollada (*en la medida que el alcance del proyecto y las directrices de la compañía lo apliquen*) a partir de la página 44 del texto.

5.3. MARCO TECNOLÓGICO

A continuación, se describen los métodos y herramientas de software necesarias para la implementación del PDS planteado en este proyecto.

Entendiendo que el proyecto parte de un análisis de riesgos, análisis de brechas de seguridad y el diseño de pasos estratégicos basados en un marco metodológico de investigación que permite rediseñar y fortalecer los mecanismos de SI de la compañía es importante señalar que la mayoría del proyecto es realizado con

procedimientos escritos siguiendo los lineamientos e indicaciones de dichas metodologías, basados en la observación, datos previos sobre los recursos tecnológicos (*Inventario de equipos, infraestructura de red, licenciamiento, software ERP, software ofimático, formatos de TI, etc.*) y el acceso a la configuración del Appliance de seguridad perimetral Fortinet de la compañía, así como el paquete de office y algunas herramientas de colaboración que serán útiles en los proyectos de mejora planteados en el documento.

Como se hace mención anteriormente, la compañía utiliza aplicaciones tecnologías basadas en Microsoft, desde servidores hasta equipos de usuarios finales, al igual que aplicaciones de antivirus y protección remota como Kaspersky y FortiAuthenticator, adicional a esto un sistema de Firewall avanzado como FortiGate para la administración y seguridad de la red corporativa, dichas herramientas presentan las siguientes características:

5.3.1. *Kaspersky Endpoint Security:*

Compañía fundada en 1997 por el experto en Seguridad informática Eugene Kaspersky quien también es su CEO y presidente, desde su sede principal ubicada en el Reino Unido esta empresa a desarrollado un software de alta calidad y confiabilidad que ha estado brindando protección frente a virus informáticos a mas de 400 millones de usuarios y 240.000 compañías alrededor del mundo por más de 26 años.[20]

A lo largo de su expansión internacional Kaspersky se ha convertido en líder, promotor y colaborador de diferentes iniciativas mundiales conjuntas para la mitigación de riesgos y el descubrimiento de nuevos ataques y variantes

[20] Kaspersky. Acerca de nosotros. Consultado el 20 de marzo de 2023. Obtenido de: https://latam.kaspersky.com/about

cibernéticas, además, su grado de efectividad a permitido que sus productos se utilicen en organizaciones gubernamentales e incluso de seguridad internacional como la Interpol.

Pronavicola cuenta con más de 130 licencias Kaspersky Endpoint Security y una consola de administración instalada en el Servidor BI con la cual realiza gestión de dichas licencias y sus actualizaciones, herramienta de vigilancia sumamente útil para el establecimiento de políticas y excepciones de seguridad, así como rutinas de análisis diarias, instalación remota de la aplicación mediante el agente Kaspersky (*Utilidad instalada en la mayoría de equipos de la compañía al momento de ser unidos al dominio*) alertas de seguridad en los diferentes equipos, control RDP desde la consola, entre otras.

Actualmente, Kaspersky es y ha sido una ayuda fundamental para la compañía en la mitigación y protección de los equipos de usuarios finales principalmente, siendo en ocasiones el primer filtro de seguridad y permitiendo el descubrimiento de diferentes ataques y comportamientos sospechosos a lo largo de los años en la empresa, así como apoyo crucial en la aplicación de las políticas de seguridad y uso de dispositivos portátiles como los PENDRIVE y demás.

5.3.2. *FortiAthenticator:*

Herramienta complementaria en el Appliance Fortinet para la gestión de identidades y conexiones remotas seguras. FortiAthenticator permite garantizar que solo usuarios autorizados puedan conectarse de forma segura a la red corporativa y acceder a los recursos compartidos a los cuales tenga permisos y privilegios específicos[21].

[21] Quanti. ¿Cómo funciona FortiAuthenticator? Publicado el 23 de junio de 2021. Obtenido de: https://quanti.com.mx/articulos/como-funciona-fortiauthenticator/#:~:text=Esto%20quiere%20decir%20que%20FortiAuthenticator,conectados%20localmente%20o%20con%20cable.

Para lograr dicha seguridad la herramienta utiliza autenticación de doble factor (*requiere licenciamiento*) que puede ser configurado para generar claves dinámicas vía mensaje de texto, correo o desde una App, además, por medio del directorio activo de la compañía establecer una conexión VPN perfectamente escalable y limpia.

Dicha herramienta puede ser instalada de forma "física" en un servidor local o de forma virtual en formato MV, se trata una instalación Linux diseñada para tal fin y fácilmente configurable gracias a diferentes manuales y recomendaciones que pueden encontrarse en el portal de Fortinet o en la web.

Para que la herramienta pueda ser utilizada correctamente es necesario que este corriendo dentro de la red corporativa (*LAN que determine el área IT*) y que se configure para establecer comunicación con el directorio activo de la compañía por medio de comunicación cifrada LDAPS y Kerberos, servicios y protocolos diseñados para dicha interlocución, permitiendo así la comprobación y autorización de permisos y políticas establecidas para los usuarios desde el dominio.[22]

Actualmente, Pronavicola cuenta con FortiAthenticator en su modalidad Virtual desde una distribución de Linux CentOS, este se encuentra unido a la red de servidores de la compañía los cuales son en su mayoría máquinas virtuales administradas desde una plataforma VMWARE. Se adquieren 40 licencias para ser utilizadas mediante el método de autenticación de doble factor FortiToken, esto gracias a la generación de un código QR que se envía desde la consola FortiAuthenticator vía email al usuario que tendrá acceso remoto por VPN, dicho usuario deberá instalar en su Smartphone la App FortiToken Mobile, desde la App

[22] FortiXpert. Blog Técnico Fortinet. Publicado el 25 de enero de 2021. Obtenido de: https://fortixpert.blogspot.com/2021/01/proteccion-sistemas-linux-con.html

leer el código enviado y automáticamente empezara a generar claves dinámicas cada minuto, ahora, la forma de uso es la siguiente: El usuario se conecta a la VPN mediante la aplicación FortiClient instalada previamente en su computadora (*instalación que se realiza principalmente en las computadoras portátiles de la compañía*) y que cuenta con dos direcciones VPN disponibles para todos los usuarios, una vez se conecte utilizando su usuario y contraseña de red actual la aplicación solicitará un código dinámico FortiToken de cuatro o seis dígitos para continuar con el proceso de conexión, el usuario digita el código que este generando actualmente la aplicación FortiToken Mobile y una vez se realice la comprobación satisfactoria del mismo la conexión VPN se establecerá.

Es importante resaltar que para que se realice dicha conexión deben existir políticas de conexión seguras desde el firewall FortiGate y los usuarios estar agregados a un grupo especial creado desde el Directorio Activo y sincronizado con FortiAuthenticator, solo de esta forma se podrá establecer conexión VPN con o sin autenticación de doble factor, privilegio que será determinado y concedido por el área IT.

5.3.3. *Firewall y Seguridad Perimetral*

Antes de hablar de un tipo o clase de Firewall es importante entender y abarcar las diferentes consideraciones inherentes al concepto de seguridad perimetral, el cual es una metodología o grupo de herramientas que permiten blindar y monitorear eficientemente el funcionamiento y seguridad de una red, por tanto, se presentan sus características y precisiones más relevantes.

La seguridad perimetral puede traducirse como la integración de sistemas y herramientas de protección informática que permitan crear una “barrera” o “línea defensiva” para la detección y prevención de ciberataques, dicha protección se alcanza mediante el cifrado y control del flujo de navegación, red e incluso

aplicaciones.[23]

Para tal fin, existen soluciones completas y robustas de ciberseguridad como Fortinet, la cual integra dispositivos y un sistema propio el cual lo posiciona como líder en divulgación de amenazas cibernéticas.

Existen diferentes tipos como son:

- **Seguridad perimetral de infraestructura**: Control de comunicaciones a través de métodos o mecanismos que alerten sobre comportamientos sospechosos, bloqueando inmediatamente todo tipo de flujo de información que cause desconfianza. Utiliza filtros de acceso para determinar servicios internos y externos válidos. Algunas de los productos de ciberseguridad más utilizados para tal fin son los cortafuegos de software o hardware, VPN´s o IPS, todas con funciones de control, cifrado o bloqueo de conexiones sospechosas.[24]
- **Gestion de identidades y control de acceso NAC**: Parte fundamental de la seguridad perimetral, ya que es importante poder tener control sobre los usuarios y sus accesos, hacer una trazabilidad de su comportamiento, entre otras, de allí la importancia de mecanismos como NAC, esto debido a que las compañías ahora deben tener en el radar el rápido crecimiento de dispositivos móviles que acceden en la red corporativa y el riesgo que eso conlleva, por lo tanto, un sistema como este puede denegar el acceso a dispositivos que no cumplan con ciertos criterios, aislarlos en cuarentena y

[23] Accensit. Seguridad perimetral informática: información necesaria. Consultado el 8 de octubre de 2021. Disponible en: https://www.accensit.com/blog/seguridad-perimetral-informatica-informacion-necesaria/

[24] Avansis. Seguridad perimetral tipos y métodos aplicados a cibersegurdiad. Consultado el 11 de octubre de 2021. Disponible en: https://www.avansis.es/sin-categorizar/que-es-seguridad-perimetral/?cn-reloaded=1

limitar sus accesos.[25]

Algunas de sus bondades son: gestión de ciclo de vida de políticas, creación de perfiles, acceso a redes de invitados, verificación de postura de seguridad, respuesta a incidentes e integración bidireccional.

- **Single Sign On**: Permite a los usuarios acceso a diferentes aplicaciones y recursos con solo una cuenta. Resulta muy útil cuando hay diferentes sistemas y aplicaciones que requieren de un usuario y contraseña, de esta forma con SSO se puede acceder a todas con solo iniciar la primera vez. En términos de seguridad es muy eficaz ya que permite identificar sin equivocación a un usuario en dicho ambiente y además cifra todo lo que este sucediendo en dichas sesiones.[26]

5.3.4. *Sistema de Prevención y Detección de Intrusos (IDS/IPS)*

5.3.5. *IDS:*

Sus siglas en ingles traducen “sistema de detección de intrusos” y se trata de un software destinado a la detección de accesos sin autorización en un equipo o red de computadoras, es decir, se limita a dar una alerta del suceso, para luego generar un log informativo del evento, el cual podrá ser analizado por el administrador de infraestructura y red.[27]

Existen varios tipos de IDS como son:

---

[25] Cisco. ¿Qué es el control de acceso a la red?. Consultado el 11 de octubre de 2021. Disponible en: https://www.cisco.com/c/en/us/products/security/what-is-network-access-control-nac.html

[26] Chakray. ¿Qué es el Single sign On (SSO) y para qué sirve?. Consultado el 11 de octubre de 2021. Disponible en: https://www.chakray.com/es/que-es-el-single-sign-on-sso-definicion-caracteristicas-y-ventajas/

[27] CLAVEI. ¿Qué es un IDS o Intrusion Detection System? Publicado el 16 de abril de 2018. Disponible en: https://www.clavei.es/blog/que-es-un-ids-o-intrusion-detection-system/

- **Host IDS**: Monitorea el tráfico en ambas direcciones de un host o equipo definido, también escanea el OS y los procesos corriendo en él, vigilando también modificaciones inusuales en registros o datos y software, incluso puede ayudar a detectar si el equipo está siendo atacado, es decir, solo corre en el sistema donde se instale; muy utilizado en servidores.
- **Network IDS**: Realizan análisis de la red y capturan de tráfico sospechoso; los conocidos sniffer.
- **IDS Basado en firmas**: Vigilan todo el tráfico de red comparándolo con una base de datos de firmas o patrones en busca de software o cambios maliciosos, similar al funcionamiento de un antivirus.

La forma como un IDS detecta el tráfico malicioso es utilizando patrones o firmas en conjunto con una serie de configuraciones y reglas, que, al cumplirse, generan la alarma correspondiente.

Un software IDS muy popular y de licencia open source es **SURICATA**, cuenta con sistema de detección de intrusos de código abierto, es robusto y veloz, fue desarrollado por la Open Information Security. La aplicación es sumamente potente y capaz de realizar detección en tiempo real, prevenir y alertar sobre accesos no autorizados tanto en línea como en la red o sistema interno, cuenta además con módulos para capturar, recopilar, decodificar, detectar y salida, capturando el tráfico que recorre un flujo previo a la decodificación.

Funciona bajo las principales plataformas, Windows, MacOS y Linux.

5.3.6. *IPS:*

Sistema diseñado para prevenir intrusos en un determinado dispositivo de seguridad, que por lo general suele orientarse a redes, por ello realiza monitoreo a

nivel de capa 3 y/o capa 7 del modelo OSI, realizando contingencia en caso de encontrar comportamientos sospechosos o maliciosos.[28]

Su naturaleza es de tipo complementaria junto a otros sistemas de seguridad más avanzados como firewalls y incluso IDS, por ello sus características y diseño se desprenden de estas herramientas, sin embargo, este hecho no le resta importancia en cuento a su operación proactiva y otras bondades, como tomar medidas en base al flujo de tráfico y no sobre direcciones IP o puertos, como es el caso de un firewall.

Su clasificación puede basarse en su método de detección o la tecnología donde se implementa.

Según su Método de Detección:

- **IPS basado en Firmas**: Cuenta con base de datos de firmas con ataques y patrones de seguridad conocidos, dicha información se suma al dispositivo donde se realiza la detección, de esta manera se puede contrastar con lo que detecte para identificar si hay una amenaza y contrarrestarla. Haciendo una analogía, podríamos decir que es un comportamiento similar al de una vacuna.
- **IPS basado en Anomalías o Perfil**: Realiza un análisis basado en indicadores de tráfico para determinar si un comportamiento esta fuera de la rutina normal en un dispositivo o en la red corporativa.
- **IPS basado en Detección "Pote de Miel"**: Se trata de un señuelo, un equipo visiblemente desprotegido pero aislado y controlado, de forma que pueda ser atacado y de esa forma analizar y determinar cómo fue accedido y a partir de ahí, establecer políticas de protección.

[28] INCIBE. ¿Qué son y para qué sirven los SIEM, IDS, e IPS?. Publicado el 3 de septiembre de 2020. Disponible en: https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips

Según su Modelo de Tecnología:

- **IPS basado en Host**: Realiza un monitoreo de todo el comportamiento de un dispositivo, su tráfico de red (cableada o inalámbrica), procesos que se ejecutan, servicios, registro del sistema, archivos, entre otros. Genera de igual manera acciones preventivas o correctivas según detecte anomalías y se suele usar en servidores o sistemas encendidos 24/7.
- **IPS basado en Red**: Monitorea el tráfico de red por segmentos, analizando protocoles de transporte y aplicaciones en busca de un comportamiento malicioso. Su rasgo principal es que monitorea en tiempo real todo el flujo y tráfico de red, por ello suele implementarse junto al Firewall para maximizar su efectividad.

La forma como un IPS funciona se basa en una serie de instrucciones avanzadas que permite monitorear cada bit que se mueve en los paquetes de red; significa que antes de que a un paquete se le permita salir, ha sido inspeccionado y filtrado completamente, al igual que las rutas de destino.

Debido al constante crecimiento de nuevas amenazas en la red, los IPS de nueva generación ahora incluyen monitorización en línea e ininterrumpida, tecnología para reconocer aplicaciones e implementar las políticas de seguridad optimas según las características de la aplicación, conceptos de conciencia e inteligencia artificial para decidir la mejor acción preventiva y correctiva y agilidad de procesamiento y retroalimentación para protegerse ante eventos futuros.

5.3.7. *Firewall*

Conocido también como cortafuegos, es una herramienta diseñada para impedir el acceso de elementos entrantes y salientes de una red, usuarios o la web, esto con

el objetivo de frenar cualquier software o hardware que no se ajuste a las medidas de seguridad establecidas.

Pensemos en el firewall como las llaves o sistema de bloqueo de un vehículo, sin el nuestro automóvil estaría totalmente disponible para que cualquier persona pueda ingresar, manipular todo en su interior y además conducirlo, la pregunta es: ¿nos sentiríamos tranquilos sabiendo que nuestro vehículo puede ser manipulado por cualquiera?

Entonces, el firewall se ubica entre el ordenador y la red a la que se conecta, principalmente internet, vigilando y registrando toda la actividad que se está llevando a cabo y comprobando que el flujo de información es segura y ajustada al criterio de seguridad establecido para decidir si concede o no acceso[29].

Su operación consiste en saber diferenciar una conexión segura y una riesgosa, utilizando mecanismos como:

- **Políticas de Firewall**: Por medio de la dirección IP u otro elemento de identificación de equipo, se filtra y restringe cualquier conexión que no pertenezca al rango o segmento de red local, ocultando de esta manera todos los recursos al interior de la misma de forma que no sea visible al exterior.
- **Filtrado Contenido**: Utilizando las llamadas “reglas de exclusión” el firewall identifica que conexiones son potencialmente riesgosas y cuales son permitidas por el administrador.
- **Operaciones de Anti-Malware**: Hoy en día los cortafuegos incorporan definiciones de malware y diferentes variantes de virus que han sido

[29] PEREZ, Anna. Tipos de firewall: características y recomendaciones de uso. Publicado el 7 de junio de 2021. Obtenido de: https://www.obsbusiness.school/blog/tipos-de-firewall-caracteristicas-y-recomendaciones-de-uso

liberadas por muchas aplicaciones de protección, de esta forma se amplía la protección ante dichas amenazas.

- **Servicios DPI**: Esta sigla significa (Deep Package Inspection) o también inspección profunda de paquetes, lo cual funciona como una segunda verificación más exhaustiva de los datos en busca de contenido malicioso.

5.3.8. *Clases de Firewall Existentes:*

- **Firewall de filtrado o Inspección de paquetes**: El menos seguro, ya que su labor consiste en abrir o cerrar determinados puertos que el administrador establezca para el flujo de tráfico, pero no inspecciona ni tampoco identifica paquetes seguros de inseguros.
- **Firewall de Proxy**: funciona como mediador entre una red externa y el equipo al que se conecta, colocándose en medio para impedir el intercambio libre de paquetes, entonces, los analiza y una vez considera que son seguros permite el paso.
- **Firewall de última generación**: Combinan funcionalidades de los cortafuegos típicos con software para prevenir intrusos, utilizando técnicas avanzadas contra malware y otros virus.
- **Firewall de aplicación**: Controla completamente los movimientos de un software o servicio específico, de esta forma puede administrarse para restringir o permitir el acceso a un recurso de red para un grupo de usuarios o hacia un equipo en particular.

5.3.9. *Tipos de Cortafuego:*

- **Cortafuego de hardware**: Se instala comúnmente luego del router que concede conexión a internet, de esta forma se filtra y controla todos los paquetes que utilizaran los usuarios, protegiendo la información y los equipos de la red.

- **Cortafuego de software**: Normalmente viene inherente al sistema operativo de los ordenadores, con una configuración por defecto y lógicamente diseñado para proteger al equipo en específico.
- **Cortafuego comercial**: Típicamente viene anexo a las aplicaciones de antivirus y por lo general cuando se instalan este tipo de suite, este cortafuego reemplaza al que opera por defecto en el sistema operativo, el cual además incorpora funcionalidades más avanzadas y especializadas en protección.

5.3.10. *Solución de Seguridad Perimetral en Pronavicola S.A.*

Fortinet: Compañía dedicada a brindar soluciones de seguridad perimetral de alto rendimiento y confiabilidad, posee una gran reputación en el mercado y además es líder en identificación y publicación de amenazas cibernéticas. Posee un software integrado exclusivo llamado Security Fabric, el cual centraliza un sistema operativo, procesos de seguridad y actualizaciones sobre nuevas amenazas constantemente.

Entre sus múltiples productos que ofrece la compañía podemos encontrar el **Fortigate 200E**, el cual está diseñado para trabajo pesado en administración de seguridad en redes y firewall.

Figura 1. Fortigate 200E

Fuente: FORTINET. Fortigate 200E Series. Recuperado el 2 de noviembre de 2021. Disponible en: https://www.fortinet.com/content/dam/fortinet/assets/data-sheets/FortiGate_200E_Series.pdf

Los firewalls Fortinet son conocidos como “Firewall de siguiente generación” (NGFW) debido a sus características y OS avanzado de protección que permite seguridad con políticas automatizadas frente a las nuevas amenazas.

La ventaja con FortiGate es que gracias a sus características permite la integración de varias de las técnicas y tecnologías de seguridad mencionadas anteriormente, es decir, permite la creación rápida de políticas específicas por diferentes categorías y tipos de agrupación o filtrado, cuenta con funcionalidades IDS e IPS para la vigilancia y detección de intrusos, sistema de antivirus sumamente efectivo ante ataques espía y demás, inspección SSL y Sandboxing para la prevención ante tráfico cifrado y malware, entre otras características.

Adicional a esto, Fortinet cuenta con su propia organización para la investigación de amenazas y ataques llamada FortGuard, la cual está integrada por especialistas, analistas e ingenieros en ciberseguridad, garantizando así la máxima protección en sus productos.[30]

Pronavicola cuenta tres diferentes modelos de FortiGate, un FortiGate 40F en la sede de producción (*Planta de Incubación*), un ForiGate 100D en la sede de insumos (*Planta de Alimento Balanceado*) y dos FortiGate 200E en el Data Center de la sede principal (*Oficinas Administrativas*), estos últimos conectados uno como respaldo del otro (*NO en alta disponibilidad*) y siendo el FortiGate 200E el firewall principal donde las demás sedes establecen conexión y enrutamientos necesarios para entregar red y protección en cada centro de trabajo, políticas y configuraciones que son explicadas y repotenciadas en las páginas 135 a 149 del presente documento.

[30] Quanti. Que es FortiGate: Conociendo el Firewall. Publicado el 15 de febrero de 2022. Obtenido de: https://quanti.com.mx/articulos/conociendo-el-firewall-fortigate/

5.4. MARCO CONCEPTUAL

5.4.1. *¿Qué es la seguridad informática?*

Se entiende como el acto de prevenir o detectar posibles robos o ataques cibernéticos como información personal sensible, contraseñas, entre otras.

Por tal motivo, la seguridad informática procura la utilización de software para la protección de los mencionados ataques, herramientas como programas de antivirus, sistemas de firewall y demás medidas que cada usuario debe adoptar y utilizar.

5.4.2. *¿Qué es la seguridad de la información?*

La seguridad de la información son una serie de prácticas y medidas diseñadas para proteger los datos de una organización, en otras palabras, es la manera como una compañía puede gestionar los riesgos a los que su data está expuesta, controlarlos, superarlos y monitorearlos con el objetivo de reducir al máximo el impacto que pueda tener dicho riesgo y así mantener su información siempre integra, confiable, disponible y verificable.[31]

5.4.3. *Ciberseguridad:*

Conjunto de técnicas, medidas y herramientas designadas para la protección informática de un compañía u organización.

[31] Lisa Institute. Diferencia entre Ciberseguridad, Seguridad Informática y Seguridad de la Informacion. Publicado el 3 de marzo de 2021. Obtenido de: https://www.lisainstitute.com/blogs/blog/diferencia-ciberseguridad-seguridad-informatica-seguridad-informacion

En una compañía seria la ciberseguridad es una cultura que involucra los procesos, personal y recursos tecnológicos para que en conjunto creen una defensa eficiente y eficaz ante los ataques cibernéticos, de allí la importancia de que todos los colaboradores sean parte de dicha barricada, pues los ataques suelen tener éxito porque encuentran el eslabón más débil de la cadena, que históricamente es el usuario final.

Cabe mencionar que algunos de los tipos de amenazas más comunes y de los cuales se busca capacitar a todos los colaboradores son: suplantación de identidad, ransomware, malware e ingeniera social. [32]

Existen también otros tipos de ciber amenazas que se definen así:

Delito Cibernético: agentes independientes o equipos de black hackers que se concentran en causar daños o interrupciones, o también desfalcos financieros.

Ciberataques: por lo general perpetrados con fines de agitación o divulgación de información política.

Ciberterrorismo: Buscan declinar sistemas informáticos para hacerlos inaccesibles y causar pánico.

Ciber amenazas recientes:

Malware Dridex. Troyano de finanzas que desde 2014 y hasta 2019 cuando se le imputaron cargos a sus creadores, utilizando phishing y demás malware robaron contraseñas e información financiera de miles de víctimas para luego realizar

[32] Cisco. ¿Qué es la ciberseguridad?. Consultado el 14 de octubre de 2021. Disponible en: https://www.cisco.com/c/es_mx/products/security/what-is-cybersecurity.html

transacciones y fraudes de miles de millones.

Estafas Románticas: Ataques de tipo ingeniera social, los cuales se basan en la obtención de información personal y sensible de las victimas conquistándolas por redes sociales, casos que suceden a diario en todo el mundo y que 2019 en EE. UU. causaron millonarias pérdidas.

Malware Emotet: Troyano que a final de 2019 demostró que podía robar información al descifrar contraseñas de baja complejidad.[33]

5.4.4. *Pilares de la Seguridad informática*

***Se entiende como pilares de la seguridad informática los siguientes conceptos*:**

Integridad: todo proceso que se lleve a cabo en aras de la seguridad de la información debe garantizar que la data de una organización es precisa, absoluta y contrastable, de ello depende el futuro y continuidad del negocio, así como también debe brindar certeza en que los datos no han sido modificados, violados o alterados por ningún ente o personal diferente al autorizado.

Ejemplo: Una entidad auditora o de seguridad solicita información contenida en bases de datos o cintas de Backup, pero dicha información no está completa o contiene archivo dañado o inaccesibles. Esto podría significar una sanción o reporte como hallazgo grave pues el área TI no está garantizando ni resguardando adecuadamente la información.

[33] Kaspersky. ¿Qué es la ciberseguridad?. Consultado el 14 de octubre de 2021. Disponible en: https://latam.kaspersky .com/resource-center/definitions/what-is-cyber-security

Disponibilidad: Así como ningún individuo o entidad puede acceder a información sensible de una compañía, todo aquel que tenga autorización previa y consentida debe tener siempre acceso a la información y demás recursos cuando lo solicite, lógicamente a través de los medios o canales que la compañía disponga, así como todos los protocolos que dicho acceso requiera.

Ejemplo: Se requiere acceder a los datos para consultar una información vital en un proceso jurídico o para completar algún proceso financiero urgente, pero el servidor donde se contiene esa información esta colgado ya que no se le han hecho las actualizaciones y el seguimiento correspondiente desde el área TI para su rendimiento optimo.

Confidencialidad: Es de vital importancia garantizar que solo aquellos usuarios con los niveles de autorización y de alta confianza pueden acceder a la información, ya que este pilar vela por data que en este caso es la propiedad intelectual de la organización y mantenerla en secreto resulta clave en el andamiaje de cualquier empresa.

Ejemplo: No se tiene un sistema de control de acceso o un protocolo adecuado para proteger la confidencialidad de la información de nómina de la compañía, entonces un usuario inescrupuloso y sin autorización extrae información sobre los salarios y patrimonio de las altas gerencias en la compañía y luego decide divulgarlos en redes sociales creando así una inestabilidad en la confianza y reputación de la organización así como con el recurso humano de la empresa, además de las sanciones al área TI y otros.[34]

[34] SGSI. Los tres pilares de la seguridad de la información: confidencialidad, integridad y disponibilidad. Publicado el 1 de febrero de 2018. Obtenido de: https://www.pmg-ssi.com/2018/02/confidencialidad-integridad-y-disponibilidad/

5.4.5. *Tipos de Hacker Existentes*

Black Hackers: También llamados Black Hat o ciberdelincuentes son intrusos de redes privadas, datos personales y financieros, algunas veces de ing. Social e implantadores de virus.

Crackers: por la misma línea de los Black Hat, estos se dedican principalmente a la desestabilización e infección de servidores y redes, su aparente objetivo es solo causar caos.

Phreakers: Este tipo de Hacker es similar al Cracker con la diferencia que se enfocan en centrales telefónicas y telecomunicaciones, sin embargo, con los cambios que ha sufrido la telefonía hoy en día convirtiéndose casi que por completo en digital a obligado a que dichos personajes adopten comportamientos y técnicas propias de un Hacker normal.

White Hackers: También llamados White Hat, se enfocan más como vigías y alertan sobre sistemas inseguros y vulnerabilidades en redes privados o portales web, su labor suele casi del tipo activista.

Hacker: El termino más común y globalizado para referirse a un pirata informático, término que se podría considerar erróneo en muchos casos, ya que este tipo de personas suelen ser vigilantes de la red y desarrollan soluciones o plantean sugerencias respecto a vacíos o vulnerabilidades de cualquier sistema informático.

Lammers: Son una comunidad paradójica ya que no son Hackers como tal pues cuentan con pocos conocimientos en computación, pero a la vez muy peligrosos y molestos ya que en su afán de demostrar que pueden infectar o desestabilizar algún

sistema informático constantemente prueban todo tipo de métodos y ataques esperando que alguno funcione.[35]

5.5. MARCO HISTORICO

A lo largo de casi una década de construcción y crecimiento en materia de gobernanza y ciberseguridad en cabeza del área IT de la compañía, se ha logrado establecer controles y políticas que han permitido proteger y organizar como tal el área y los activos informáticos de la organización, pero además de eso, el área ha tenido que enfrentar pruebas difíciles en materia de infraestructura y seguridad informática, tal como paso años atrás cuando el Core de servidores era totalmente físico y esto causo varios incidentes de rendimiento, problemas de hardware y ataques cibernéticos organizados, los cuales, gracias a la experticia y competencias del área IT, se pudieron solucionar y posteriormente dieron pie a la decisión de implementar un ambiente virtualizado de servidores.

Pero no solo eso ha tenido que enfrentar la compañía, también en 2016 vivió una de sus pruebas más duras a nivel administrativo y tecnológico, año en el que tuvo que sufrir un desastre ecológico por inundación, donde el Data Center actual tuvo pérdidas considerables que por fortuna pudieron ser sopesadas en términos económicos por aseguradoras, y en términos informáticos gracias al buen diseño del Data Center y la activación oportuna de un plan de contingencia que permitió que la compañía no detuviera su operación.

Por otro lado, vino la pandemia y estallido social en Colombia, situación que obligo al mundo entero a enfrentarse de golpe con la virtualidad y el teletrabajo, retos importantes en nuestro país a nivel tecnológico y de ciberseguridad.

---

[35] ROMERO, Sarah. ¿Cuántos tipos de hacker existen?. 5 de septiembre de 2019. Disponible en: https://www.muyinteresante.es/tecnologia/articulo/que-es-un-hacker-de-sombrero-gris-831473842564

Llegando hasta estos días, la compañía a nivel tecnológico ha dado grandes pasos, sin embargo, la tecnología se expande todos los días y los ciberataques igual, dejando a veces obsoleta las medidas existentes en la compañía y haciendo cada vez más difícil la mitigación de riesgos, situación que puede estar enfrentando Pronavicola S.A., no porque no cuente con buenos controles o medidas, sino porque requieren de actualizaciones, reconfiguración y evaluación para poder garantizar su efectividad y plantear nuevos proyectos y planes de mejora.[36]

5.6. ANTECEDENTES O ESTADO ACTUAL

Citando dos trabajos donde se elaboró o desarrollo un Plan Director de Seguridad (PDS) con éxito, encontramos uno elaborado en España para la Asociación Gubernamental APSA en 2019; la organización brinda apoyo a familias en proyectos de salud, vivienda, formación, recreación, empleo, entre otros. Como era de esperarse, la organización cuenta con una infraestructura y recursos tecnológicos que requieren ser protegidos y enmarcados en procesos de gobernanza de TI, por lo tanto, quien elabora esta implementación, desarrolla un trabajo muy interesante basado en las metodologías MAGERIT y los estándares de la familia ISO/IEC 27000, 27001 y 27002, diseñando un SGSI con claros lineamientos y estrategias tecnológicas que garantizan la seguridad informática de la entidad.[37]

El segundo trabajo interesante es el PDS diseñado por estudiantes de la Universidad Cooperativa de Colombia en este año 2021. En dicho diseño los

[36] MORENO, GALINDO, Eliseo. Metodologia de investigacion, pautas para hacer tesis. Publicado el 26 de agosto de 2017. Obtenido de: https://tesis-investigacion-cientifica.blogspot.com/2017/08/elaboracion-del-marco-historico.html

[37] MONTERO VALENCIA, Jessica Alexandra. Desarrollo del Plan Director de Seguridad para la Asociacion APSA. Publicado en septiembre de 2019. Disponible en: https://core.ac.uk/download/pdf/237118547.pdf

especialistas diseñan un plan de seguridad para una institución educativa, en él se plantean desarrollar políticas y controles para la mitigación y protección de los datos sensibles de la institución, haciendo uso de normas ISO/IEC 27001 y proponiendo diferentes proyectos tecnológicos y políticas claras en base a las vulnerabilidades encontradas.[38]

5.7. MARCO LEGAL

5.7.1. *Delitos informáticos*

Ley 1273 de 2009 – Delitos Informáticos en Colombia.

Delitos informáticos en Colombia

Por medio de esta ley se determinan las diferentes modalidades de crímenes informáticos y las sanciones de tipo penal y monetario que suponen dichas faltas, describiendo de manera breve y concisa las condiciones del código cuando se trate de una suplantación, robo, destrucción, violación, interceptación, transferencia, entre otros.

Cualquiera sea el caso, se puede aplicar una u otra, incluso varias, esto debido al escenario y manera como se configure el delito. Algunos de los más comunes y por los cuales Pronavicola S.A. debe estar alerta son:

- **269A**: ***Acceso abusivo a un sistema informático***, el cual se materializa debido al acto en si de irrumpir en una red corporativa sin autorización y con

[38] CARVAJAL ARTUNDUAGA, Juan Felipe, *et al.* Diseño de un plan de seguridad informática para el sistema de información del colegio Gimnasio los Pinos. Publicado en enero de 2021. Disponible en: https://repository.ucc.edu.co/bitstream/20.500.12494/33277/2/2021_Dise%C3%B1o_plan_seguridad.pdf

la intensión de entorpecer sus operaciones y excluirlo totalmente de su administración, por lo tanto, incurriría en una pena de prisión de 48 o 96 meses, al igual que una multa de entre 100 y 1.000 SMLMV, esto siempre y cuando la conducta no configure una pena mayor.

- **269B**: ***Obstaculización ilegitima de sistema informático o red de telecomunicaciones***, el cual se ajusta a la realización del ataque DDoS, por el cual podrían incurrir en una pena de prisión de 48 a 96 meses y una multa de entre 100 y 1.000 salarios mínimos legales mensuales vigentes, esto siempre y cuando la conducta no configure una pena mayor.
- **269B**: ***Interceptación de datos informáticos***, El cual se configura cuando se interceptan datos desde el origen, destino o desde adentro de una privada o sistema, al igual que cuando se captan ondas electromagnéticas que provienen de un sistema sin tener previamente una orden judicial, incurriendo en una posible pena de 36 a 72 meses.
- **269E**: ***Uso de Software Malicioso***: se configura al utilizar Botnets, lo cual es clasificado como un virus informático que puede causar daños a los datos sensibles de una compañía y de los equipos de cómputo, por lo tanto, incurriría en una pena de prisión de 48 a 96 meses y una multa de entre 100 y 1.000 salarios mínimos legales mensuales vigentes, esto siempre y cuando la conducta no configure una pena mayor.

Teniendo en cuenta estos artículos, la condena podría juntar las penas y multas por los tres delitos y seria la justicia colombiana quien determine la totalidad de la misma.

Actualmente en Colombia los delitos informáticos más comunes son los relacionados con estafas y falsificación de documentos e ID.

Uno de los más comunes es conocido como “carta nigeriana” el cual consiste en convencer a la victima de que es merecedor de un gran premio y se le solicita que

para liberar dicho premio debe transferir o pagar una suma de dinero por adelantado para gestión de tramites del premio, se realiza comúnmente vía correo electrónico de tipo spam y por ende, alguno de los colaboradores de la compañía podría ser víctima.

Este delito podría configurarse en el artículo 269I: ***Hurto por medios informáticos y semejantes*** y también según fuere el caso en el artículo 269J: ***Transferencia no consentida de activos,*** el cual contempla pena de prisión de 48 a 120 meses y una multa de entre 200 y 1.500 SMLMV, esto siempre y cuando la conducta no configure una pena mayor.[39]

6. DISEÑO METODOLÓGICO

NIST CSF: NIST (Instituto Nacional de Estándares y Tecnologías) por ejemplo es talvez uno de los marcos más robustos y fácilmente implementables que existen ya que su objetivo se centra en resultados, en la manera más eficiente de aprovechar y madurar los recursos tecnológicos y el nivel de seguridad existente de la compañía.

Dicha implementación se traduce en los tres pilares que edifican el marco, Framework Core, Tiers (Niveles de Implementación) y Perfiles. El primero de ellos se trata de un conjunto de actividades y resultados esperados en cuanto a ciberseguridad; categorizados y enfocados dentro de los estándares actuales, de esta forma presenta cinco (5) funciones vitales para determinar el estado actual, alcance y puntos críticos a fortalecer a través de una serie de categorías y

[39] Policía Nacional de Colombia. Normatividad sobre delitos informáticos. Actualizado 16 de julio 2023. Disponible en: https://www.policia.gov.co/denuncia-virtual/normatividad-delitos-informaticos

subcategorías que establecerán claramente la ruta de éxito del CSF (Cibersecurity Framework).[40]

6.1.1. *Niveles de Framework Core*

Identificar: Entendimiento global de la organización en todos sus frentes para gestionar adecuadamente la ciberseguridad de este. Todos sus recursos, personal, responsabilidades, activos y todo aquello que permita dibujar un mapa de riesgo y como mitigarlo inicialmente. (Inventario de activos de hardware y software, personal, funciones y responsabilidades, políticas de ciberseguridad, entre otros.)

Proteger: Medidas de ciberseguridad que garanticen la prestación de servicios críticos de la organización con el objetivo de estar preparado ante un incidente grave de seguridad. (Controles de acceso a los usuarios, software de seguridad, capacitaciones en ciberseguridad, copias de seguridad, entre otros.)

Detectar: Medidas y técnicas efectivas para identificar la ocasión de una situación de ciberseguridad, permitiendo así la detección eficaz del ataque o la vulnerabilidad. (Monitoreo constante de la red corporativa y el uso que dan los usuarios)

Responder: Toma de decisiones ante un evento de ciberseguridad; estrategias para mitigar la ocasión de un evento mayor. (Preparación, notificación, análisis y actualización de las actividades y políticas de ciberseguridad)

[40] OEA, AWS. Un abordaje integral de la ciberseguridad. Publicado en 2019. Disponible en: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

Recuperar: Plan de actividades pertinentes para la rápida recuperación y continuidad de las operaciones de la organización. (corrección rápida y divulgación de los incidentes)[41]

6.1.2. *Niveles de Implementación*

El marco propone cuatro grados de gestión del riesgo de ciberseguridad (Parcial, Riesgo Informado, Repetible y Adaptativo), los cuales respaldan las decisiones, se ajustan según la compañía y la forma como opera la información de sus negocios y actores externos.

Dichos riesgos se definen en base al proceso de gestión de riegos, programa integrado de gestión de riesgos y participación externa.[42]

6.1.3. *Perfiles*

El momento cumbre del CSF, ya que es aquí cuando se establece el momento actual y futuro de las metas organizacionales (Perfil Actual y Perfil Objetivo), así como los límites de riesgo, plan de acción y recursos necesarios en la búsqueda de los resultados esperados del Core.[43]

---

[41] ACOSTA, David E. Guía rápida para entender el marco de trabajo de ciberseguridad del NIST. Publicado el 11 de enero de 2017. Disponible en: https://www.deacosta.com/guia-rapida-para-entender-el-marco-de-trabajo-de-ciberseguridad-del-nist/

[42] JIMÉNEZ, Mónica Maria. Conoce el marco de ciberseguridad del NIST. Publicado el 22 de enero de 2021. Disponible en: https://www.piranirisk.com/es/blog/marco-ciberseguridad-nist-que-es

[43] GÓMEZ MORALES, Gianncarlo. Implementando el Cybersecurity Framework del NIST. Publicado el 21 de junio de 2018. Disponible en: https://es.linkedin.com/pulse/implementando-el-cybersecurity-framework-del-nist-g%C3%B3mez-morales

En base al marco NIST, y todas las metodologías y mecanismos de apoyo presentados en el marco teórico y conceptual, la manera de abordar este proyecto requerirá de **6 fases**:

Fase 1: **Priorización y determinación del alcance**. Esto analizando los objetivos según su línea de negocio y estableciendo nivel de prioridades en la organización.

Fase 2: **Creación de Perfil Actual**: Se realizará evaluación del estado de ciberseguridad actual, Identificando los sistemas y recursos tecnológicos dentro del alcance, así como términos legales o normativos de la compañía y valoración de riesgos en general, de esta forma sabremos cuales de las categorías del Framework Core se están cubriendo y cuáles no. Este perfil debe abarcar todo aquello que se involucre en el proceso, como son políticas, personal, procedimientos, recursos y tecnología en general.

Fase 3: **Evaluación de Riesgos**: Análisis de la posibilidad de ocurrencia de un problema de ciberseguridad y su impacto en la compañía, es importante que la organización este consciente de las vulnerabilidades a las que se está expuesto todo el tiempo, utilizando como herramienta de análisis la metodología MAGERIT, fundamental en el descubrimiento y medición de riesgos existentes y latentes.

Fase 4: **Creación Perfil Objetivo**: En base a las categorías del marco que describen como debe ser un resultado esperado, dentro de la legalidad y apoyado en los objetivos estratégicos del negocio.

Fase 5: **Determinar, evaluar y dar prioridad a las brechas**: Se realiza una comparación de los perfiles actual y objetivo y se planifica la manera como serán abordadas y conquistadas dichas brechas, los costos, recursos, actores y demás

ítems para conquistar dicho perfil objetivo, lo cual deberá ser evaluado y aprobado por las directivas posteriormente.

Fase 6: Implementar plan de acción: Una vez aprobados los planteamientos del punto anterior se procede a ejecutar paso a paso los proyectos o medidas que permitirán reducir las brechas, mitigar riesgos y alcanzar el perfil objetivo. Todas estas acciones deben estar enmaradas en las premisas de gobernanza TI y de ciberseguridad e incluir todos los diferentes recursos y sus responsables para el éxito del objetivo.[44]

Durante el desarrollo de las **6 fases**, se utilizará también una herramienta estándar de evaluación GAP, dicha herramienta permitirá determinar nivel de madurez, rendimiento y brechas en determinadas aplicaciones al interior de la compañía, como simuladores GAP 27001 y las normas de la familia ISO/IEC 27001 como apoyo a dicha actividad.[45]

También se diseñará o mejoraran las políticas de seguridad existentes en la compañía, esto como principio fundamental de seguridad básica de las compañías, para ello se requiere de guías, modelos ya establecidos y el material existente para su debida elaboración.[46]

También se llevará a cabo la reconfiguración del sistema de seguridad perimetral de Pronavicola S.A., el cual está basado en Fortinet, para dicha labor se recurrirá a

[44] OEA, AWS. OEA, AWS. Un abordaje integral de la ciberseguridad. Publicado en 2019. Disponible en: https://www.oas.org/es/sms/cicte/docs/OEA-AWS-Marco-NIST-de-Ciberseguridad-ESP.pdf

[45] ISOtools. Análisis y evaluación de riesgos según ISO 27001: identificación de amenazas, consecuencias y criticidad. Publicado el 30 de julio de 2019. Disponible en: https://www.isotools.org/2019/07/30/analisis-y-evaluacion-de-riesgos-segun-iso-27001/

[46] Mintic. Elaboracion de la política general de seguridad y privacidad de la información. Consultado el 10 de octubre de 2021. Disponible en: https://mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

un experto en dicha solución y coste y tiempo dependerá de las horas que se requieran para los ajustes, personalización y capacitación básica del personal TI.[47]

Por último, es importante resaltar que el PDS permitirá, durante el desarrollo de los 7 puntos mencionados y tras la evaluación y calificación de riesgos surgidas del análisis previo de los procesos, áreas y actividades de la compañía, una visión clara de cuáles son los proyectos y medidas que pueden llevarse a cabo y que luego deberán ser presentadas y aprobadas por las altas gerencias para su futura implementación. Afortunadamente, para esto existen diferentes posibilidades y ejemplos útiles para determinar cuáles pueden ser los mejores proyectos a emprender y la manera como pueden ser presentados.[48]

7. PROCESO METODOLOGICO

7.1. *Fase 1*

Alcance del PDS

Al ser PRONAVICOLA S.A. una compañía con más de 40 años en el negocio avícola, se debe tener claridad de sus procesos de negocio, factores internos y externos que interactúan en la organización y aspectos que deben ser fortalecidos en términos de estandarización y seguridad, por lo tanto, la elaboración del Plan Director de Seguridad deberá abarcar dichos factores que serán analizados y definidos a continuación:

[47] Quanti. La guía definitiva para configurar un Fortigate. Publicado el 14 de noviembre de 2019. Disponible en: https://quanti.com.mx/articulos/la-guia-definitiva-para-configurar-un-fortigate/

[48] LOPEZ BALLOQUI, José María. Elaboración de un plan de ciberseguridad en una empresa aeroespacial. Publicado en 2021. Disponible en: https://biblus.us.es/bibing/proyectos/abreproy/93364/fichero/TFG-3364+L%C3%93PEZ+BALLOQU%C3%8D%2C+JOS%C3%89+M..pdf

Procesos de negocio dentro del alcance

La razón de ser de la compañía PRONAVICOLA S.A. es su rol como INCUBADORA, por lo tanto, se dedica a la venta y comercialización de pollitas y pollitos de un día de nacidos, servicio que lleva prestando por más de 40 años y que hoy representa más del 40% de la genética del país. La compañía tiene clientes en todo el país a los cuales brinda no solo pollitos y pollitas con una genética de última generación, sino que sus vendedores que también son médicos veterinarios, acompañan a los clientes en el proceso de levante y adecuación de las granjas.

El mencionado proceso y líneas de negocio exigen un compromiso, confianza y apoyo ejemplar por parte de las directivas de la compañía para que de esta manera se puedan establecer objetivos estratégicos alineados con objetivos y procesos tecnológicos que permitan establecer un gobierno y gestión de TI conforme con los retos y riesgos que deberán asumirse en la búsqueda de alcanzar las aspiraciones de los inversionistas y directivas, que a su vez desembocará en la satisfacción de los clientes y aliados estratégicos. Dicho esto, el alcance del PDS debe comprender y gestionar los procesos, actividades y personal del área *Informática y Tecnología* principalmente, ya que, a partir de una buena gestión de ciberseguridad, todos los procesos de negocio y tecnológicos podrán seguir realizándose con plena certeza que la integridad, confidencialidad y disponibilidad de la compañía están garantizadas.

A nivel interno, la compañía en su PDS debe proveer los recursos tecnológicos adecuados y ajustados a las características de la empresa, políticas de ciberseguridad y de gestión de activos, implementación y afinamiento de una solución de seguridad perimetral, instalaciones e infraestructura, planes de contingencia y respaldo de la información, gestión de servicios de TI, y, por último, programas de sensibilización ante riesgos cibernéticos.

A nivel externo, la compañía debe garantizar a todos sus proveedores, aliados y clientes desde su PDS los tres pilares fundamentales de la SI, integridad, disponibilidad y confidencialidad, aspectos que serán alcanzados una vez se alcance un nivel de madurez, automatización y estandarización óptimos que permita procesos de mejora continua y generación de valor de principio a fin.

En conclusión, el alcance del PDS permitirá el afinamiento de los procesos y procedimientos existentes en el área TI, de forma que pueda brindar, adecuada y eficientemente los servicios que requiere el negocio, así como garantizar la seguridad, resguardo y disponibilidad de la información y recursos tecnológicos de la compañía. Por otra parte, los departamentos de comercial y alquiler y ventas tendrán los mejores canales de comunicación y herramientas para brindar a los clientes, aliados y proveedores, actuales y futuros, un servicio de calidad para una excelente fidelización y satisfacción de los mismos.

7.1.1. *Fase 2*

Perfil actual e identificación de recursos tecnológicos y riesgos generales:

Basado en lo que plantea el marco NIST CSF en sus cinco funciones y categorías, se desarrolla un perfil actual tomando aquello que pueda aplicar y ajustarse a la compañía.

Figura 2. Funciones y Categorías

FUNCIÓN IDENTIFICADOR ÚNICO	FUNCIONES	CATEGORÍA IDENTIFICADOR ÚNICO	CATEGORIAS
ID	IDENTIFICAR	ID.AM	Gestión de activos
		ID.BE	Ambiente de negocios
		ID.GV	Gobernanza
		ID.RA	Evaluación de riesgos
		ID.RM	Estrategia de gestión de riesgos
		ID.SC	Gestión del riesgo de la cadena de suministro
PR	PROTEGER	PR.AC	Gestión de identidad, autenticación y control de acceso
		PR.AT	Conciencia y capacitación
		PR.DS	Seguridad de datos
		PR.IP	Procesos y procedimientos de protección de la información
		PR.MA	Mantenimiento
		PR.PT	Tecnología de protección
DE	DETECTAR	DE.AE	Anomalías y Eventos
		DE.CM	Monitoreo continuo de seguridad
		DE.DP	Procesos de Detección
RS	RESPONDER	RS.RP	Planificación de respuesta
		RS.CO	Comunicaciones
		RS.AN	Análisis
		RS.MI	Mitigación
		RS.IM	Mejoras
		RS.RP	Planificación de respuesta
RC	RECUPERAR	RC.RP	Planificación de la recuperación
		RC.IM	Mejoras
		RC.CO	Comunicaciones

Fuente: GÓMEZ, MORALES, Gianncarlo. ¿Qué es el cibersecurity Framework de NIST de los Estados Unidos?. Publicado el 30 de abril de 2019. Disponible en: https://www.esan.edu.pe/conexion/actualidad/2019/04/30/que-es-el-cybersecurity-framework-de-nist-de-los-estados-unidos/

Entendiendo esto, la compañía cuenta con la mayoría de los recursos tecnológicos en un nivel aceptable y en proceso de mejoría o implementación de algunos de los ítems mencionados en la fase 1 de la siguiente forma:

Datos:

- Documentos digitalizados.
- Correo electrónico.
- Información en computadoras.
- Datos de grabación de cámaras de seguridad.
- Copias de seguridad en cinta magnética.

Aplicaciones Sensibles:

- ERP (Siesa Enterprise, Siesa Access, Nomina Web).
- Aplicaciones de videoconferencia (Microsoft Teams y Zoom).
- Softwares varios (Autocad, Project, otros).
- Aplicación Veritas Backup Exec para copias de seguridad.

Infraestructura TI:

- Tres sedes con oficinas.
- Escritorios.
- Archivadores.
- Data Center.
- Racks de Comunicaciones (Sede Principal).
- Rack de Servidores (Sede Principal y sede Producción).
- Rack Eléctrico (Sede Principal y Sede Producción).

Activos y Hardware TI:

- Computadoras de escritorio y portátiles (En su mayoría Dell y Lenovo).
- Switches (Dell)
- Fortiswitch 248D (Sede Producción).
- Cajas de Discos, Biblioteca de Cintas de Backup, discos externos para copias, racks para copias (Dell).
- Herramientas para mantenimiento preventivo.
- Equipos de redes como routers, wifi (FortiAps y D-Link).
- Teléfonos IP (Grandstream).
- Lectores biométricos de marcación de huellas (Zkteco).
- UPS en diferentes centros de trabajo (Emerson o APC).

- Firewall FortiGate 200E (Sede Principal).
- Fortinet FortiMail 200E (Sede Principal).
- Forinet FortiVoice 100E (Sede Principal)
- Firewall Fortigate 40F (Sede Producción).
- Antivirus Kaspersky Endpoint Security.
- Portal web informativo.
- Sistemas Operativos Windows (server y pro en diferentes versiones).
- Paquete de Office (Diferentes versiones).

Equipo TI:

- Director TI.
- Asistente TI.
- Practicante de sistemas.

7.1.2. *Términos normativos de la compañía*

Pronavicola S.A. dentro de sus normas y específicamente en la política de seguridad informática actual, estipula que cualquier actividad malintencionada o en perjuicio de la propiedad material o intelectual de la compañía o su reputación, será castigado y sancionado a nivel interno, o bien, si la falta sobrepasa las competencias normativas de la compañía, materializándose como un delito punible, será denunciado y juzgado por la justicia colombiana, según se configure dicha falta.

7.1.3. *Valoración General de Riesgos*

La compañía podría verse afectada por las siguientes clases de amenazas cibernéticas:

7.1.4. *Clasificación de Amenazas*

Amenazas Tipo Malware:

- Virus.
- Gusano.
- Troyano.
- Spyware.
- Adware.
- Keyloggers.
- Ransomware.
- APT.

Amenazas Tipo Denegación de Servicio:

- Denegación de Servicio (DoS)
- Denegación de Servicio Distribuido (DDoS).

Amenazas de Tipo Ingeniería Social:

- Phishing.
- Spear Phishing.
- Correo Spam.
- Smishing.
- Vishing.

- Pretexting.

Otras Amenzas

- Fuerza Bruta.

7.1.5. *Identificación de vulnerabilidades de software malicioso que pueden afectar tanto software como hardware*

Vulnerabilidad por Malware

A pesar de contar con una solución FortiMail y FortiGate, puede filtrarse un correo con adjuntos capaz de infectar equipos y la red, también la descarga de software malicioso por parte de usuarios con privilegios o la utilización de memorias USB infectadas en usuarios con equipos portátiles o con acceso concedido a los puertos. Impacto alto.

Vulnerabilidad por Denegación de Servicio

Debido a que el firewall requiere ser afinado en su configuración actual, existe la posibilidad de que un atacante avanzado trate de lanzar un ataque. Impacto alto.

Vulnerabilidad por Ingeniería Social

Es poco probable debido al sistema de seguridad perimetral y el acceso restringido de navegación en la mayoría de usuarios, sin embargo, podría suceder en otros ámbitos, como contraseñas escritas en papeles sobre escritorios o que haya usuarios con permisos de navegación que le permitan acceder a redes sociales y otros sitios óptimos para esta modalidad, así como el desconocimiento e ingenuidad propias del usuario. Impacto Medio.

Vulnerabilidad por Fuerza Bruta

Algunos usuarios que acceden por VPN desde fuera, no cuentan con autenticación de doble factor, por lo tanto, un ataque de Fuerza Bruta podría materializarse. Impacto alto.

Indicadores de Gestion

La importancia de los indicadores radica en la manera como le permiten a la compañía medir y evaluar la eficiencia y las posibilidades de riesgo latentes en el PDS o SGSI existente o en desarrollo, es decir, brindan la posibilidad de un seguimiento detallado de los compromisos y estrategias asumidas por todos los actores de la implementación.[49]

En conclusión, los indicadores permitirán presentar a las directivas un informe detallado y periódico sobre la gestión de la seguridad informática en la organización, por lo tanto, los objetivos y actividades que se plantee desarrollar deben tener un porcentaje aterrizado que permita un margen de mejora considerable para dar cabida a oportunidades de crecimiento.

[49] SGSI. ¿Cuáles son los principales indicadores de seguridad de la informacion? Publicado el 11 de julio de 2019. Disponible en: https://www.pmg-ssi.com/2019/07/principales-indicadores-en-seguridad-de-la-informacion/

A continuación, los indicadores de gestión de los puntos o aspectos críticos en la gobernanza de seguridad informática en la compañía.

INDICADOR # 1 - DOCUMENTOS DE SEGURIDAD	
Código Indicador:	PDS - 1.0.1
Fecha de creación:	10 de noviembre de 2021
Fecha última actualización:	---
Título del indicador:	Política de Seguridad Informática
Objetivo:	Detallar la correcta utilización de los servicios, aplicaciones de software, computadoras e infraestructura de red (en caso de existir). Dichas normas buscan proteger la información, colaboradores y la compañía misma, así como generar un ambiente de confianza y seguridad entre todos los colaboradores, sean internos o externos.
Soporte de medida:	Porcentaje de políticas y actividades documentadas en función de la seguridad de la información y todo recurso tangible e intangible de la compañía.
Meta porcentual del indicador:	Mínima: 70-80% Aceptable: 80-90%

	Destacado: 100%
Fuente de información:	Manuales de seguridad informática, manual de funciones, procedimientos de copia, resguardo y recuperación de la información, formatos de creación, modificación y eliminación de usuarios, controles de acceso, políticas de directorio activo, entre otros.
Fórmula de cálculo:	(# de políticas y requisitos de seguridad informática documentadas y aprobadas / # total, de políticas y requisitos realizados) * 100

Fuente del cuadro: Diseño propio.

Cuadro 1. Documentos de Seguridad

7.1.6. *Documentación de Seguridad Existente*

Actualmente existe una política de seguridad informática, la cual es firmada y anexada a la hoja de vida de cada colaborador, sin embargo, dicha política fue diseñada en el año 2011 y actualizada por última vez en 2018.

La política comprende los siguientes ítems:

- Uso de la tecnología para el procesamiento y propiedad de la información.
- Condiciones para creación de claves de seguridad de usuario.
- Uso inadecuado de la red.

- Actividades prohibidas en la red.
- Actividades prohibidas en el correo electrónico.
- Anexo sobre uso de memorias USB.

Siguiendo la formula del indicador de gestión sobre la política de seguridad, se considera que el cumplimento se encuentra en un nivel aceptable con **80%** de calificación, esto debido a que el documento como tal esta desactualizo e incompleto en ciertos valores actuales, además, en los últimos años se a identificado el incumplimiento de varias normas con cierta eventualidad, como revelar la contraseña de usuario a otro compañero, abrir sin ninguna precaución adjuntos que puedan ser maliciosos, impresión y desarrollo de actividades ajenas a la compañía, entre otros.

También se detecta que existen políticas y grupos de usuarios con determinados permisos de manera desorganizada en el servidor de dominio.

INDICADOR # 2 – ANALISIS SEGURIDAD PERIMETRAL (PDS)	
Código Indicador:	PDS - 1.1.0
Fecha de creación:	10 de noviembre de 2021
Fecha última actualización:	---
Título del indicador:	Análisis y valoración de la solución de seguridad perimetral
Objetivo:	Identificar y analizar el porcentaje de protección, organización y efectividad de las políticas de seguridad establecidas en la solución del firewall.

Soporte de medida:	medida porcentual de avance de las políticas de seguridad de la solución de seguridad perimetral.
Meta porcentual del indicador:	Mínima: 70-80% Aceptable: 80-90% Destacado: 100%
Fuente de información:	Manuales, procedimientos, roles, funciones y análisis del estado actual y planteamiento de la problemática a solucionar en términos de seguridad informática.
Fórmula de cálculo:	(% realizado analizado y reconfigurado / % esperado de avances

	De las nuevas políticas definidas para el firewall) * 100

Fuente del cuadro: Diseño propio.

Cuadro 2. Análisis de Seguridad Perimetral

7.1.7. *Políticas de Seguridad de la solución de Firewall FortiGate 200E y FortiMail 200E Existentes*

Actualmente existen una serie de controles y políticas de seguridad configuradas en ambos dispositivos, las cuales fueron diseñadas e implementadas por el anterior director del área TI en compañía de soporte experto en la materia.

A pesar de que dichas configuraciones han sido eficaces hasta la fecha, existentes muchas otras de las cuales no se tiene compresión, al igual que otras que posiblemente no estén funcionando; además no existe una documentación o registro sobre las políticas existentes o los cambios que han presentado o que han sido necesarios debido a una solicitud.

Siguiendo la formula del indicador de gestión sobre el firewall, se considera que el cumplimento se encuentra en un nivel aceptable con **80%** de calificación, esto debido a que no existe documentación de los controles y cambios en el firewall, además, recientemente se han presentado casos de virus y algunos ataques cibernéticos menores, pero que han logrado pasar el firewall. Adicionalmente, el equipo actual de TI no tiene conocimientos amplios en el manejo y configuración de esta solución de Firewall.

INDICADOR #3 – GESTIÓN DE LOS ACTIVOS TECNOLOGICOS (PDS)	
Código Indicador:	PDS - 2.0.0
Fecha de creación:	10 de noviembre de 2021
Fecha última actualización:	---
Título del indicador:	Valoración de la gestión y seguridad de los activos de cómputo de la compañía.
Objetivo:	Identificar y analizar el porcentaje de gestión y control que se lleva sobre los activos de software y hardware como servidores, equipos de usuarios, equipos de interconexión de red, software y licenciamiento instalados, entre otros.
Soporte de medida:	medida porcentual de avance de las políticas de control, gestión y protección de los recursos tecnológicos de la compañía.

Meta porcentual del indicador:	Mínima: 70-80% Aceptable: 80-90% Destacado: 100%
Fuente de información:	Inventario de equipos (si existe), inventario de software (si existe), licenciamiento, políticas locales en cada equipo y configuradas desde el servidor de dominio, entre otros.
Fórmula de cálculo:	(% existente analizado y reconfigurado / % esperado de avances De los controles y gestión de activos de software y hardware) * 100

Fuente del cuadro: Diseño propio.

Cuadro 3. Gestion de Activos Tecnológicos

7.1.8. *Gestion y Seguridad de los Activos Tecnológicos Existentes*

Actualmente, en cuanto a la gestión de TI desde la prestación del servicio, se a implementado un archivo de Excel compartido en OneDrive donde el equipo TI registra todas las solicitudes y eventos de sistemas que requieren de soporte o

intervención, esto con el objetivo de poder llevar una base de datos del conocimiento y realizar análisis de los eventos y sus características.

En cuanto a políticas establecidas desde el dominio y también localmente en los equipos de cómputo, existen políticas como el bloqueo del panel de control, fondo de pantalla y otras, y en cuanto a los equipos, se han desactivado permisos de administrador local en la mayoría.

Por último, se cuenta con un inventario de activos tecnológicos en un archivo de Excel, el cual recopila principalmente todas las computadoras, servidores, Ups, impresoras y equipos de interconexión como switches. Adicionalmente, el archivo también recopila el software instalado en dichos equipos y digitalmente en una carpeta se encuentran imágenes de todos los equipos con las licencias del software con el que cuenta cada uno y sus respectivas facturas de compra en algunos casos, y también existe una carpeta física con las demás licencias pertinentes al Core de comunicaciones en general.

Siguiendo la formula del indicador de gestión sobre la seguridad de los activos tecnológicos, se considera que el cumplimento se encuentra en un nivel aceptable con **90%** de calificación, esto debido a que se cuenta con la mayoría de los controles necesarios para alcanzar el nivel destacado y solo requeriría de afinamiento, como por ejemplo: rotular la totalidad de los activos tecnológicos, incluir activos tecnológicos de todo tipo, no solo computadoras, servidores y equipos de networking, entre otros.

En cuanto a la gestión de eventos que es llevada en un archivo de Excel en OneDrive, lo ideal sería implementar una herramienta de software más sofisticada que convine tiquetera, inventario de equipos, base de datos del conocimiento y reportes personalizables.

Sobre las políticas desde el dominio y localmente, se trataría básicamente de confirmar que todos los equipos de cómputo están debidamente configurados en este sentido y corregir en caso de no ser así, para luego aplicar dichas políticas o crear nuevas y vigilar su comportamiento.

En cuanto al inventario como tal, este requiere integrar todos los equipos de naturaleza tecnológica, no solo servidores, computadoras y equipos de interconexión de red o eléctricos, también teléfonos IP, Wifi´s, Router´s u otros.

INDICADOR #4 – PROTECCION LOCAL DE LOS EQUIPOS DE COMPUTO (PDS)	
Código Indicador:	PDS - 2.1.1
Fecha de creación:	10 de noviembre de 2021
Fecha última actualización:	---
Título del indicador:	Valoración de la protección brindada por el Antivirus Kaspersky Endpoint Security en los equipos de cómputo.
Objetivo:	Identificar y analizar el porcentaje de protección que se lleva sobre los equipos de computo donde se encuentre instalado el software Kaspersky Endpoint Security.

Soporte de medida:	medida porcentual de avance de las políticas de protección de los equipos de cómputo de la compañía.
Meta porcentual del indicador:	Mínima: 70-80% Aceptable: 80-90% Destacado: 100%
Fuente de información:	Consola de administración de Kaspersky Endpoint Security, software instalado en cada máquina, versiones, actualizaciones, políticas sobre la consola.
Fórmula de cálculo:	(# de equipos con antivirus instalado y actualizado / # de total de equipos con antivirus debidamente configurado y actualizado) * 100

Fuente del cuadro: Diseño propio.

Cuadro 4. Protección Equipos de Computo

7.1.9. *Protección por Software Antivirus Existente*

Actualmente se cuenta con 130 licencias del antivirus Kaspersky Endpoint Security y una consola de administración desde un servidor virtual.

Siguiendo la formula del indicador de gestión sobre protección local de os equipos de cómputo, se considera que el cumplimento se encuentra en un nivel aceptable con **85%** de calificación, esto debido a que, aunque los antivirus se encuentran instalados en la totalidad de los equipos, muchos de ellos no se actualizan automáticamente y la consola de administración tampoco está cumpliendo dicha función.

7.1.10. *Fase 3*

7.1.11. *Evaluación de Riesgos*

Una metodología que nos permite realizar análisis de riesgos y ser apoyo a los postulados de NIST es MAGERIT v3**.**

Inicialmente debemos identificar los activos de información, procesos y recursos de la compañía; MAGERIT afirma que un activo es un componente o funcionalidad de un sistema de información susceptible a ser atacado, trayendo problemas para la organización. Un activo incluye: información, datos, servicios, aplicaciones

(software), maquinas (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos.[50]

Acto seguido debemos identificar todos los componentes fundamentales para la operación de la compañía, actividades o elementos sin los cuales el negocio no podría operar.

MAGERIT clasifica los activos de la siguiente manera:

[D] Datos/Información: Se refiere a los datos generados, procesados, y que se almacenan y/o eliminan, relacionados a un servicio prestado por la compañía.

[S] Servicios. Actividades ejecutadas para que los procesos de la compañía funcionen correctamente, satisfaciendo las necesidades de los usuarios internos y externos.

[SW] Software – Aplicaciones de Informática. Los programas o aplicaciones con los cuales se procesan y registran los datos de la compañía.

[HW] Hardware – Equipos de Informática. Parte física, lugar donde se instalan los programas informáticos y se manipulan los datos de la compañía, como servidores, computadoras, dispositivos de seguridad, etc.

[COM] Redes de Comunicaciones. Se refiere a los componentes que conectan la red y permiten intercambiar datos entre los equipos informáticos.

[50] Magerit V3, Libro I. Metodología MAGERIT. Consultado el 12 de noviembre de 2021. Obtenido de: https://www.ccn-cert.cni.es/documentos-publicos/1789-magerit-libro-i-metodo/file.html

[MEDIA] Soporte de Información. Equipos físicos donde se almacena la información de manera permanente o por periodos muy extensos, como son: Cajas de discos, cintas magnéticas, memoria USB, etc.

[AUX] Equipamiento Auxiliar. Dispositivos que soportan equipos informáticos como: fuentes de poder, circuitos eléctricos, escritorios, entre otros.

[L] Instalaciones. Ubicación física donde se encuentran instalados todos los equipos o recursos tecnológicos.

[P] Personas. Se refiere al personal de TI o que tenga a cargo funciones dentro de dicha área.

Teniendo en cuenta que dichos componentes ya fueron identificados en la fase 2, se procede a describir la manera como se llevara a cabo el análisis.

El análisis de riesgos se realiza de cuatro pasos:

7.1.12. *Primer Paso*

Tabla 1. Descripción del Método de Análisis de Riesgo

Análisis de riesgos	
Paso 1: Caracterización de los activos	Tarea T1.1: Identificación de los activos Tarea T1.2: Valoración de los activos
Paso 2: Caracterización de las amenazas	Tarea T2.1: Identificación de las amenazas Tarea T2.2: Valoración de las amenazas
Paso 3:	Tarea T3.1: Identificación de las salvaguardas

Caracterización de las salvaguardas	Tarea T3.2: Valoración de las salvaguardas
Paso 4: Estimación del estado del riesgo	Tarea T4.1: Estimación del impacto Tarea T4.2: Estimación del riesgo

Fuente de la tabla: Diseño propio.

7.1.13. *Caracterización de los Activos*

7.1.14. *Tarea T.1.1. Identificación de los Activos*

Se identifican los activos tecnológicos y de ciberseguridad más importantes de la compañía, los cuales son clasificados e identificados con un código, nombre, descripción, tipo de activo al que pertenece y cantidad.

7.1.15. *Aplicaciones (Software)*

Tabla 2. Aplicaciones y Software

No.	Item Activo	Nombre del activo	Descripción del activo	Tipo de activo	Función del activo	cantidad
1	ERP – Siesa Enterprise	Uno Enterprise	Software para gestión contable, comercial y de cartera.	Aplicación (Tercero)	Procesamiento y administración de datos financieros en general.	01
2	ERP – Siesa Enterprise	Nomina Web	Software para la gestión de nómina.	Aplicación (Tercero)	Procesamiento y registro de datos de nomina.	01
3	ERP – Siesa Enterprise	Siesa Access	Software para registro y gestión de marcación en	Aplicación (Tercero)	Protección de ataques cibernéticos y malware.	04

			lectores biométricos.			
4	Software Antivirus Kaspersky Endpoint Security	Aplicación de Antivirus.	Programa para la detección, prevención y eliminación de virus informático.	Aplicación	Protección ante virus informático.	130
5	Plataforma Virtual de Servidores	Plataforma Virtual VMWare – Dell de Servidores	Appliance diseñado para virtualizar todo el Core de servidores.	Aplicación	Ambiente de Core de Servidores en máquinas virtuales.	8 Máquinas Virtuales

Fuente de la tabla: Diseño propio.

7.1.16. *Activos (Hardware)*

Tabla 3. Activos Críticos (Hardware)

No.	Item Activo	Nombre del activo	Descripción del activo	Tipo de activo	Función del activo	cantidad
1	Solución Fortinet	Appliance de seguridad perimetral (FortiGate, FortiMail, FortiAuthenticator y FortiVoice).	Programas informáticos para sistemas operativos.	Hardware y Aplicación	Protección de ataques cibernéticos y malware.	04
2	Rack de Servidores Principal	Armario de servidores Físicos.	Rack que contiene e interconecta servidores.	Hardware	Almacenar y soportar Appliance VMWare-Dell.	04

3	Rack Servidor – Planta de Producción	Armario único de servidor Físico y Firewall.	Rack que contiene servidor y Firewall	Hardware	Almacenar, soportar y administrar la red de la sede de producción.	02
4	Equipos de Computo	Computadoras portátiles y de escritorio	Computadoras de diferentes fabricantes dispuestas en los centros de trabajo para el uso de los usuarios de la red corporativa.	Hardware y Software	Equipos para el procesamiento y almacenamiento de datos	130

Fuente de la tabla: Diseño propio.

7.1.17. *Redes de Comunicaciones*

Tabla 4. Dispositivos de Interconexión Críticos

No.	Item Activo	Nombre del activo	Descripción del activo	Tipo de activo	Función del activo	cantidad
1	Rack de Comunicaciones Sede Principal	Armario de dispositivos de interconexión	Rack que soporta y contiene dispositivos de interconexión de la red corporativa.	Hardware	Almacenar y soportar dispositivos networking.	05
2	Rack de Comunicaciones Sede Producción	Armario de dispositivos de interconexión en oficina planta de producción	Rack que soporta y contiene dispositivos de interconexión de la red corporativa en planta de producción.	Hardware	Almacenar y soportar dispositivos networking.	02

Fuente de la tabla: Diseño propio.

7.1.18. *Soporte de Información*

Tabla 5. Dispositivos para Salvaguardar Información

No.	Item Activo	Nombre del activo	Descripción del activo	Tipo de activo	Función del activo	cantidad
1	Biblioteca de Cintas – Sede Principal	Biblioteca de Cintas Magnéticas	Equipo diseñado para gestionar cintas magnéticas.	Hardware	Alojar copias de información en cintas magnéticas.	01
2	Disco duro 1 Tera – Planta de Producción	Disco Backup	Disco conectado en rack USB al servidor para alojar copias de seguridad de información del servidor de planta de producción.	Hardware	Almacenar información de unidades de red del servidor de planta de producción.	01

Fuente de la tabla: Diseño propio.

7.1.19. *Equipamiento Auxiliar*

Tabla 6. Dispositivos Eléctricos de Protección

No.	Item Activo	Nombre del activo	Descripción del activo	Tipo de activo	Función del activo	cantidad
1	Rack Eléctrico Sede Principal	Armario de circuitos y UPS	Rack que contiene cableado de circuitos eléctricos y UPS de respaldo.	Hardware	Protección y funcionamiento eléctrico de los equipos de cómputo y Data Center principal.	01
2	UPS Servidor	UPS	Equipo de soporte y protección para	Hardware	Soporte y protección	01

	Planta de Producción		el respaldo del servidor.		eléctrica de servidor y comunicaciones de planta de producción.	

Fuente de la tabla: Diseño propio.

Instalaciones

- Guadalajara de Buga (Sede Principal – Data Center)
- Km 8 Vía Buga / Buenaventura (Planta de Producción)

Personal de TI

- Director IT
- Asistente IT
- Practicante IT

7.1.20. *Tarea T.1.2. Valoración de los Activos*

Se valoran los activos más importantes de la compañía mediante entrevistas con las personas responsables de los activos.

Para la valoración de los activos se establecen tres dimensiones básicas: Disponibilidad (D), Integridad (I) y Confidencialidad (C). MAGERIT propone una cuarta dimensión llamada Autenticidad (A), sin embargo, se considera que no es necesaria para este caso.

Tabla 7. Dimensiones de valoración de los activos

Dimensión	Descripción
Disponibilidad	Importancia del activo al no estar disponible y gravedad de sus consecuencias.
Integridad	Importancia del activo al sufrir modificaciones sin supervisión.
Confidencialidad	Nivel de gravedad si personas no autorizadas acceden a información restringida del activo.
Autenticidad (NO APLICA)	Importancia que tendría el evento en que quien acceda a la información no sea realmente quien tiene permisos.

Fuente de la tabla: Diseño propio.

Se valora la lista de activos de la Tarea T1.2, lo cual permitió determinar los resultados de daños muy graves a la organización con su respectiva calificación.

Tabla 8. Criterios de valoración de MAGERIT para activos

Valor		Criterio
10	Muy alto	Daño muy grave a la organización
7-9	alto	Daño grave a la organización
4-6	medio	Daño importante a la organización
1-3	bajo	Daño menor a la organización
0	despreciable	Irrelevante a efectos prácticos

Fuente de la tabla: Diseño propio.

Tabla 9. Valoración Aplicaciones y Software

Valoración de Software informático					
No.	**Nombre del Activo**	**Valoración de Activos**			
		D	**I**	**C**	**Resultado de valoración**
1	Uno EE	10	9	10	**10**
2	Nomina Web	10	9	10	**10**
3	Siesa Access	10	9	10	**10**
4	Software de Antivirus	10	9	10	**10**
5	Plataforma Virtual VMWare - Dell	10	10	10	**10**

Fuente de la tabla: Diseño propio.

Tabla 10. Valoración Activos Críticos (hardware)

Valoración de Hardware					
No.	**Nombre del Activo**	**Valoración de Activos**			
		D	**I**	**C**	**Resultado de valoración**
1	Appliance Seguridad Perimetral	10	10	10	**10**
2	Rack Servidor Físico Principal	10	10	10	**10**
3	Rack Servidor Planta de Producción	10	10	10	**10**
4	Computadoras	6	6	8	**7**

Fuente de la tabla: Diseño propio.

Tabla 11. Valoración Dispositivos de Interconexión Críticos

Valoración Equipos de Networking					
No.	Nombre del Activo	Valoración de Activos			
		D	I	C	Resultado de valoración
1	Rack de Comunicaciones Sede Principal	10	9	9	9
2	Rack Comunicaciones Sede Producción	10	9	9	9

Fuente de la tabla: Diseño propio.

Tabla 12. Valoración Dispositivos para Salvaguardar Información

Valoración Backup Información					
No.	Nombre del Activo	Valoración de Activos			
		D	I	C	Resultado de valoración
1	Biblioteca de Cintas de Backup	10	10	10	10
2	Disco Duro Copias Planta de Producción	10	10	10	10

Fuente de la tabla: Diseño propio.

Tabla 13. Valoración Dispositivos Eléctricos de Protección

Valoración Equipos Electricos					
No.	Nombre del Activo	Valoración de Activos			
		D	I	C	Resultado de valoración
1	Rack Eléctrico Sede Principal	10	10	10	10
2	UPS Rack Servidor Planta de Producción	10	10	10	10

Fuente de la tabla: Diseño propio.

A continuación, se detallan mediante otra tabla todos los activos analizados dentro de la gestión de riesgos según su criticidad.

Tabla 14. Activos con criticidad: Muy Alto, Alto y Medio

Tipo	Activo	Criticidad
Software y Aplicaciones	Uno EE	Muy Alto
	Nomina Web	
	Siesa Access	
	Software Antivirus	
	Plataforma Virtual VMWare - Dell	
Hardware	Appliance Seguridad Perimetral	Alto
	Rack Servidor Físico Principal	
	Computadoras	
Networking	Rack de Comunicaciones Sede Principal	Alto
	Rack de Comunicaciones Sede Producción	

Soporte de información	Biblioteca de Cintas Magnéticas	**Muy Alto**
	Disco Duro Copias Rack Servidor de Producción	
Equipamiento auxiliar	Rack Eléctrico Sede Principal UPS Rack servidor sede Producción	**Muy alto**

Fuente de la tabla: Diseño propio.

7.1.21. *Segundo Paso: Caracterización de las Amenazas*

7.1.22. *Tarea T.2.1. Identificación de las Amenazas*

El objetivo de la Tarea T2.1 es identificar todas las amenazas relevantes que atentan sobre los activos de TI con calificación “Muy Alto” y “Alto”.

MAGERIT V3, define y agrupa las amenazas típicas asociadas a un sistema de información.

De origen natural:

- Terremotos
- Inundaciones
- Erupción Volcánica

De origen industrial:

- Causadas por el personal
- Daños causados por agua o fuego

Errores y fallos no intencionados:

- Errores de usuarios
- Errores de administradores
- Deficiencias de la organización.

Ataques intencionados:

- Manipulación de registros
- Manipulación de configuraciones
- Abuso de accesos
- Ataques cibernéticos
- Abuso de privilegios o permisos

Tabla 15. Identificación de las amenazas que atentan a las aplicaciones de software.

Amenazas		Siesa EE	Nomina Web	Siesa Access	Software Antivirus	Plataforma VMWare - Dell
De origen natural	Terremoto	**X**	**X**	**X**	**X**	**X**
De origen industrial	Desastre de origen físico o lógico	**X**	**X**	**X**	**X**	**X**
	Errores de usuarios				**X**	

Errores y fallos no intencionados	Errores de Administradores de la red	X	X	X	X	X
	Deficiencias de la organización	X	X	X	X	X
	Alteración accidental de la información	X	X	X		
Ataques intencionados	Manipulación de registros	X	X	X		X
	Manipulación de configuraciones	X	X	X	X	X
	Abuso de accesos	X	X	X	X	X
	Ataques Cibernéticos	X	X	X		X
	Abuso de privilegios	X	X	X	X	X
	Ciberataques	X	X	X	X	X

Fuente de la tabla: Diseño propio.

Tabla 16. Identificación de las amenazas que atentan a los activos críticos (hardware).

Amenazas		Appliance Seguridad Perimetral	Rack Servidores sede Principal	Rack Servidores sede Producción	Computadoras
Deo	Fuego	X	X	X	X
	Daños por agua	X	X	X	X
	Desastres naturales	X	X	X	X

rigennatural					
De origen industrial	Fuego Causados	**X**	**X**	**X**	**X**
	Daños por agua Causados	**X**	**X**	**X**	**X**
	Condiciones inadecuadas de temperatura y/o humedad			**X**	**X**
	Errores de usuarios				**X**
	Errores de administradores	**X**	**X**	**X**	**X**
	Robo				**X**

Errores y fallos no intencionados	Errores de mantenimiento / actualización de equipos	**X**	**X**	**X**	**X**
Ataque	Abuso de privilegios Ciberataques	**X** **X**	**X** **X**	**X** **X**	**X** **X**

sintencionados						
	Abuso de privilegios	**X**	**X**	**X**	**X**	**X**
	Ciberataques	**X**	**X**	**X**	**X**	**X**

Fuente de la tabla: Diseño propio.

Tabla 17. Identificación de las amenazas que atentan el networking.

Amenazas		**Rack de Comunicaciones Sede Principal**	**Rack de Comunicaciones Sede Producción**
De origen natural	Desastres naturales	**X**	**X**
De origen industrial	Fuego Causado	**X**	**X**
	Daños por agua Causado	**X**	**X**
	Condiciones inadecuadas de	**X**	

	temperatura y/o humedad		
Errores y fallos no intencionados	Error de usuarios		
	Errores de administradores	**X**	**X**
	Suplantación		
	Errores de mantenimiento / actualización de equipos	**X**	**X**
Ataques intencionados	Abuso de privilegios	**X**	**X**
	Ciberataques	**X**	**X**

Fuente de la tabla: Diseño propio.

Tabla 18. Identificación de amenazas que atentan al soporte de información.

Amenazas		**Biblioteca de Cintas Magnéticas**	**Disco Duro Copias Rack Servidor sede Producción**
De origen natural	Desastres naturales	**X**	**X**
	Daños por agua	**X**	**X**
	Fuego	**X**	**X**
De origen industrial	Fuego causado	**X**	**X**
	Daños por agua causado	**X**	**X**
	Condiciones inadecuadas de temperatura y/o humedad	**X**	**X**

Errores y fallos no intencionados	Robo		X
	Errores de administradores	X	X
	Errores de mantenimiento / actualización de equipos	X	X
Ataques intencionados	Revelación de información	X	X

Fuente de la tabla: Diseño propio.

Tabla 19. Identificación de las amenazas que atentan a los equipos de protección eléctrica.

Amenazas		Rack Eléctrico sede Principal	UPS Rack Servidor sede Producción
De origen natural	Desastres naturales	X	X
	Daños por agua	X	X
	Fuego	X	X
De origen industrial	Fuego causado		X
	Daños por agua causado	X	X
	Condiciones inadecuadas de temperatura y/o humedad		X
Errores y fallos no intencionados	Robo		X
	Errores de administradores	X	X
	Errores de mantenimiento /	X	X

	actualización de equipos		
Ataques intencionados	Uso no previsto	**X**	**X**
	Ciberataques	**X**	**X**

Fuente de la tabla: Diseño propio.

7.1.23. *Tarea T.2.2. Valoración de las Amenazas*

Una vez identificadas las amenazas que pueden afectar los recursos tecnológicos de la compañía, se procede a realizar valoración de las amenazas mediante dos ítems: “daño causado” (degradación del activo) y “estimación de ocurrencia” (probabilidad).

Degradación del activo:

Tabla 20. Valores de degradación que causan las amenazas

Criterio	valor		
Degradación muy considerable del activo	**Alta**	A	80%-100%
Degradación medianamente considerable del activo	**Media**	M	30%-79%
Degradación poco considerable del activo	**Baja**	B	1%-29%

Fuente de la tabla: Diseño propio.

Tabla 21. Valoración de amenazas por degradación en aplicaciones y software en general.

Aplicativos	Amenazas		Degradación		
			D	I	C
Uno EE Nomina Web Siesa Access Appliance VMWare-Dell Sistema de antivirus	De origen natural	Desastre natural Desastre por agua Desastre por fuego	95%		
	De origen industrial	Avería de origen Físico o lógico.	80%		
	Errores y fallos no intencionados	Errores de usuarios	20%	60%	50%
		Errores de administradores	20%	40%	40%
		Deficiencias de la organización	70%	50%	60%
		Alteración accidental de la información	90%	70%	70%
	Ataques intencionados	Manipulación de registros	90%	70%	70%
		Manipulación de configuraciones	90%	70%	70%
		Abuso de accesos Ciberataques	90%	60%	80%

Fuente de la tabla: Diseño propio.

Tabla 22. Valoración de las amenazas por degradación en equipos informáticos (hardware)

Hardware	Amenazas		Degradación		
			D	I	C
Equipos de trabajo Servidor de dominio Router (Cortafuegos)	De origen natural	Fuego	80%		
		Daños por agua	80%		
		Desastres naturales	80%		
	De origen industrial	Fuego causado	80%		
		Daños por agua causado	80%		
		Condiciones inadecuadas de temperatura y/o humedad	70%		
	Errores y fallos no intencionados	Errores de usuarios	70%	60%	50%
		Errores de administradores	40%	60%	50%
	Ataques intencionados	Abuso de privilegios Ciberataques	70%	60%	50%

Fuente de la tabla: Diseño propio.

Tabla 23. Valoración de las amenazas por degradación en recursos tecnológicos críticos de hardware como servidores, dispositivos de networking, dispositivos de respaldo.

Hardware	Amenazas		Degradación		
			D	I	C
Rack de Servidores Rack de Comunicaciones Rack Eléctrico Computadoras Dispositivos de Respaldo	De origen natural	Fuego	80%		
		Daños por agua	80%		
		Desastres naturales	80%		
	De origen industrial	Fuego causado	80%		
		Daños por agua causado	80%		
		Condiciones inadecuadas de temperatura y/o humedad	70%		
	Errores y fallos no intencionados	Errores de usuarios	70%	60%	50%
		Errores de administradores	40%	60%	50%
	Ataques intencionados	Abuso de privilegios Ciberataques	70%	60%	50%

Fuente de la tabla: Diseño propio.

Frecuencia de la amenaza (probabilidad): Tasa de ocurrencia de una amenaza. Para valorar la frecuencia de la amenaza se utiliza la escala definida por la metodología MAGERIT de la siguiente forma:

Tabla 24. Valores de probabilidad de ocurrencia de una amenaza.

Criterio	Valor
Prácticamente seguro	**MA**
Probable	**A**
Posible	**M**
Poco probable	**B**
Muy raro	**MB**

Fuente de la tabla: Diseño propio.

Tabla 25. Valoración de las amenazas por probabilidad en aplicativos.

Aplicativos	Amenazas		Probabilidad
	De origen natural	Desastre ambiental	**M**
Uno EE **Nomina Web** **Siesa Access**	**De origen industrial**	Avería de origen Físico o lógico.	**M**
	Errores y fallos no intencionados	Errores de usuarios	**M**
		Errores de administradores	**M**
		Deficiencias de la organización	**B**
		Alteración accidental de la información	**B**

Appliance VMWare-Dell	**Ataques intencionados**	Manipulación de registros	**B**
		Manipulación de configuraciones	**B**
		Abuso de accesos	**B**
		Ciber ataques	**M**

Fuente de la tabla: Diseño propio.

Tabla 26. Valoración de las amenazas por probabilidad en activos informáticos (hardware)

Hardware	Amenazas		Probabilidad
Rack de Servidores	**De origen natural**	Fuego	**B**
		Daños por agua	**M**
		Desastres naturales	**M**
Rack de Comunicaciones	**De origen industrial**	Fuego causado	**B**
		Daños por agua causado	**B**
Computadoras		Condiciones inadecuadas de temperatura y/o humedad	**B**
Dispositivos de Respaldo	**Errores y fallos no intencionados**	Errores de administradores	**B**

	Ataques intencionados	Abuso de privilegios	**M**
		Ciberataque	**M**

Fuente de la tabla: Diseño propio.

Tabla 27. Valoración de las amenazas por probabilidad a los equipamientos auxiliares.

equipamientos auxiliares	Amenazas		Probabilidad
Rack Eléctrico **UPS**	**De origen natural**	Desastres naturales	M
		Daños por agua	M
		Fuego	B
	De origen industrial	Fuego causado	B
		Daños por agua causado	B
		Condiciones inadecuadas de temperatura y/o humedad	B
	Errores y fallos no intencionados	Robo	B
		Errores de administradores	B
		Errores de mantenimiento / actualización de equipos	B
	Ataques intencionados	Ataque destructivo Ciberataque	M B

Fuente de la tabla: Diseño propio.

7.1.24. *Tarea T.2.2. Fase 4: Perfil Objetivo*

Tomando como base los indicadores de gestión y el análisis de riesgos a partir de método MAGERIT, se concluye que los items a tomar en cuenta para la debida operación, gobernanzas y mitigación de riesgos de seguridad y ciberseguridad dentro del PDS de la compañía Pronavicola S.A. son los siguientes:

- Rediseño de las políticas de seguridad informática, con revisión y actualización al menos una vez cada dos años. Esto con el objetivo de garantizar el uso adecuado de todos los recursos tecnológicos por parte de los usuarios y responsables de la gestión.
- Reorganización y afinamiento de políticas establecidas desde el servidor de dominio, así como los grupos de usuarios existentes y sus permisos dentro de la red corporativa.
- Reorganización, afinamiento y documentación de las políticas y configuraciones de ciberseguridad establecidas en el Firewall Fortigate 200E y FortiMail 200E principalmente. De esta manera se podrá tener plena certeza de cómo está protegida la compañía y donde hay brechas de ciberseguridad.
- Afinamiento del inventario de activos de la compañía, recopilando todos los activos existentes y categorizándolos según su tipo y función, además de rotulación de los mismos. Esto con el objetivo de tener control absoluto de los activos tecnológicos.
- Adquisición de aplicativo para la gestión de eventos (tickets de soporte) e incidentes de seguridad.
- Afinamiento de la configuración de las licencias Endpoint de Kaspersky en los equipos de cómputo para su debida actualización y protección de los equipos.

- Charlas de concientización sobre seguridad informática y divulgación de las políticas existentes.
- Capacitación en el uso y administración de la solución de seguridad perimetral Fortinet para el área IT.

Teniendo en cuenta los anteriores ítems como objetivos alineados a la misión y visión de la compañía, así como a los objetivos de TI trazados durante el planteamiento de este trabajo, se puede afirmar que una vez sean elaboradoras y afinados estos puntos, la compañía gozara de una excelente protección, gobernanza y gestión de TI, alcanzando su punto máximo de satisfacción.

7.1.25. *Fase 5: Análisis de Brechas*

Comparando el perfil actual versus el perfil objetivo, se concluye que la mayoría de las actividades que se requieren para la elaboración de un PDS acorde a la necesidad de la compañía son de tipo afinamiento y reorganización de los controles existentes, los cuales se encuentran en un nivel de funcionamiento aceptable.

Se da inicio al desarrollo de las actividades y proyectos que no requieren inversión monetaria como tal, pero si recurso humano y temporal, de esta forma, el asistente IT de la compañía y desarrollador de este trabajo elabora el diseño de la nueva política de seguridad informática y propuesta de proyecto de capacitación y sensibilización de ciberseguridad e ingeniería social.

Dichos proyectos son presentados y posteriormente implementados por la compañía en el tiempo y momento que lo considere pertinente.

A continuación, se realiza la propuesta desde el punto 7 de este trabajo (Desarrollo de los Objetivos) cumpliendo así con el curso del proyecto.

Los demás proyectos serán propuestos y desarrollados a lo largo de este trabajo, al igual que los costos que requieren algunos de ellos.

8. DESARROLLO DE LOS OBJETIVOS ESPECIFICOS

8.1.1. POLITICA DE SEGURIDAD - DESARROLLO DE OBJETIVO 1

Propuesta para la nueva política de seguridad informática de la compañía Pronavicola S.A.

DEPARTAMENTO DE TECNOLOGIA E INFORMATICA

Políticas de Seguridad y Privacidad de la Información (PDS)

Responsables: Directivas, Área IT, Usuarios.

El propósito del Departamento de Tecnología e Informática de PRONAVICOLA S.A. es presentar una política del correcto uso de los recursos tecnológicos suministrados para el trabajo diario, apoyo a la misión y objetivos de la compañía y garantizar la disponibilidad, integridad y confiabilidad de toda la información de la organización.

Toda información en medios electrónicos, red corporativa, infraestructura de red (abarcando equipos de comunicación e interconexión, computadoras, tabletas, e incluso teléfonos fijos o celulares, aplicaciones de software, sistemas operativos, medios o unidades de almacenamiento, cuentas de correo electrónico corporativo, mensajes, páginas o portales Web, bases de datos y cualquier archivo que pueda ser descargado de la red corporativa) pertenecen y son de propiedad exclusiva de

PRONAVICOLA S.A.. Estos sistemas deben ser utilizados únicamente en actividades propias de la compañía y al servicio de los intereses de la misma.[51]

La efectividad de políticas de seguridad es una fuerza de equipo que involucra la participación y compromiso de todos y cada uno de los colaboradores de la compañía que de una manera u otra manipulen información y los sistemas en general de la compañía.

Es compromiso de cada colaborador que utilice una computadora y la red corporativa, conocer y acatar estas políticas mientras desarrolle sus actividades a nombre de la empresa.

Objetivos

- Detallar la correcta utilización de los servicios, aplicaciones de software, computadoras e infraestructura de red de PRONAVICOLA S.A.. Dichas normas buscan proteger la información, colaboradores y la compañía misma.
- Crear un ambiente de confianza para con los proveedores, aliados estratégicos, terceros y cualquier colaborador de la compañía.
- Establecer buenas prácticas y cultura de ciberseguridad entre todos los colaboradores de la compañía PRONAVICOLA S.A..

Alcance

Estas políticas están dirigidas a los colaboradores, contratistas o proveedores, personal temporal y personal vinculado con firmas que presten servicios a la compañía y que tengan acceso a sus recursos tecnológicos e información, así como a sus instalaciones en las diferentes sedes. Dichas políticas se aplican a todos los

51 Mintic. Seguridad y Privacidad de la Información. Actualizado el 11 de mayo de 2016. Disponible en: https://mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

equipos propios o arrendados que posea la compañía y a todo equipo que pertenezca a personas que se conecten dentro de la red corporativa.[52]

Nivel de Cumplimiento

Todos los colaboradores que sean arropados por el alcance de esta política deberán cumplirla a cabalidad en un 100%.

La garantía del cumplimiento de esta política será responsabilidad de cada miembro de PRONAVICOLA S.A. pues su desacato afecta a toda la compañía.

Es primordial señalar que el uso indebido de los recursos tecnológicos o el acceso a lugares o información restringida expone a la compañía a riesgos innecesarios como ciberataques, comprometer la integridad de la red corporativa en general y problemas legales a nivel nacional, e internacional.

La compañía PRONAVICOLA S.A. por tanto se compromete a:

- Proteger toda información procesada y resguardada dentro del marco de su existencia y razón de ser en la compañía con el objetivo de minimizar cualquier impacto negativo a las finanzas de la compañía.
- Proteger la información de cualquier ciberataque o riesgo que pueda provenir de los colaboradores, así como las instalaciones y centros de datos críticos para la compañía.
- Implementación de controles de acceso para los usuarios, información e instalaciones.

52 Blog Ceupe. Políticas de Seguridad de la Información y SGSI. Consultado el 19 de octubre de 2021. Disponible en: https://www.ceupe.com/blog/ejemplo-politica-seguridad-informacion-y-sgsi.html

- Garantizar en todo momento la disponibilidad y conectividad en todos los procesos que lleve a cabo la compañía.
- Garantizar el cumplimiento de obligaciones legales y regulatorias que sean establecidas.

Uso de la tecnología para el procesamiento y propiedad de la información

Responsables: Área IT, Usuarios.

Mientras las directivas de la compañía tengan como objetivo brindar un nivel óptimo de confidencialidad en la red corporativa, los usuarios deben ser conscientes que todos los datos que crean, gestionan y manipulan en la red o en las computadoras que les fueron asignadas durante el desarrollo normal de sus actividades, son propiedad y responsabilidad de la compañía. A pesar de esto y de la necesidad imperativa de proteger y vigilar la red corporativa y los recursos tecnológicos de la compañía, las directivas no pueden garantizar la completa confidencialidad e integridad de la información almacenada en los equipos de su propiedad.

Los colaboradores de PRONAVICOLA S.A. deben tener criterio suficiente para decidir cuándo pueden hacer uso personal de los recursos tecnológicos y así mismo serán responsables de dicha decisión.

Para propósitos de mantenimiento de la red corporativa, equipos de cómputo y seguridad de los mismos, el personal profesional en sistemas autorizado dentro de la compañía, podrá monitorear y analizar el uso y tráfico de red en todo momento.

La compañía PRONAVICOLA S.A. se reserva el derecho para auditar la red corporativa y todos los recursos tecnológicos periódicamente y sin previo aviso para garantizar el cumplimiento de todas las políticas.

Política de Uso de Teléfonos Celulares de la Compañía

Responsables: Área IT, Usuarios.

Los Ing. del área IT deberán entregar al usuario el nuevo equipo celular previamente configurado, cargado, en perfectas condiciones dentro de su caja original y con todos sus accesorios, acompañado de un acta de entrega que ambos deben firmar.

Si se trata de un teléfono inteligente el área IT creará una cuenta de Gmail o de iCloud (según la marca del equipo), necesaria para el uso de la Tienda de Aplicaciones y demás características del teléfono, lo anterior según el cargo o área donde se dispondrá de este, dicha cuenta no podrá ser cambiada por el usuario, tampoco su contraseña, por lo tanto, cualquier cambio que se requiera en su configuración solo puede ser realizado por un Ing. del área IT, así mismo con cualquier aplicación que se instale.

En caso de que el teléfono presente un mal funcionamiento o se dañe por cualquier motivo, el usuario deberá reportarlo al jefe inmediato y al área IT, explicando lo sucedido, luego, en base a dicho informe se determinará si se trata de un problema del equipo, si el usuario causó el daño de forma accidental, o si el usuario causó el daño por imprudencia y esto determinará la forma como se hará la reposición del equipo.

El usuario no puede instalar ninguna aplicación diferente a las que tenga al momento de la entrega, y, en caso de requerirse, deberá solicitar autorización al jefe inmediato y al área IT justificando la solicitud.

Cabe resaltar que el teléfono es de uso exclusivo de las actividades de la compañía, es decir, llamadas entre los demás usuarios que hacen parte del plan corporativo, intercambio de mensajes vía WhatsApp o SMS con los usuarios que hacen parte

del plan o la compañía, fotografías o videos relacionadas con las actividades del usuario y/o instalación de la App Outlook para descargar el correo del usuario; cualquier otra actividad o uso de este recurso con fines personales NO está permitido y podría ser considerado como un riesgo de seguridad informática, acarreando posibles llamados de atención o sanciones para el usuario.

Política de Control de Acceso, Resguardo y Controles de Seguridad de la Información

Responsables: Área IT, Usuarios.

Los usuarios deben crear contraseñas seguras y NO deben compartir su cuenta de usuario y contraseña con ningún otro usuario interno o externo por ningún motivo. Las contraseñas de acceso deben cumplir con los siguientes requisitos[53]:

- Debe tener mínimo 11 caracteres.
- Debe contener mínimo una letra mayúscula.
- Debe contener mínimo un caracter numérico.
- No debe iniciar por caracteres especiales (* / ¿ ¡, $, etc).
- No debe contener parte o todo el nombre del usuario de red.
- Tiene una vigencia de 42 días.

53 Cámara de Comercio de Honda. Política de Seguridad. Consultado el 19 de octubre de 2021. Disponible en: https://www.camarahonda.org.co/wp-content/uploads/2017/09/POLITICADESEGURIDADDELAINFORMACION.pdf

- No debe repetir sus contraseñas anteriores, se guarda historia de las 5 últimas.

- Todas las computadoras, portátiles y de escritorio, deben tener configurado un protector o bloqueo de pantalla con contraseña y tiempo de espera máximo de 5 minutos cuando el equipo se encuentre desatendido.

- Se recomienda NO modificar la firma de los mensajes de correo electrónico y las cubiertas de fax (en caso de ser usadas aun).
- Todos los equipos pertenecientes a la red corporativa de PRONAVICOLA S.A. aun siendo propiedad de la persona que lo utiliza, deben escanear regularmente la computadora (siguiendo indicaciones del área IT) con el software de antivirus adquirido y licenciado por la compañía o con el software que cuente el propietario, lo anterior con el fin de mantener la computadora protegida todo el tiempo.

- Todos los usuarios pertenecientes a la red corporativa de PRONAVICOLA S.A. deben ser precavidos al abrir anexos (attachments) adjuntos a los mensajes de correo electrónico que reciban de remitentes desconocidos o sospechosos ya que pueden contener virus y en caso de tener dudas comunicarse inmediatamente con el área IT.

- Por defecto el servidor de correos o firewall de correo bloquea las siguientes extensiones en los archivos adjuntos o attachments: *.aiff, *.asf, *.av, *.avi, *.bat, *.chm, *.cpl, *.crt, *.ink, *.reg, *.wsf, *.cob, *.com, *.dat, *.dll, *.dvr-ms, *.exe, *.midi, *.mp3, *.mp4, *.mpg, *.mpeg, *.pps, *.wav, *. wma, *.wmv, los cuales son formatos de video, audio, ejecutables

y otros que pueden ser sumamente peligrosos al usarse en la red corporativa.[54]

- Los puertos USB de los equipos de cómputo están restringido para todo el personal con excepción del Departamento IT, Gerencias, RTVs y Directores de Área y/o algún usuario el cual tenga una justificación valida y sea autorizado previamente por su jefe inmediato y el área TI, no obstante, cualquier usuario que traiga un Pen Drive o "Memoria USB" debe informar al Dpto. IT y permitir que un Ing. de área verifique que no representa ninguna amenaza.

- Todos los usuarios de la red corporativa de PRONAVICOLA S.A. deben almacenar la información de mayor relevancia e importancia para su trabajo en las unidades de red dispuestas por el área IT (PUBLICO Y USER) (en caso de contar con ellas o de tener una intranet), o en los espacios compartidos en la nube o a través de plataformas o aplicaciones permitidas por el Departamento IT. De esta misma forma los usuarios que no se encuentran permanentemente en las oficinas administrativas deben realizar copias de su información en otros medios, ya sea en un espacio en la nube, USB, CD`s, DVD`s, Disco Duro Externo o cualquier otro medio que garantice la integridad y resguardo de su información, ya que el Dpto. IT no puede garantizar la permanencia y totalidad de dicha información en caso de algún percance, falla sistemática o electrónica de la máquina. Si el usuario no es receptivo ante dichas recomendaciones y directrices el área tecnológica de la compañía no se hará responsable.

54 Sophos Central Admin. Tipos de archivos adjuntos de correo electrónico bloqueados por Sophos por defecto. Consultado el 19 de octubre de 2021. Disponible en: https://docs.sophos.com/central/Customer/help/es-es/central/Customer/concepts/SophosDefault.html

Control de Acceso al Data Center o Servidores

Responsables: Área IT.

El acceso a la compañía y en especial al Data Center o áreas de producción estará restringido, solo personal perteneciente a PRONAVICOLA S.A. que cuente con carnet y autorización previa de las directivas y área IT podrá ingresar.

Si una persona(s) externa debe ingresar a una de estas zonas deberá ser programado bajo calendario, estar acompañado de personal de PRONAVICOLA S.A. con permiso de acceso y registrado en una planilla detallando número de identificación del visitante, nombre, fecha entrada y salida, hora entrada y salida, motivo de la visita, elementos que ingresan y salen y observaciones.

Los espacios o vías de acceso, así como áreas seguras y emergencia deberán estar perfectamente demarcadas y detalladas.

Acceso a Internet y Portal Web de la Compañía

Responsables: Área IT, Usuarios.

Los permisos de navegación serán establecidos en base al rol y funciones que cumple el colaborador en la compañía, de esta forma se crearán en el servidor de dominio y firewall grupos con diferentes niveles de acceso así:

- Grupo Administradores
- Grupo Directores de Área
- Grupo Usuarios de red

Estos grupos tendrán perfiles de navegación que pueden ser ampliados o limitados según lo consideren directivas y área IT y serán delimitados de la siguiente forma:

- Navegación IT
- Navegación Administrativo
- Navegación Gerencia
- Navegación Operativo

De igual manera se determinarán los usuarios que gestionen y manipulen información en la aplicación web de la compañía, la cual será administrada por el área IT.

Acceso a las Redes Wi-Fi de Pronavicola

Responsables: Área IT, Usuarios.

El área IT dispondrá de dos redes Wi-Fi, una para los usuarios registrados en la compañía y otra para los usuarios visitantes de las instalaciones y las contraseñas de dichas redes deberán ser solicitados al área IT.

La primera (Wi-Fi Pronavicola) estará configurada para que los usuarios pertenecientes al dominio Pronavicola puedan conectarse y tener acceso a las unidades compartidas de red, impresoras y navegación a internet según aplique su perfil de navegación, cabe resaltar que dicha red NO está diseñada para ser usada por usuarios externos.

La segunda (Wi-Fi Invitados) estará configurada para que usuarios externos y ajenos a la red corporativa puedan conectarse y tener acceso únicamente a navegación en internet, la cual será controlada y monitoreada por una política de seguridad especial en el Firewall de seguridad de la compañía. Cabe resaltar que a

esta red también podrán conectase usuarios pertenecientes al dominio de Pronavicola, sin embargo, al igual que los usuarios externos solo tendrán acceso a navegar en internet bajo la misma política que los externos.

Las redes Wi-Fi están diseñadas para que los usuarios se conecten únicamente en el perímetro que comprende el interior de los edificios de Oficinas Buga, Planta de Incubacion (Wi-Fi Plantainc) y Planta de Alimento Balanceado (Wi-Fi PAB), ya que es el rango en que los equipos podrán conectarse con la potencia y estabilidad suficientes.

Los usuarios NO deben utilizar sus computadoras (Portátiles, Tablet´s, etc.) o teléfonos celulares para repetir o multiplicar dicha conexión con otros equipos, esta práctica será considerada peligrosa e irresponsable y podría acarrear llamados de atención o sanciones.

Dicha política podría sufrir cambios, mejoras o actualizaciones según lo disponga el área IT y así mismo dichos cambios serán divulgados vía correo electrónico.

Creación y Eliminación de Usuarios

Responsables: Área IT, Auditor Interno, Coordinador Mantenimiento

Al momento de ingresar un nuevo usuario (colaborador que tendrá acceso a la red corporativa) el jefe directo del mismo debe diligenciar un formato de creación de usuario que será solicitado al área IT, en dicho formato se determinará el nombre de usuario, correo electrónico (si se requiere), aplicativos a los que tendrá acceso y las carpetas compartidas a las que puede ingresar.

Adicional a dicho formato tendrá anexo un formato que deberá diligenciar en caso de que el usuario deba tener acceso a algún aplicativo del ERP de la compañía

(Siesa Enterprise) u otro, esto para determinar creación de usuario y/o permisos necesarios en dicho software.

Al momento de que determinado/s colaborador se retire de la compañía, las áreas involucradas deberán ser notificadas vía correo electrónico y deberán desactivar dicho/s usuario/s hasta que el formato de eliminación del mismo sea firmado y entregado a las áreas involucradas, posteriormente se hará efectiva su eliminación y todos los formatos deberán ser archivados.

Dichos formatos serán entregados a las áreas correspondientes, su diseño y autorización estarán sujetos a procedimientos clara y previamente descritos por cada departamento.

Cabe resaltar que la importancia de esta política reside en la trazabilidad que se debe dar a la existencia de un usuario en la red y la confidencialidad de la información que manipule, la cual no debe ser alterada ni borrada por el usuario ya que esto puede considerarse como un ataque consciente a la seguridad informática de la compañía y por tanto estaría sujeto de sanciones.

Gestion y Control de Activos

Responsables: Área IT

Todos los recursos tecnológicos como computadoras, servidores, routers, swtiches de interconexión, teléfonos inteligentes, etc. Deberán ser plenamente identificados, rotulados y clasificados dentro de un archivo o software de gestión de inventarios en el cual se podrá identificar ítems como:

- Características del recurso (portátil, escritorio, servidor u otro. Marca, modelo, capacidad de sus componentes, accesorios)

- Ubicación (país, ciudad, oficina, área a la que pertenece y usuario a quien fue asignado)
- Software legal que utiliza (sistema operativo y versión, paquete de aplicaciones de oficina y versión, otras aplicaciones y versión)
- Características comerciales y de adquisición (tipo de garantía, lapso de garantía, factura de venta, proveedor, imágenes del equipo, números de serie, entre otras)

Cabe resaltar que el documento donde se levante esta información no está limitado por estos ítems, pueden incluirse más siempre y cuando no confundan o distorsionen la información que se pretende identificar.

Rotulación de Activos

La forma como se rotularán los activos será por medio de una pequeña placa metálica que se colocará al costado o sobre el equipo, la cual tendrá un código dispuesto en base a estándares y normas legales para el caso. Dicha plata será entregada por un funcionario del área de Almacen y su colocación será labor de un integrante del área IT, lo anterior con el objetivo de tener control y claridad del equipo y su lugar en los activos financieros de la compañía, placa que NO podrá ser removida por el usuario. En caso de extraviarse deberá ser reportado inmediatamente por el usuario.

Entrega y Devolución de Activos

Cada equipo asignado se entregará junto con un acta oficial y una lista de chequeo que deberá ser firmada por el usuario para su posterior archivo en el área IT, de igual manera se procederá al momento de su devolución, lo anterior con el objetivo de tener control y trazabilidad sobre el estado del equipo y el cuidado que se le prestó.

Cabe resaltar que entrega y devolución solo puede celebrarse con acta en mano, bajo ningún motivo ninguna de las partes puede disponer del equipo sin este documento.

Disposición Final de Activos

Aquellos activos que el área TI considere y justifique son totalmente obsoletos e irreparables y que además estén total o parcialmente depreciados en los estados financieros de la compañía, serán identificados y plasmados en un acta la cual mencionara:

- Código de rotulación
- Estado y valor de depreciación
- Marca
- Modelo
- Número de serie
- Estado actual

Dicho documento será firmado por el director de IT, Director Contable, Auditor Interno (en caso de no existir dicha figura deberá crearse), Gerente Financiero y Gerente General.

Cabe mencionar que dicho documento puede contener otros ítems mientras no se distorsione la finalidad del mismo.

Es importante resaltar que su objetivo principal es y será siempre proteger a la compañía ante ataques o virus que puedan penetrar fácilmente en equipos con tecnología y versiones antiguas de software.

En caso de que los recursos tecnológicos sean propiedad de los usuarios, estos deberán someterse a los mencionados controles o recibir un nuevo equipo por parte de la compañía, por lo tanto, es sumamente recomendable que todos los activos sean propiedad de PRONAVICOLA S.A..

Política de Auditoría y Control Interno

Responsables: Directivas

Se creará la figura o el cargo de un especialista en auditoría interna (en caso de no existir) el cual deberá realizar evaluaciones periódicas del estado de las políticas de ciberseguridad y otras según lo disponga la compañía, velar por su cumplimiento dentro del alcance y normatividad legal y certificar la efectividad de las mismas, o bien, será contratado un servicio de auditoría externa que realice dicha labor.

Política de Gestion de Incidentes de Ciberseguridad

Responsables: Área IT

Todo evento que suponga un riesgo para la compañía en cuanto a la integridad de los datos, recursos tecnológicos y continuidad del negocio será registrado y documentado en acta o archivo donde se recopilará:

- Tipo de incidente
- Nivel de riesgo e impacto
- Infractor o sospechoso
- Descripción del incidente
- Información o recurso afectado
- Nivel de afectación
- Análisis de mitigación

- Solución y tiempo de respuesta ante el incidente
- Medidas correctivas y preventivas de mejora
- Documentación detallada en base del conocimiento
- Sanciones o implicaciones legales

Cabe mencionar que dicho documento puede contener otros ítems mientras no se distorsione la finalidad del mismo y sus hallazgos y correctivos serán compartidos con todos los colaboradores, así como las precauciones y acciones correctivas que deben realizar, esto con el objetivo de prevenir su repetición.

Todo usuario que no atienda a dichas recomendaciones e indicaciones estará incurriendo en una actividad que puede considerarse riesgosa para la compañía y por tanto acarrear llamados de atención o sanciones.

Política de Capacitación y sensibilización en Ciberseguridad

Responsables: Directivas, Área IT, Usuarios

Con previa aprobación e inclusión en el presupuesto por parte de las directivas de la compañía PRONAVICOLA S.A. se creará un programa de capacitación en buenas prácticas de ciberseguridad que estará dirigido a todos los colaboradores de la compañía, dicha iniciativa podrá llevarse a cabo de forma virtual, presencial o de forma combinada. Podrá contener información multimedia, cursos interactivos, practicas, tips, recomendaciones, entre otros.

Dichas actividades serán evaluadas para verificar su receptividad y aplicabilidad.

Cabe mencionar que dicha política estará abierta a cualquier sugerencia en pro de las mejores prácticas y ética profesional.

Política de No Repudio - Usos Inadecuados e incorrectos

Responsables: Área IT, Usuarios.

Bajo ninguna circunstancia los empleados de PRONAVICOLA S.A. pueden utilizar los recursos tecnológicos de la compañía para realizar actividades prohibidas por las normas de la compañía o por leyes jurídicas nacionales e internacionales.
A continuación, una lista de actividades que, sin ser integra o definitiva, intenta establecer una referencia de las actividades que se consideran indebidas para el uso de la red corporativa, correo electrónico y equipos de comunicaciones:

- Violación de los derechos de cualquier individuo o institución protegidos por derechos de autor, patentes o cualquier otra forma de propiedad intelectual.
- Distribución o instalación de software sin la licencia de uso adecuada adquirida por la compañía.

- Copia no autorizada de material protegido por derechos de autor que incluye, sin estar limitado a, digitalización y distribución de imágenes o fotografías de cualquier origen e índole (revistas, libros, páginas web, etc.) así como digitalización y distribución de música o contenido audiovisual.
- Instalación penetración de software malicioso en la red corporativa o en los servidores (virus, bots, correo spam, etc.).

- Revelar la contraseña o código de una cuenta de usuario a otros (ej: cuenta de correo electrónico, usuario de bases de datos, código de acceso a instalaciones, etc.) o permitir su uso a terceros para actividades ajenas a la misión de la compañía. La política de prohibición incluye familiares y cualquier otro individuo que conviva o haga parte del círculo personal del colaborador cuando la actividad se realiza desde su hogar u otra ubicación.

(ej: cuando el usuario utiliza equipos portátiles, celulares y demás equipos propiedad de la compañía).

- Utilizar la infraestructura tecnológica e informática de la compañía para adquirir o transmitir material con ánimo de lucro. Igualmente se prohíbe el uso del sistema de comunicaciones de la compañía para realizar alguna clase de difamación, acoso, calumnia o cualquier forma actividad hostil o intimidante.

- Realizar actos de corrupción con productos o servicios pertenecientes a la compañía.

- Llevar a cabo actividades que contravengan la seguridad de la red corporativa o que generen interrupciones en la operación y continuidad del negocio. Entre las acciones que contravienen la seguridad en la red se encuentran, sin estar limitada a estas, acceder o interceptar datos que no vayan dirigidos a usted, ingresar a una cuenta con privilegios de administrador o una aplicación para la cual no está autorizado. Interceptación de tráfico de red, asediar de comandos ping la red corporativa (ping es un comando que permite verificar que otro equipo está conectado y activo en la red), realizar spoofing de paquetes (spoofing es la falsificación de la dirección de la red), ataques de denegación de servicios (agresiones desde la red que buscan que servicios validos como el correo electrónico o el servidor web se “ocupen” y no atiendan a usuarios legítimos. Se conoce también como ataques DDoS) o falsificar información de enrutamiento y de configuración de los equipos y la red en busca de alguna vulnerabilidad.

- Está prohibido explícitamente el monitoreo de puertos o análisis de trafico de red con el propósito de evaluar vulnerabilidades de seguridad. Las personas

responsables de la seguridad informática pueden realizar dichas actividades en coordinación con el administrador de red y el director de IT.

- Ejecutar cualquier herramienta o mecanismo de monitoreo de red de manera No autorizada.

- Burlar los mecanismos de seguridad, autenticación, autorización o de auditoría de cualquier servicio de red, aplicación, servidor o cuenta de usuario.

- Interferir o negar el servicio a usuarios autorizados con el objetivo de entorpecer la prestación del servicio o la reputación de la compañía.

- Usar código, comandos o herramientas con el objetivo de interferir o deshabilitar una cuenta de usuario, bien sea local o remotamente.

- En caso de recibir una tarjeta de proximidad para el ingreso a locaciones o ubicaciones específicas de la compañía, esta debe ser de uso intransferible del usuario.

Actividades en Correo electrónico y sistemas de Comunicación

Responsables: Área IT, Usuarios.

Las siguientes actividades están prohibidas por la compañía:

- Enviar mensajes de correo no solicitados, incluyendo junk mail (material publicitario enviado por correo) o cualquier otro tipo de anuncio comercial a personas que no lo han solicitado (correo spam).

- Realizar cualquier tipo de intimidación o acoso a través del correo electrónico, teléfono fijo o celular, o mensajes texto o SMS, sin importar el idioma, la periodicidad o tamaño y contenido del correo.
- Redactar o enviar correos electrónicos suplantando o a nombre de otra persona.

- Envío de mensajes de correo electrónico con una dirección de correo diferente al verdadero remitente con el fin de realizar algún tipo de acoso, difamación u obtener información.

- Redactar o reenviar cadenas o cualquier otro esquema piramidal de mensajería.

- Redactar mensajes de correo electrónico iguales o parecidos que no tenga tengan relación con las actividades de la compañía grupos de noticias que no lo han solicitado.

Advertencia

Cualquier miembro de la compañía que sea encontrado realizando actividades que vayan en contra de estas políticas podrá ser investigado y ser causal de sanciones, sin perjuicio de las acciones disciplinarias y/o jurídicas que puedan ser adelantadas por la compañía.

Certifico que he leído y entendido la presente cláusula de sistemas de información y firmo en constancia de aceptación a los (____) días del mes _____ del año 2023.

xxxxxxxxxx	**xxxxxxxxx**
Gerente General (R. Legal)	Gerente Administrativo y Financiero
xxxxxxxxx	xxxxxxxxx
Director Gestion Humana	Director IT

xxxxxxxxx
Firma del Empleado
C.C.

La presentación de esta renovación del documento de política de seguridad esta aun en estudio para su aprobación.

8.2.1. IMPULSO TECNOLOGICO - DESARROLLO DE OBJETIVO 2

Siguiendo las directrices mencionadas en la propuesta de Política de Seguridad, se propone realizar una o dos veces por mes capacitaciones tipo Web Conference, interactivas multimedia o presenciales sobre las últimas novedades en cuanto a las nuevas amenazas cibernéticas y mecanismos de plagio a través de ingeniería social, recomendaciones para su prevención y tips informáticos, además, también capacitaciones para reforzar conocimientos informáticos en los usuarios de la red corporativa, basados en las aplicaciones de uso diario en la compañía. Dicha iniciativa llevará por nombre "**DIA TECNOLOGICO**" y será desarrollado por el asistente y el practicante IT.

Inicialmente se propone desarrollar videos a través de aplicaciones ya existentes en la compañía como Microsoft Teams, la cual permite establecer una videoconferencia y su posterior grabación, o bien, capacitaciones presenciales según lo permita el horario laboral y aforo; cuando se requiera editar un video, se utilizarán herramientas de edición gratuitas, sin embargo, se recomienda adquirir al menos dos licencias del software de edición de video FILMORA.

Durante el mes se planeará el tema que será presentado, este será socializado y afinado en reunión con el Director IT para su posterior aprobación. Una vez sea aprobado, se coordina un horario previo a la capacitación, según lo permita la carga laboral, para luego desarrollar y editar el video que será compartido a todos los colaboradores de la compañía, o bien, para preparar la presentación que será impartida en formato Web Conference o presencialmente.

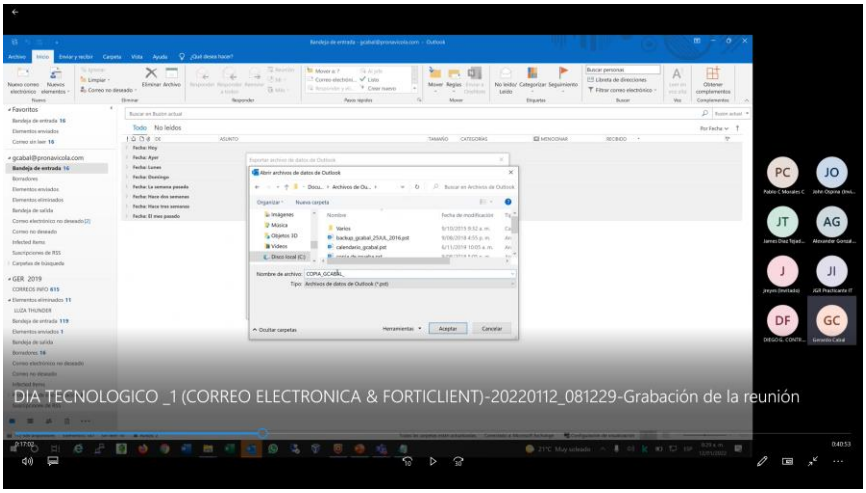
Luego de tres a seis meses de su realización, se evaluará la asertividad y satisfacción de los usuarios con las capacitaciones vía formulario de preguntas, de esta forma se podrá determinar su efectividad y sugerencias de mejora.

Esta propuesta ya ha dado inicio con la realización de capacitaciones y videos de carácter explicativo, así como manuales digitales para el uso de algunas de las herramientas tecnológicas más utilizadas en la compañía, como son el correo electrónico y las conexiones vía VPN (Video Conferencias explicando su uso, configuración en diferentes dispositivos y su administración), además de la identificación de equipos de Networking (Switches, cableado de red, Router´s, Lectores Biométricos, etc.) en los puestos de trabajo (Usuarios con acceso a las computadoras de las Granjas de Producción principalmente) con el objetivo de que los usuarios se conviertan en el primer "filtro" o "nivel" de soporte, en especial aquellos que se encuentran en centros de trabajo remotos, lo cual permite un conocimiento básico que puede en la mayoría de los casos servir como solución inicial o definitiva de un evento o incluso un incidente.

Dentro de la planificación del área IT para el año 2022, se plantea hacer especial énfasis en capacitaciones de concientización de ciberataques, phishing e ingeniería social, con capacitaciones de tipo Web Conference y juegos didácticos en línea.

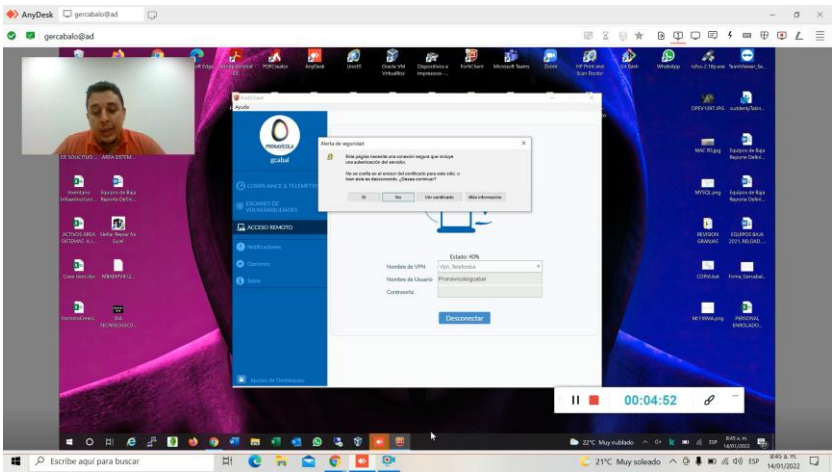
8.2.2. *Evidencias del Inicio del Proyecto “DIA TECNOLOGICO”.*

Figura 3. Web Conference Administración de Correo



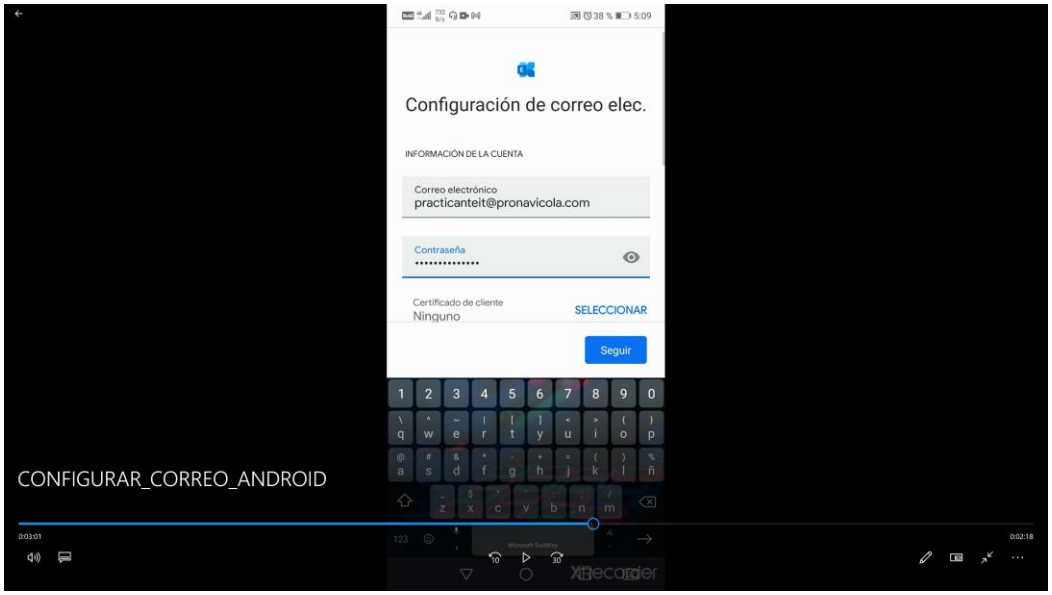
Fuente: Diseño Propio.

Figura 4. Uso Adecuado VPN´s



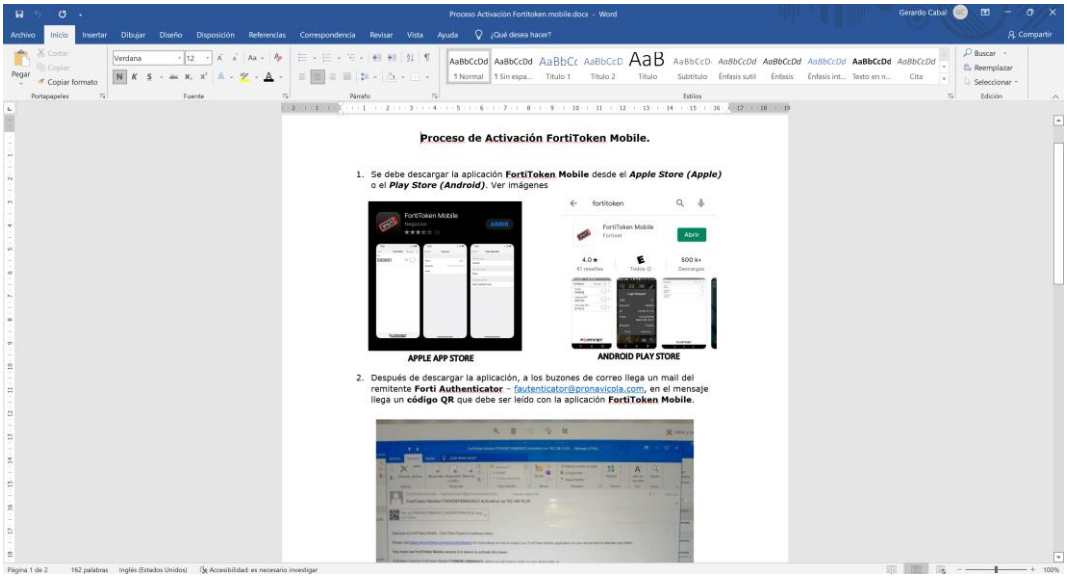
Fuente: Diseño Propio.

Figura 5. Config. Correo en Dispositivos



Fuente: Diseño Propio.

Figura 6. Config. Autenticación Doble Paso



Fuente: Diseño Propio.

8.3.1. APPLIANCE FORTINET DESARROLLO DE OBJETVO 3

8.3.2. *Afinamiento y Reconfiguración del Appliance Fortinet*

¿Qué es Fortinet y de qué manera funciona?

Fortinet es una compañía fundada en el año 2000 en los Estados Unidos con el objetivo de brindar soluciones de seguridad informática y en redes, esto de forma integral con diferentes dispositivos y funciones unificados en una sola plataforma global de ciberseguridad, convirtiéndose en una de las organizaciones más grandes y prestigiosas del mundo en este campo.[55]

Actualmente Pronavicola cuenta con un Appliance de seguridad perimetral con dos Firewall FortiGate 200E ubicados en el Data Center de la sede Principal, siendo uno el respaldo del otro y en la sede de Producción llamada Planta de Incubación un Fortigate 40F.

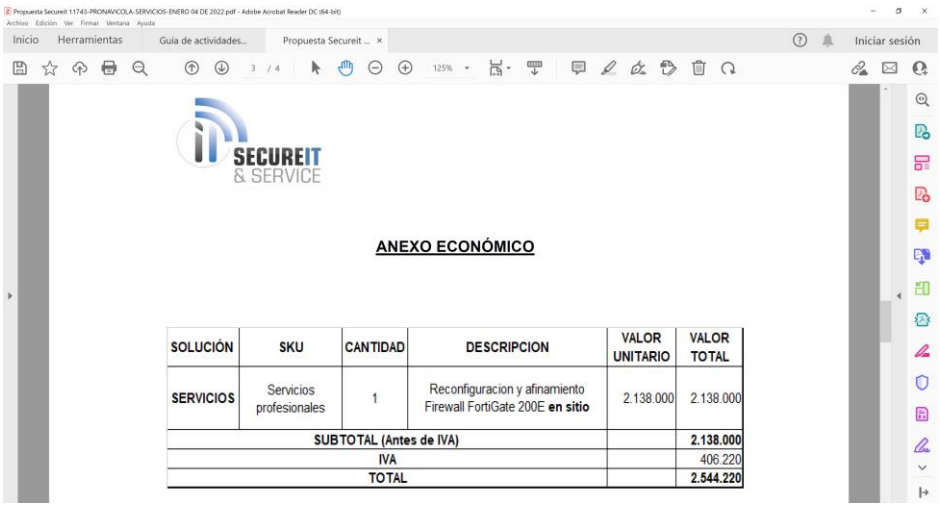
Por otro lado, se propone instalar y configurar un FortiGate 100D (Activo en posesión de la compañía) en la sede llamada Planta de Alimento Balanceado (PAB) para que de esta forma se tenga una protección integral en las tres sedes principales de la empresa.

Se realiza cotización para dichos servicios con la compañía experta SecureIT & Service, con los cuales se planteó el afinamiento de los FortiGate de la sede principal para ser realizados en sitio y de las demás sedes de manera remota, esto dimensionaría un costo total de $3.139.220 IVA incluido, sin embargo, después de

[55] LEMUS, José. Que es Fortinet y como funciona. Publicado el 19 de febrero de 2020. Obtenido de: https://vertical-iberica.com/que-es-fortinet-y-como-funciona/

un análisis de la seguridad actual y otros proyectos tecnológicos en curso, se decidió inicialmente optar por el afinamiento de los FortiGate 200E, debido a su criticidad para la compañía, por lo tanto, el costo de esta primera etapa del proyecto seria de $2.544.220 IVA incluido. A continuación, evidencia de la cotización:

Figura 7. Cotización Afinamiento Fortinet



SECUREIT & SERVICE

ANEXO ECONÓMICO

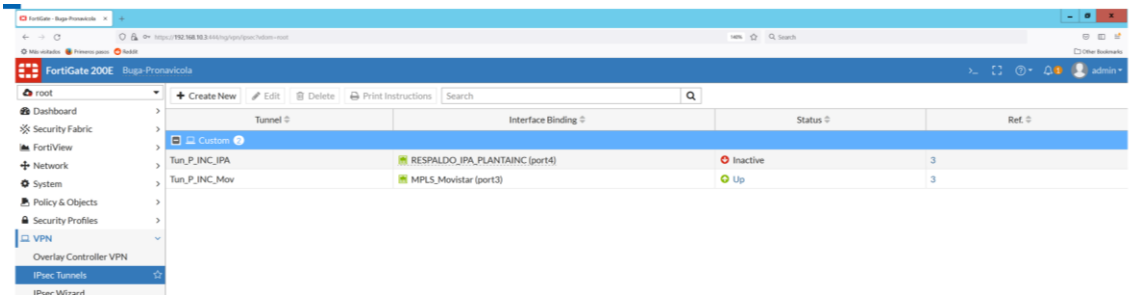
SOLUCIÓN	SKU	CANTIDAD	DESCRIPCION	VALOR UNITARIO	VALOR TOTAL
SERVICIOS	Servicios profesionales	1	Reconfiguracion y afinamiento Firewall FortiGate 200E **en sitio**	2.138.000	2.138.000
SUBTOTAL (Antes de IVA)					2.138.000
IVA					406.220
TOTAL					2.544.220

Fuente: Documento Cotización SecureIT & Service.

Gracias al impacto e importancia de la propuesta, la alta gerencia da visto bueno para dar inicio a esta primera etapa del proyecto, la cual tuvo lugar entre el jueves 20 y el viernes 21 de enero del año 2022, recibiendo la visita de un ingeniero especialista en Fortinet, para lo cual se comenzó con una evaluación del estado actual del firewall, el cual mostró políticas y configuraciones innecesarias, desactualización del dispositivo en directo y del dispositivo de respaldo, ausencia del registro oficial de uno de los dispositivos en la plataforma de Fortinet, lo cual es fundamental para recibir el soporte adecuado y la ausencia de ajustes necesarios para la estabilidad y armonía con el FortiGate 40F de la sede de producción, los cuales permitirían una verdadera centralización de la protección y visibilidad entre los sitios.

A continuación, algunas evidencias de políticas y configuraciones vulnerables:

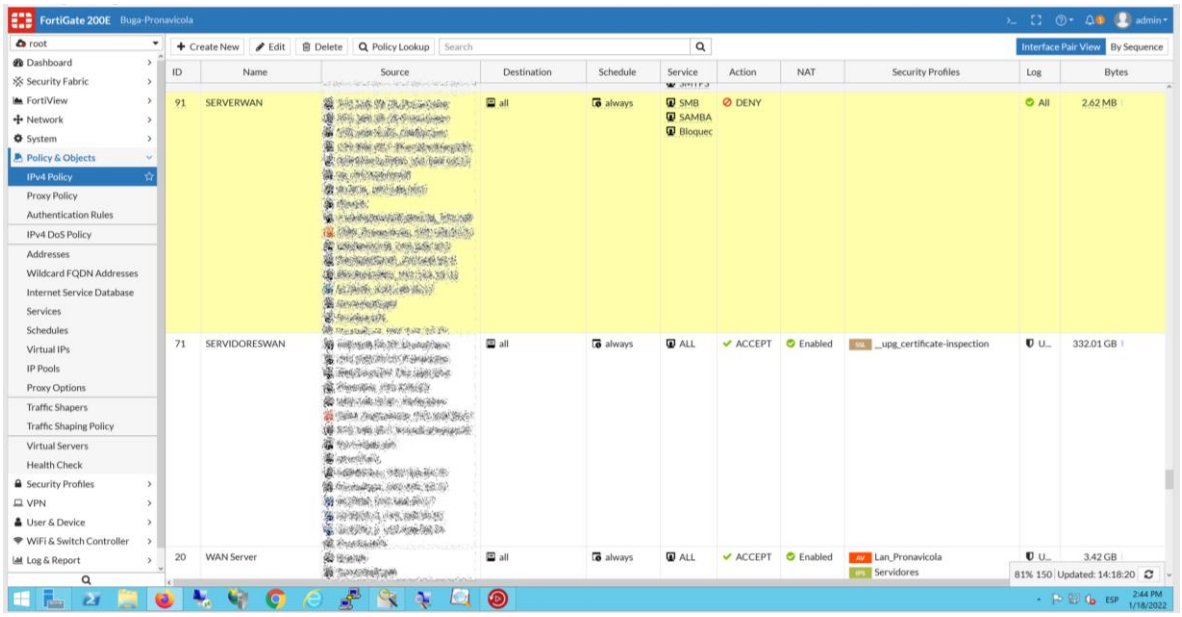
Figura 8. VPNs



Fuente: Diseño Propio.

En esta figura se muestra una configuración llamada “Túneles IP” en ella se configura una red VPN con el servicio principal de conexión (Telefónica en este caso) y otra con el enlace de servicio alterno, (Respaldo IPA en este caso) la cual muestra este último como “Inactivo”, lo cual no significa que en caso de un fallo con el proveedor principal entre las dos sedes (Canal de datos dedicado de fibra óptica) se perdería comunicación totalmente con la sede de producción debido a la configuración actual no alcanza correctamente el enlace alterno.

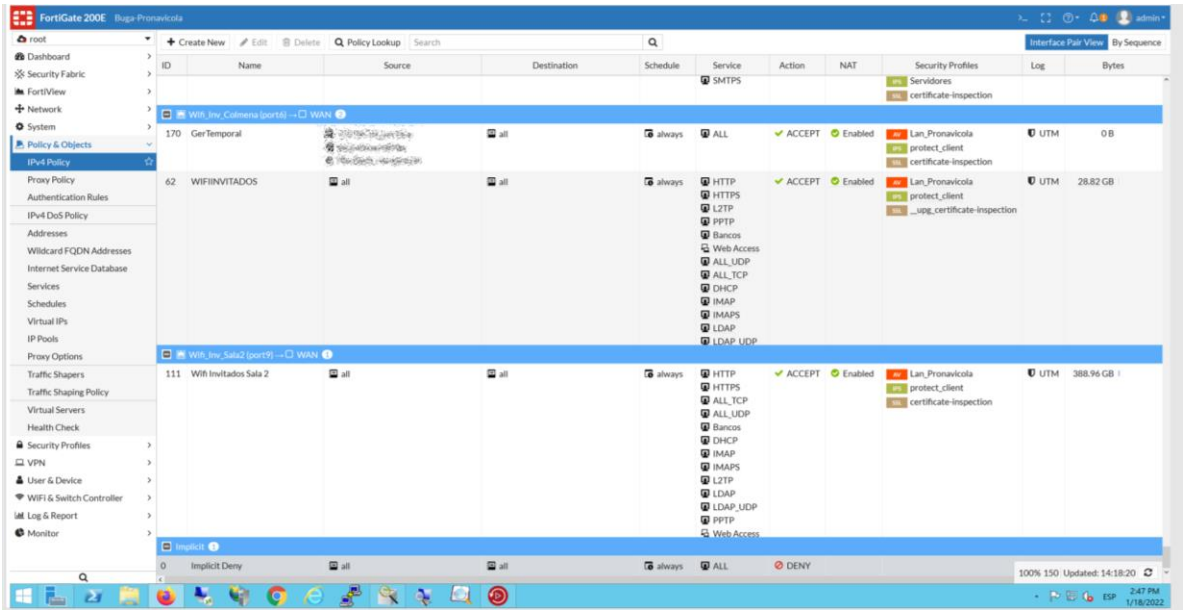
Figura 9. Políticas Riesgosas Previo a la Revisión



Fuente: Diseño Propio.

En esta figura se visualiza el apartado “Políticas IPv4” en donde están creadas la mayoría de políticas, menú en el cual se recopilaron más de 100 políticas, la mayoría sin uso específicos, redundantes o riesgosas para la seguridad de la red corporativa, como la que se presenta en la figura 10, donde se tiene una política que permite navegación sin ningún tipo de restricción en todos los servidores, practica poco recomendada por el riesgo de que alguno de los servidores sea secuestrado.

Figura 10. Redes Wifi Previo a la Revisión



Fuente: Diseño Propio.

En la figura 11 se visualizan las políticas establecidas para las redes Wifi de la sede principal, las cuales a pesar de ser FortiAP´s perfectamente visibles y multitareas entre sí, se encuentran en grupos de políticas separados y con permisos diferentes.

Esto se entiende como un desperdicio del recurso, ya que la compañía cuenta con cinco dispositivos que pueden trasmitir dos tipos de redes cada uno y desde FortiGate configurarse para que todos estén anclados y bajo las mismas políticas, de esta forma un usuario puede conectar a la red inalámbrica que desee desde cualquier punto de las instalaciones, bien sea a una Wifi local (con permisos destinados a los usuarios del dominio Pronavicola) o a una red Wifi alterna (con permisos solo de navegación para usuarios externos o invitados).

Como medida de seguridad se procede a realizar una copia de la configuración existente. Una vez realizada, se dio inicio a configurar casi que, desde el inicio en

el firewall alterno, de este modo no se alterarían las operaciones de la compañía durante la labor. Se configurar nuevas políticas y perfiles de navegación discriminados en grupos según su categoría y funciones, grupos que fueron creados igualmente desde el directorio activo del servidor de dominio, de esta forma se tiene una coherencia en los usuarios anexos a dichos grupos y se evita la confusión o duplicidad de configuraciones.

Por otro lado, se realiza la configuración llamada **SD-WAN**, la cual permite un balance de cargas del tráfico y los canales de datos que utiliza la compañía, de esta forma el firewall garantiza siempre el camino más “despejado” para dirigir dicho tráfico y navegación de forma más fluida y segura, además, permite garantizar que tanto la sede principal como la de producción se mantenga en el más alto rendimiento y sin interrupciones del servicio, ya que los canales alternos se configuran de modo que inmediatamente el canal con prioridad deje de responder estos entren a operar, de forma transparente para los usuarios.

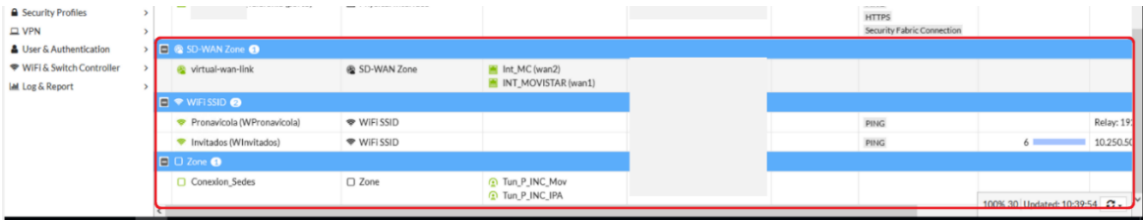
También se eliminan todas aquellas políticas creadas durante los años de uso del firewall y que no representan ninguna mejora o cambio significativo, organizándolas de forma que sean fácilmente reconocibles y editables, concentrándose en garantizar seguridad y coherencia para una fácil administración.

Por último, se acuerda con el área IT una ventana de maniobras para mover todo el cableado conectado en el firewall activo al firewall donde se realiza la nueva configuración (maniobra que desconecta a toda la compañía por unos minutos) y se realiza conexión en un puerto especifico (*puerto **ha***) de ambos firewall para que su configuración se replique y a su vez actualice cualquier cambio que se haga de forma que se guarde en ambos, de este modo, en caso de que el dispositivo que se encuentre activo sufra alguna falla, el equipo de IT solo debe conectar manualmente en el otro y la operación de la compañía seguirá sin problemas. También se verifica el estado de la configuración del FortiGate 40F (Firewall de la sede de Producción

en Planta de Incubación), su visibilidad y armonía con el FortiGate 200E (Firewall de la sede Principal) determinando que se encuentra OK, además, se prepara configuración en el FortiGate 100D (Firewall destinado para la sede PAB) para que su montaje y puesta en funcionamiento en la etapa dos del proyecto no sufra traumatismos.

A continuación, algunas ilustraciones de los principales cambios en la reorganización de los objetos, VPNs y políticas del Firewall en mención:

Figura 11. Definición de Zonas y Redes

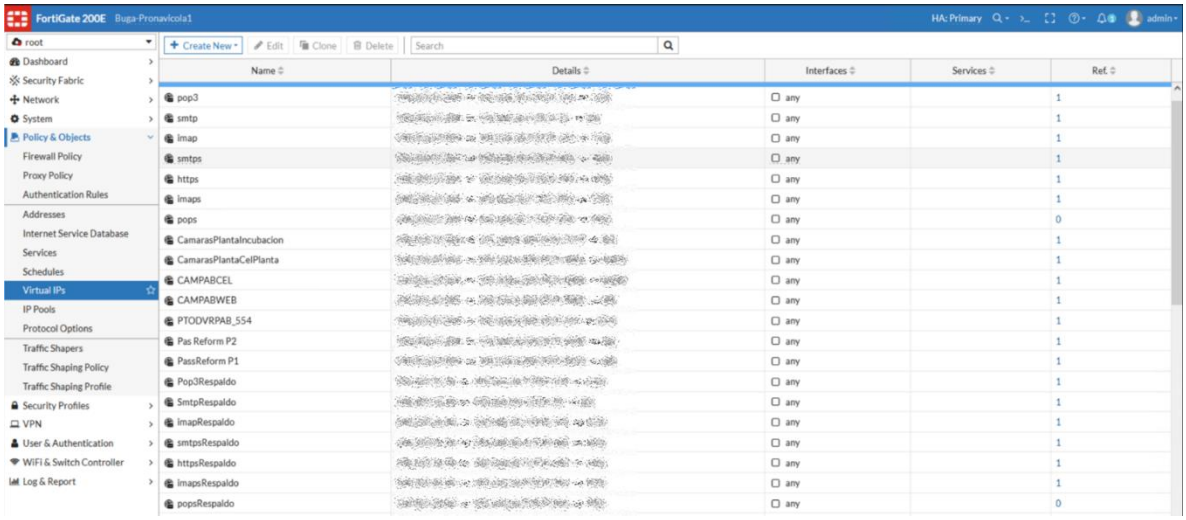


Fuente: Diseño Propio.

En esta figura se define la zona SD-WAN que concentra el canal principal de navegación (Telefónica) y el canal alterno (Media Commerce), con los cuales se hará el balanceo de las cargas de navegación y trafico web de la compañía.

Se definen dos perfiles de redes WIFI para toda la sede principal (WPronavicola y WInvitados), esto con el objetivo de que cada FortiAP que se instale en el perímetro de la compañía, se configure para brindar acceso a estos dos únicos perfiles, los cuales tienen unas restricciones y permisos definidos según la naturaleza y tipo de dispositivo que se conecte.

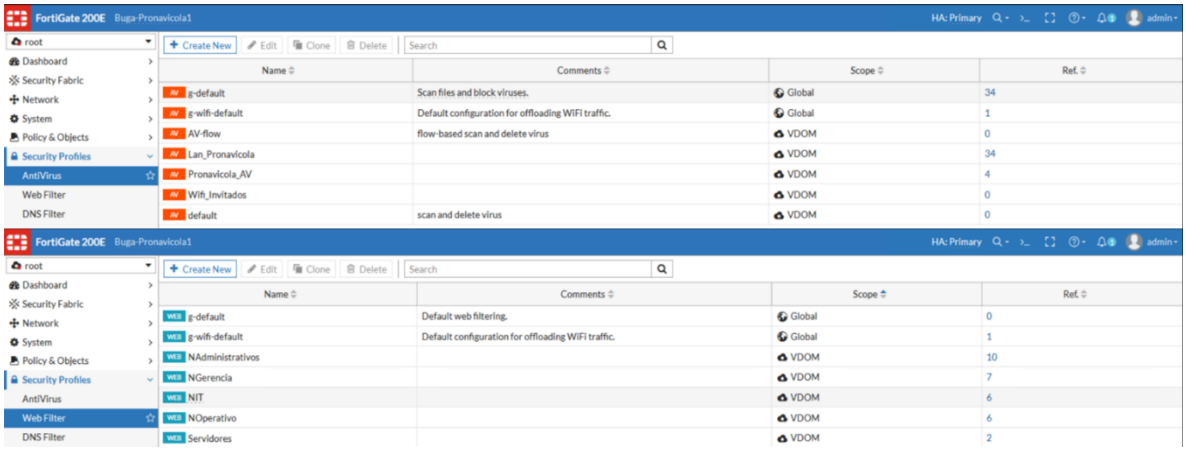
Figura 12. Virtual IPs



Fuente: Diseño Propio.

Se definen cada una de las herramientas y el enrutamiento virtual que requieren para será accedidas al interior y exterior de la compañía, limitando la conexión a un puerto especifico y por las direcciones IP Publicas que se determinaron para dichas conexiones, direcciones IP Publicas distintas a las configuradas para la navegación, de esta forma se optimiza dicho servicio y se controlan de mejor manera estos accesos.

Figura 13. Perfiles de Seguridad



Fuente: Diseño Propio.

Como se ve en la figura 14, se crean perfiles de filtrado de seguridad (Antivirus) y perfiles de navegación que se aplican en controles de aplicación y demás, estos perfiles son aplicados en base a las funciones de los usuarios en las diferentes sedes y la apertura de navegación que requiera su cargo. Su aplicación se da mediante Directorio Activo y se distribuye inicialmente así:

- ✓ **Perfil NAdministrativo**: Sede Principal (Oficinas Buga y Laboratorio), directores y supervisores de los diferentes centros de trabajo.
- ✓ **Perfil NGerencia**: Junta directiva y subgerentes de la compañía.
- ✓ **Perfil NIT**: equipo IT de la compañía.
- ✓ **Perfil NOperativo**: Personal de producción con baja necesidad de navegación (Planta de Incubacion, Granjas, PAB).
- ✓ **Perfil Servidores**: Diseñado con suma restricción para que los servidores solo tengan navegación en los portales autorizados de actualizaciones de SO y similares.

Figura 14. Políticas de Firewall

Fuente: Diseño Propio.

La cantidad de políticas es optimizada y pasa de más de 100 políticas (muchas inoficiosas o sin operar) a reducirse a 55 políticas bien definidas y personalizadas específicamente para cada uno de los servicios y necesidades de la compañía y sus redes.

Estas son las principales mejoras en la reorganización del Firewall principal, además, dichas mejores son directamente proporcionales en los Firewalls ubicados en los otros centros de trabajo ya que su función, filtrado y regulación de redes depende fundamentalmente del FortiGate optimizado.

Figura 15. Cotización Afinamiento Firewalls Restantes

ANEXO ECONÓMICO

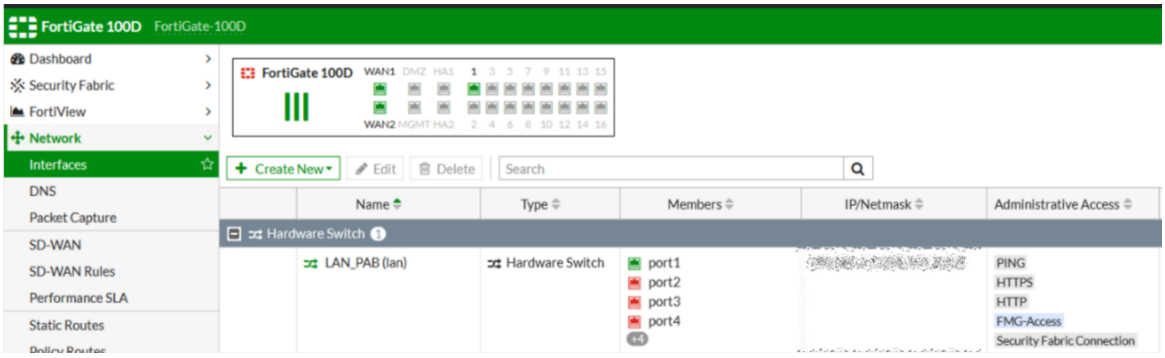
SOLUCIÓN	SKU	CANTIDAD	DESCRIPCION	VALOR UNITARIO	VALOR TOTAL
SERVICIOS	Servicios profesionales	6 Horas	Configuracion Firewall y ajuste de la conectividad **en forma remota**	30	180
SUBTOTAL (Antes de IVA)					180
IVA					34
TOTAL					214

Diseño: Propio.

Se efectúa la instalación de un Firewall FortiGate 100D para la comunicación y enrutamiento de la conexión a granjas con la sede de Planta de Alimento Balanceado (PAB) como nodo principal de conexión, además de garantizar una primera línea de protección que no existía en dicha sede.

Con base en lo explicado anteriormente se efectúan las siguientes configuraciones:

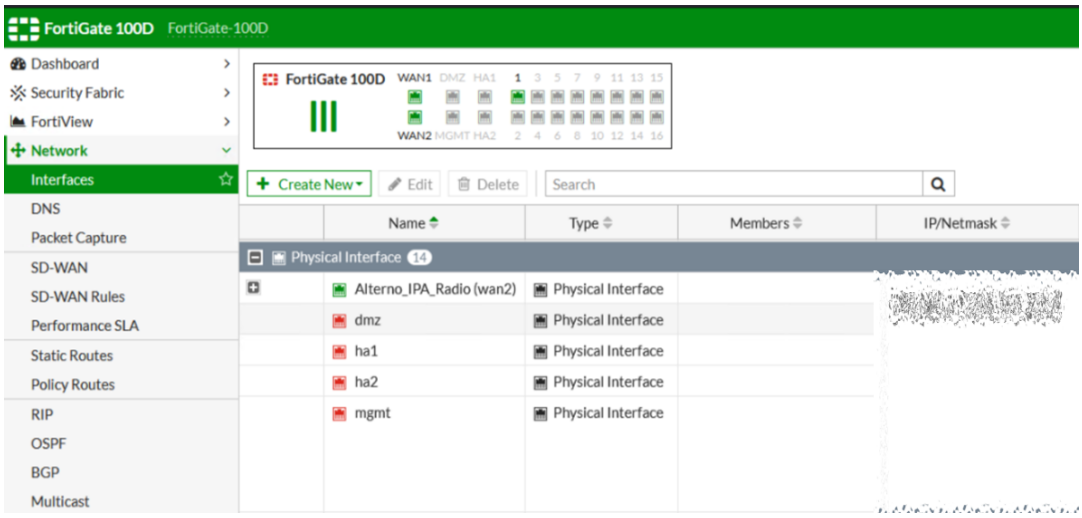
Figura 16. Config. Interfaces PAB 1



Diseño: Propio.

Se coordina con el proveedor del canal MPLS de la sede (Telefónica) cambiar direccionamiento IP de su Router para que sea el FortiGate quien pase a operar como la puerta de enlace del borde de la red.

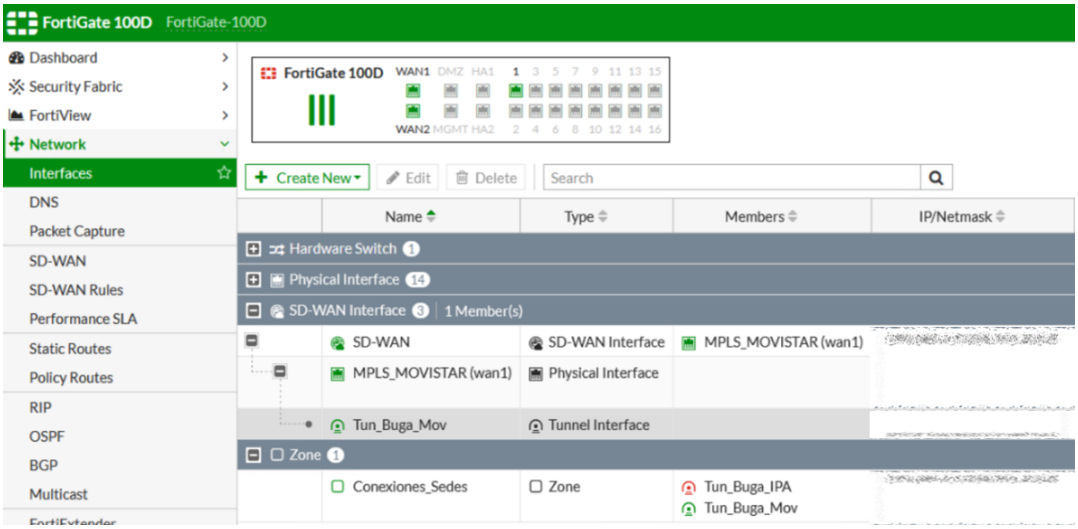
Figura 17. Config. Interfaces PAB 2



Diseño: Propio.

Debido a que la conexión con Granjas se realiza mediante un Radio-Enlace, se configura una interfaz con un direccionamiento IP acordado con el proveedor de dicha conexión de Radio-Enlaces, esta interfaz será la puerta de enlace que enrutará el tráfico de las Granjas con la red corporativa.

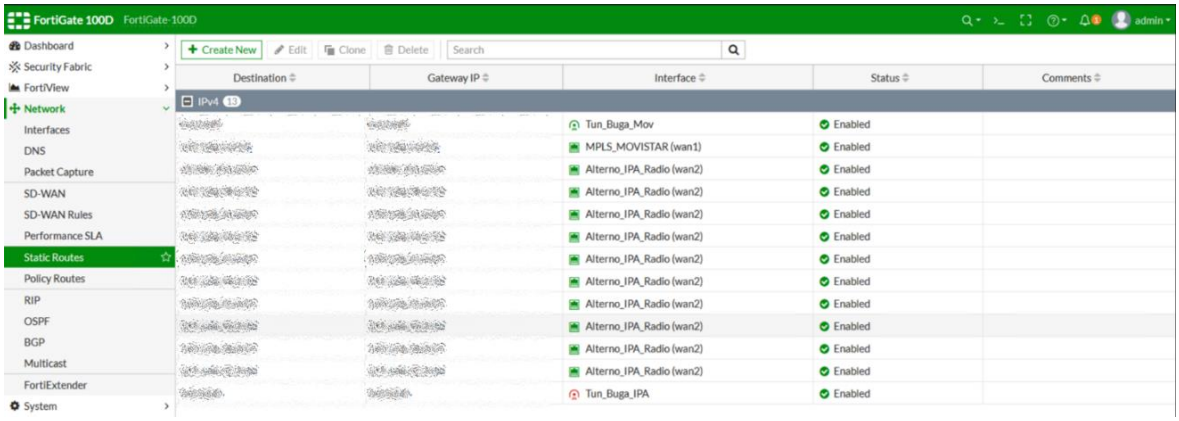
Figura 18. Config. Interfaces PAB 3



Diseño: Propio.

Finalmente se establece una SD-WAN que se enruta a través del MPLS que conecta con la sede principal (Oficinas Buga) y dos túneles Ipsec VPN, de esta forma se balancea la conexión entre el túnel predeterminado (MPLS Telefónica) y un túnel secundario del proveedor de conexión por Radio-Enlace a Granjas (IPA Telecom) como contingencia.

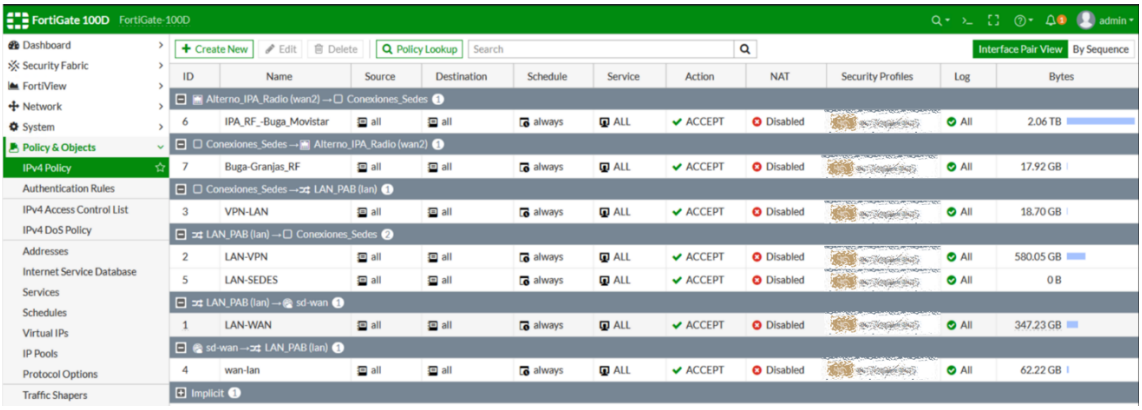
Figura 19. Config. Rutas Estáticas PAB



Diseño: Propio.

Se establecen las rutas estáticas que van a enrutar el tráfico de las diferentes granjas por medio del nodo principal ubicado en PAB y que pasar a través del FortiGate 100D, colocando en la columna “Destination” la puerta de enlace de cada granja y en “Gateway IP” la puerta de comunicación con el MPLS principal, la puerta de enlace del proveedor de Radio-Enlaces y las puertas de enlace de cada Granja.

Figura 20. Config. Políticas PAB



Diseño: Propio.

Finalmente se establecen políticas básicas y “abiertas” para que el enrutamiento y comunicación entre la red corporativa, la sede de PAB y las granjas puedan conectarse y tener un flujo de tráfico limpio y sin restricciones.

8.3.3. *Propuesta de Formato para Control de Cambios de Seguridad ante Incidentes.*

Aprovechando la apertura concedida por los marcos de referencia para combinar actividades de otros marcos o estándares de SI, se propone la elaboración de un formato en el cual se registren los diferentes hallazgos y actividades derivadas de un cambio o impacto de ciberseguridad, esto para atender un objetivo específico de este proyecto, el cual pretende alcanzar una administración total en este aspecto.

8.3.4. *Gestion de Cambios de un SGSI según la ISO/IEC 27001 de 2013*

Los SGSI según la norma ISO/IEC 27001 de 2013 plantean que se debe mantener un proceso de mejora continua siempre, soportados bajo el ciclo PHVA (Planificar, Hacer, Verificar y Actuar), proceso que debe realizarse con cada cambio que se sugiera o realice en software, hardware, procedimientos, etc.

La norma es clara en cuanto a que todo cambie que afecte directa o indirectamente la seguridad de la información debe estar debidamente controlado y registrado.

Aun cuando se resalta dicha mención, la norma no provee una forma específica de llevar a cabo dicho control, por lo tanto, se diseña el siguiente formato para la gestión de cambios en **PRONAVICOLA S.A.** (*Páginas 150 a la 153*).[56]

[56] SGSI. La gestión de los cambios en un SGSI basado en la ISO/IEC 27001 de 2013. Publicado el 29 de septiembre de 2015. Disponible en: https://www.pmg-ssi.com/2015/09/gestion-cambios-sgsi-iso-iec-27001-2013/

Tabla 28. Formato Control de Cambios.

LOGO DE PRONAVICOLA	**FORMATO CONTROL DE CAMBIOS**

1. Inicio de Solicitud *(Diligenciado por el solicitante del cambio)*			
Nombre:		**Cargo:**	
Dependencia:	*<Área o departamento>*	**Fecha:**	
Correo electrónico:		**Extensión:**	
Tipo de cambio:	*<Software, Hardware, otro>*	**Fecha del cambio:**	*<Fecha en la que se requiere el cambio>*
Descripción del cambio:	*<Describir el cambio solicitado>*		

Beneficios del cambio:	*<Mencionar la justificación del cambio, los beneficios del cambio o las consecuencias por su no realización>*

2. Análisis de Viabilidad de la Solicitud *(Diligenciado por Equipo Técnico de TI)*				
Nombre:		**Cargo:**		
Correo Electrónico:		**Fecha:**		
Prioridad del cambio:	*<Emergencia, Alto, Medio, Bajo>*	**Nivel de Clasificación del cambio:**	*<Alto, Medio, Bajo>*	
Recursos afectados	*<Mencionar los recursos tecnológicos, los servicios y los aplicativos afectados por el cambio>*			
Usuarios y/o Dptos. Afectados	*<Mencionar los usuarios o departamentos que se verán afectadas con la indisponibilidad del servicio>*			

Concepto de viabilidad	**¿Es Viable?**	**Observaciones**
	<Si o No>	*<Registrar observaciones frente al concepto de viabilidad entregado>*

3. Diseño del Plan y Riesgos				
3. 1 Plan de Trabajo *(Diligenciado por el responsable del cambio y Equipo Técnico de TI)*				
¿Se requiere ventana de mantenimiento?				
Tipo de Actividad	**Actividad**	**Responsable**	**Fecha Inicial / Fecha Final**	**Hora Inicial / Hora Final**

3.2. Análisis de Riesgos del Cambio *(Diligenciado por el responsable del cambio y Equipo Técnico de TI)*				
Riesgo	**Probabilidad**	**Impacto**	**Nivel de Riesgo**	**Actividad de Mitigación**

4. Resultados del Cambio *(Diligenciado por el responsable del cambio y Equipo Técnico de TI)*	
Fecha	
Resultados Obtenidos:	*<Indicar si el cambio fue exitoso o no y mencionar los resultados obtenidos. En caso de que el cambio no fuera exitoso, describir el inconveniente y los motivos para de su ocurrencia>* *<Describir los correctivos realizados en caso de inconveniente, teniendo en cuenta, entre otros: fecha y hora del reinicio de actividades, descripción de la solución y fecha y hora de finalización. Diligenciar solo en caso de inconvenientes que puedan ser corregidos>*

	<Describir el plan de contingencia del cambio en caso de inconvenientes, teniendo en cuenta, entre otros: actividades a realizar para la contingencia, responsables asignados, ventana de tiempo requerida>

Diseño de la tabla: Propio.

8.3.5. *Conceptos e Instrucciones del Formato*

Inicio de Solicitud

Tipo del Cambio:

Hardware: Cualquier instalación, modificación, retiro o reubicación de Rack de servidores o servidores como tal, dispositivos de red y de seguridad, computadoras, u otros dispositivos en los que se pueda almacenar o manipular datos.

Software: Cualquier instalación de aplicativos o SO, aplicación de parches, actualización o eliminación de productos de software, incluyendo SO y utilitarios.

Cambios en las aplicaciones lanzadas en producción, así como la integración de nuevos sistemas de información y la eliminación de software obsoletos.

Prioridad del Cambio:

Emergencia: Cambio que, al no ser aplicado de inmediato, estará exponiendo la compañía a riesgos de seguridad informática.

Alto: Cambio que, debe implementarse lo más pronto posible, de esta forma se podrá prevenir un riesgo informático mayor.

Medio: Cambio que, no supone un riesgo latente, pero al ser implementado traerá beneficios en producto o servicio.

Bajo: Cambio que, no está sujeto a un espacio tiempo definido.

Análisis de Viabilidad de la Solicitud

Nivel de Clasificación:

El área TI en cabeza de sus especialistas de seguridad definirá el nivel de clasificación en base a los siguientes criterios:

Bajo: Acciones rutinarias con las siguientes condiciones:

- Los recursos solicitados se encuentran dentro del proceso de Gestión de las Tecnologías de la Información.
- Baja complejidad, ya que no es solicitada una coordinación técnica.
- Bajo riesgo para la disponibilidad del sistema.
- Fácil aplicación, no requiere un plan de contingencia.
- No hay impacto para los acuerdos de niveles de servicio.

Medio: Supone las siguientes condiciones:

- Incluye recursos de más de un grupo de trabajo.
- Complejidad técnica significativa, es solicitada la coordinación técnica para uno o más grupos funcionales.
- Riesgo moderado para la disponibilidad del sistema, requiere de un plan de contingencia.
- La implementación demanda de cierta complejidad.
- Posibles impactos para los acuerdos de niveles de servicio.

Alto: Acciones de mayor nivel de complejidad, urgencia y riesgo bajo las siguientes condiciones:

- Incluye diversos grupos de trabajo.
- Alta complejidad técnica, exigente coordinación entre los diversos grupos funcionales.
- Es posible que se afecten los datos y la seguridad de la infraestructura tecnológica.
- Es necesario el soporte externo especializado.
- Nivel crítico de emergencia.

Diseño del Plan y Riesgos

Planta de Trabajo – Tipo de Actividad:

Contingencia: Actividades para reversar el cambio en caso de que falle.

Producción: Actividades requeridas para el cambio.

Pruebas: Actividades requeridas antes de un cambio para validar que funciona correctamente.

Análisis de Riesgos del Cambio – Riesgo:

Seguridad Digital: conjunto de amenazas y vulnerabilidades en el entorno digital.

Dichas amenazas pueden comprometer el logro de objetivos económicos y sociales, así como afectar la soberanía nacional, la integridad territorial, el orden constitucional y los intereses nacionales. Involucra aspectos relacionados con el ambiente físico, digital y las personas.

Gestion: Posibilidad de ocurrencia de un evento que tendrá un impacto sobre el cumplimiento de los objetivos. Se expresa en términos de probabilidad y consecuencias.

Corrupción: Posibilidad de que, por acción u omisión, se utilice el poder o influencias para desviar la gestión de lo público o netamente empresarial hacia un beneficio privado.

Análisis de Riesgos del Resultado del Cambio – Riesgo:

- Probabilidad: Se clasifica de 1 a 5.
- Impacto: Se clasifica de 1 a 5.
- Nivel de Riesgo: Bajo, Medio, Alto, Extremo.

Tabla 29. Matriz Nivel de Riesgo.

Matriz de Calificación Nivel de Riesgo					
Impacto	**Insignificante**	**Menor**	**Moderado**	**Mayor**	**Catastrófico**
Probabilidad	1	2	3	4	5
Raro 1	**Bajo**	**Bajo**	**Medio**	**Alto**	**Extremo**
Improbable 2	**Bajo**	**Bajo**	**Medio**	**Alto**	**Extremo**
Posible 3	**Bajo**	**Medio**	**Alto**	**Extremo**	**Extremo**
Probable 4	**Medio**	**Alto**	**Alto**	**Extremo**	**Extremo**

Casi Seguro 5	**Alto**	**Alto**	**Extremo**	**Extremo**	**Extremo**

Diseño de la tabla: Propio.

9. CONCLUSIONES

- Utilizando el marco de referencia NIST CSF, además del uso de metodologías como MAGERIT y GAP, se realiza un análisis exhaustivo de riesgos tecnológicos inherentes y derivados de la ausencia de un PDS, así como políticas de seguridad renovadas y sofisticadas, ejecutando seis pasos que reúnen a lo largo del proyecto el alcance fijado en materia de ciberseguridad, situación o perfil actual de la compañía en dicho ámbito, análisis de riesgos en base a metodologías e indicadores con medidas de riesgo y probabilidad de ocurrencia, perfil o estado al que se aspira llegar luego de las mejoras y finalmente el desarrollo de un plan de acción centrado en el Appliance de seguridad perimetral de la compañía, el rediseño del documento oficial de políticas de seguridad y proyectos de concientización y mejora de la ciberseguridad en general, recopilación verificable a partir del numeral 6 y 7, páginas 57 a la 110.

- Se da inicio al desarrollo de objetivos propuestos desde el anteproyecto, elaborando políticas orientadas al escalamiento en nivel de madurez tecnológica y de gobernanza TI.

  El documento de Políticas de Seguridad (*Plasmado como anexo a las hojas de vida de los colaboradores*) utilizado en la actualidad, se entrega junto al contrato del colaborador al momento de ingresar a la compañía y del cual previamente se sabe tendrá acceso a una computadora o dispositivo inteligente, una vez le sea entregado dicho equipo, el área IT hace referencia a ciertas recomendaciones de uso, sin embargo, no se está realizando una socialización de lo que está escrito en dicho documento ni de todos los procedimientos tecnológicos que deberían ser conocidos por los colaboradores en general, objetivo específico del proyecto que se diseña y

amplia como propuesta que la compañía puede mejorar y aplicar en el momento que crea conveniente, además, brinda la oportunidad de convertirlo en tema de capacitaciones y aprendizaje colectivo. Dicha propuesta se encuentra a partir del numeral 8, páginas 110 a la 130.

- Durante años, el área IT de la compañía ha centrado sus esfuerzos en brindar el mejor soporte y seguridad informática posible, esto debido a que se trata de un departamento de solo dos o máximo tres Informáticos para la atención de más de 130 usuarios, razón por la cual las capacitaciones y concientizaciones informáticas han sido esporádicas o limitadas a una sola sede, sin embargo, este proyecto y la llegada de un nuevo director de área han impulsado una reestructuración de funciones y visión del departamento, proponiendo así el proyecto "**DIA TECNOLÓGICO**" el cual se desarrollará al menos una vez al mes (*o en la periodicidad que el área IT lo disponga*) utilizando diferentes mecanismos interactivos y multimedia (*INTRANET y capacitaciones virtuales que se desarrollan en la actualidad*) los cuales ya se encuentran en marcha con gran acogida entre los usuarios, objetivo expuesto en el numeral 8.2.1., páginas 131 a la 134.

- Durante el análisis de riesgos y construcción del PDS, se evidencia que la compañía cuenta con herramientas sofisticadas (*Appliance Fortinet, Consola Antivirus Kaspersky*) y algunas políticas establecidas desde su servidor de dominio y procedimientos documentados, como son el formato y proceso de creación de un nuevo usuario, creación y restauración de copias de datos, entre otros. Estos avances en términos de seguridad resultan valiosos para el entendimiento de las operaciones del área IT y sus actividades diarias, sin embargo, también revelan que las herramientas mencionadas inicialmente, aunque están instaladas y configuradas (*en un nivel básico y casi por defecto*), carecían de una administración y entendimiento claro por parte de los actuales Ingenieros del departamento, poniendo a la compañía en un

riesgo alto aun cuando aparentemente todo opere “sin novedad”, a pesar de ello, es importante resaltar que la experticia y vigilancia del funcionamiento de la red corporativa por parte de los Ingenieros del área facilita la adopción rápida del PDS y los proyectos propuestos.

La seguridad perimetral contenida en el Appliance de Fortinet resulta tan potente y eficaz que aun siendo explotado y utilizado en un mínimo porcentaje es sinónimo de seguridad, tal como es el caso de la compañía, la cual realizó ciertas configuraciones en cabeza del anterior Director del área y el soporte del momento, pero que luego de varios años de cambios estructurales y de la red corporativa en general, no se encuentra en la armonía necesaria para brindar la mejor mitigación de riesgos e interconexión de todas las sedes y sus recursos, sin embargo, cabe resaltar que aun con su casi incomprensible configuración, la SI de la compañía estaría totalmente comprometida de no existir. Con el afinamiento que se ha llevado a cabo en primera fase al inicio del año 2022 se logra clarificar y recomponer todas las políticas existentes y por tanto mejorar exponencialmente la mitigación de ataques cibernéticos en todas las sedes.

Las mejoras principales y futuras que se llevaran a cabo al inicio del año 2023 se encuentran plasmadas en este proyecto a partir del numeral 8.3.1., páginas 135 a la 149.

10. RECOMENDACIONES

- Si bien el análisis de riesgos y perfiles del estado de ciberseguridad basados en MAGERIT, GAP y el marco de referencia NIST fueron útiles en la manera de abordar y proponer soluciones a la problemática encontrada en Pronavicola S.A., es importante resaltar que podría llegarse a resultados igualmente efectivos implementando otras metodologías o técnicas en estudios futuros de este mismo caso o similares, ya que a medida que la tecnología avanza se hace necesario abandonar ideas o premisas antiguas y adoptar nuevas perspectivas y métodos que surjan en pro del objetivo general planteado en este proyecto, que no es otro que mitigar al máximo ataques cibernéticos que comprometan la integridad de la información, por lo tanto, un paso adelante en la meta de brindar las mejores prácticas y condiciones de SI estaría en la certificación e implementación de Sistema de Gestion de Seguridad de la Información (SGSI) basado en el PDS creado a este proyecto, el cual podría integrarse y complementarse perfectamente.

- Este es un proyecto que compete a cualquier compañía tecnológica y de servicios virtuales ya que la SI es la piedra angular del éxito de cualquier desarrollo u organización que pretenda recopilar, cruzar o publicar información y soluciones tecnológicas, por tanto, de la manera más cordial y amigable se hace extensiva la invitación a la Universidad, facultad y demás actores relaciones a que utilicen este proyecto y sus objetivos como base o apoyo académico y profesional según lo consideren pertinente, pues la ampliación de conocimientos y la evaluación de nuevas perspectivas e infraestructuras de red permitirán la creación de nuevos y mejores modelos de SI en las compañías, así como desafíos académicos de los que surjan nuevas propuestas en beneficio de la ciberseguridad.

- Entendiendo la vital importancia de mantener segura y resguardada no solo la información sino también la estructura de servidores, se propone contratar servicios de respaldo con Data Center externo o migración paulatina a plataformas en la nube como Microsoft Azure o AWS, dicho proyecto permitirá liberar de la administración de redes y recursos al equipo IT, al igual que fortalecer la SI de los mismos en apoyo con el soporte especializado con el que cuente el proveedor, esto significará a una nueva configuración hibrida o completamente virtual (si así lo considera la compañía) de los componentes físicos y de interconexión de la red corporativa, dando paso a nuevos proyectos enfocados en mesas de servicio y propuestas tecnológicas de colaboración y fuerza de negocios.

11. BIBLIOGRAFÍA

ARAUJO, Adriel. ISO 27001: Como hacer tu política del SGSI. Publicado el 9 de septiembre de 2021. Obtenido de: https://blog.hackmetrix.com/politica-del-sgsi/?utm_source=GAds&utm_campaign=Blog&utm_medium=Politica_SGSI&utm_term=sistema%20de%20gesti%C3%B3n%20de%20seguridad%20de%20la%20informaci%C3%B3n&gad=1&gclid=Cj0KCQjwqs6lBhCxARIsAG8YcDjS3SPasQgfSNuv9iCE3FyfQHU-4Hn0TrsAy58JO0U7JvJhF1RrX4QaAjxqEALw_wcB

Gobierno Electrónico. Guía para la gestión de riesgos de seguridad de la información. Consultado en noviembre de 2022. Obtenido de: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/GU%C3%8DA-PARA-LA-GESTI%C3%93N-DE-RIESGOS-DE-SEGURIDAD-DE-LA-INFORMACI%C3%93N-ABRIL-2020.pdf

GOMEZ, MORALES, Gianncarlo. ¿Qué es el Cibersecurity Framework de NIST de los Estados Unidos?. Publicado el 30 de abril de 2019. Disponible en: https://www.esan.edu.pe/conexion/actualidad/2019/04/30/que-es-el-cybersecurity-framework-de-nist-de-los-estados-unidos/

Instituto Nacional de Estándares y Tecnología. Marco para la mejora de la seguridad cibernética en infraestructuras críticas. Publicado el 16 de abril de 2018. Disponible en: https://www.nist.gov/system/files/documents/2018/12/10/frameworkesmellrev_20181102mn_clean.pdf

Mintic. guía de gestión de riesgos. Actualizado el 1 de abril de 2016. Obtenido de: https://www.mintic.gov.co/gestionti/615/articles-5482_G7_Gestion_Riesgos.pdf

Mintic. Elaboración de la política general de seguridad y privacidad de la información. Actualizado el 11 de mayo de 2016. Obtenido de: https://www.mintic.gov.co/gestionti/615/articles-5482_G2_Politica_General.pdf

MONTERO, VALENCIA, Jessica Alexandra. Desarrollo del Plan Director de Seguridad para la Asociación APSA. Publicado en septiembre de 2019. Obtenido de: https://core.ac.uk/download/pdf/237118547.pdf

Normas Icontec. Normas ICONTEC: guía [2023]. Consultado en junio de 2023. Obtenido de: https://normasicontec.co/

Nqa. ISO 27001:2013. Guía de implantación para la seguridad de la información. Consultado en noviembre de 2022. Obtenido de: https://www.nqa.com/medialibraries/NQA/NQA-Media-Library/PDFs/Spanish%20QRFs%20and%20PDFs/NQA-ISO-27001-Guia-de-implantacion.pdf

Pirani. guía para hacer una política de seguridad de la información. Consultado en junio de 2021. Obtenido de: https://www.piranirisk.com/es/academia/especiales/guia-politica-de-seguridad-de-la-informacion

Secretaria Senado. Ley 1273 de 2009. Consultado el 1 de octubre de 2021. Obtenido el: http://www.secretariasenado.gov.co/senado/basedoc/ley_1273_2009.html

Universia. Escribe una conclusión memorable en tu tesis siguiendo estos consejos. Publicado el 17 de abril de 2017. Obtenido de: https://www.universia.net/uy/actualidad/orientacion-academica/escribe-conclusion-memorable-tu-tesis-siguiendo-estos-consejos-1159003.html

UVR. ¿Cómo redactar correctamente las conclusiones y recomendaciones? Actualizado el 17 de abril de 2021. Obtenido de: https://www.uvrcorrectoresdetextos.com/post/2019/03/04/-c2-bfc-c3-b3mo-redactar-correctamente-las-conclusiones-y-recomendaciones

12. ANEXOS

Anexo A. ***Lista de Consulta de Chequeo***.

LISTA DE CONSULTAS DE CHEQUEO				
A continuación, se evalúan las siguientes actividades:				
No. ITEM	**Evidencia**	**Conforme**		**Hallazgos**
		SI	**NO**	
1	¿Se evidencian mecanismos y controles de gobernanza TI?	X		Existen, pero deben ser actualizados.
2	¿Están claramente definidos todos los recursos tecnológicos y su evaluación de riesgos?	X		Existe archivo, pero debe ser actualizado y ampliado.
3	¿Están claramente definidos los controles y medidas para mitigar y prevenir riesgos informáticos?		X	Existen algunos y otros deben ser actualizados.
4	¿Se ha diseñado un formato para la solicitud y gestión de cambios dentro del PDS?		X	No existe, esta en proceso de desarrollo para el PDS.
5	¿Están claramente definidos los roles y responsables de cada actor en el proceso de construcción del PDS?	X		En proceso de construcción.
6	¿Están claramente definidas las políticas de ciberseguridad, seguridad informática y uso adecuado de los recursos e infraestructura tecnológica?		X	Existen, pero deben ser actualizadas.

7	¿Existen planes de concientización y capacitación en ciberseguridad?		X	No existe, está en proceso de desarrollo para el PDS.
8	¿El personal del área IT siente que está completamente capacitada en el uso de la solución de seguridad perimetral Fortinet?		X	No cuenta con todas las competencias, por lo tanto, es una de las propuestas a cubrir en el PDS.

Diseño: Propio.

Anexo B. ***Resumen Especializado Analítico (RAE)***.

Fecha de Realización: 01 de agosto de 2023.
Tema: Seguridad Informática.
Título: Elaboración de un Plan Director de Seguridad para la compañía Pronavicola S.A..
Autor: Gerardo Cabal Ortiz.
Publicación: Ciudad: Guadalajara de Buga. Fecha: diciembre de 2022. Páginas: 171.
Unidad Patrocinante: Pronavicola S.A..
Palabras Claves: Seguridad Informática, Análisis de Riesgos, Políticas de Seguridad.
Descripción del Problema de Investigación: Pronavicola S.A. requiere un análisis y auditoria del estado de sus políticas, procedimientos y Core de ciberseguridad, ya que dichas herramientas y el manejo de las mismas no llevan una correcta administración en términos de gestión y trazabilidad.

Existen ciertas políticas y procedimientos de las cuales no se tiene claridad y control adecuado ni medible, además de un sistema de seguridad perimetral (Fortigate, FortiMail, FortiAuthenticator y FortiVoice) los cuales garantizan un buen nivel de ciberseguridad y protección de la red corporativa, pero requieren de una reorganización en su configuración, procedimiento que el equipo TI desconoce pues no cuenta con personal experto en la solución.
Objetivo General: Elaborar un Plan Director de Seguridad (PDS) en base a los pilares de la seguridad informática y que garantice la adecuada administración, gestión y mitigación de riesgos informáticos de la compañía.
Objetivos Específicos: ➢ Examinar las políticas y prácticas actuales en busca de vulnerabilidades latentes utilizando como base el marco de metodología de NIST CSF. ➢ Establecer políticas de seguridad claras y renovadas que se adecuen a la infraestructura de red y los mecanismos de seguridad existentes, así como la reconfiguración de la solución Fortinet actual. ➢ Desarrollar proyectos de ciberseguridad y mecanismos de capacitación entre los colaboradores de la compañía para hacerles partícipes de la iniciativa.
Descripción/Resumen: Proyecto aplicado que pretende garantizar la aplicación de metodologías internacionales de seguridad informática, y por ende, la protección de todos sus activos y recursos tecnológicos al igual que la mitigación de vulnerabilidades cibernéticas al aprovechar al máximo las herramientas de seguridad existentes, así como rediseñar sus políticas de seguridad de forma que arropen a toda la compañía y creen una cultura de ciberseguridad replicable en todos sus colaboradores.
Fuentes: Se obtuvo información de diversos proyectos orientados a objetivos relacionados con la elaboración de un PDS, al igual que portales y artículos especializados en la aplicación de metodologías para la gestión y gobernanza de TI, así como el descubrimientos, análisis y creación de directrices para la

mitigación de riesgos informáticos. Algunas de ellas:

- GOMEZ, MORALES, Gianncarlo. ¿Qué es el Cibersecurity Framework de NIST de los Estados Unidos?.
- Mintic. Guía de gestión de riesgos.
- Nqa. ISO 27001:2013. Guía de implantación para la seguridad de la información.

Contenido: Dentro del campo de estudio de la seguridad informática es necesario abordar el objeto de estudio partiendo de sus necesidades, estado actual, brechas tecnológicas y estado objetivo que se pretende alcanzar, de esta forma se diseña una estrategia que inicia con un inventario de los recursos tecnológicos e infraestructura critica, su nivel de riesgo y las vulnerabilidad latentes utilizando una o varias metodologías combinadas; seguidamente se construye el nuevo PDS ajustado a las necesidades de la compañía y alineado con sus objetivos estratégicos.

Dicho análisis da paso a la otra parte del proyecto que no es otra cosa que el fortaleciendo de la red corporativa al repotenciar su Appliance de seguridad perimetral, extendiéndolo a las sedes principales y rediseñando su política de seguridad general para lograr una gestión y mitigación máxima de ataques cibernéticos, al igual que la capacitación de todos los colaboradores con el objetivo de crear un canal de retroalimentación y aprendizaje constante que permita a todos los usuarios comprender el lenguaje de la tecnología, así como los deberes y precauciones en ciberseguridad al ser parte integral de la compañía.

Metodología: Inicialmente se realiza investigación teórica acerca de cómo diseñar un PDS, su alcance y fases de elaboración, conceptos clave de seguridad informática, políticas y descubrimiento de brechas tecnológicas.

Seguidamente se realiza un análisis conceptual y científico de herramientas de

ciberseguridad, tecnologías actuales y existentes en la compañía, sus mecanismos de aplicación y las diferentes amenazas y vulnerabilidades conocidas, así como sus características e implicaciones legales. Después, se define el/los Marco/s Metodológico/s útiles para el caso de estudio, siendo NIST CSF y MAGERIT la combinación ideal para el levantamiento de información, descubrimiento de riesgos y diseño del perfil objetivo a través de seis fases. Finalmente se plantea una nueva política general de seguridad informática aplicable a todos los colaboradores de la compañía, formato para el registro de eventos de ciberseguridad, plan de capacitaciones y rediseño de configuraciones y políticas de Firewall de seguridad perimetral.
Conclusiones: Este es un proyecto que puede ser replicado en cualquier compañía con un Appliance de seguridad perimetral similar o una intención de protección basada en dichos lineamientos, ya que la información es el activo más valioso de la actualidad y su protección una tarea desafiante para cualquier área o equipo de ciberseguridad, por tanto, implementar mecanismos de análisis y políticas de seguridad como las planteadas en el proyecto si duda garantizan un nivel de seguridad aceptable y escalable en la búsqueda de un sistema de seguridad sofisticado y medible.