UNIVERSIDAD RICARDO PALMA

FACULTAD DE INGENIERÍA

ESCUELA PROFESIONAL DE INGENIERÍA ELECTRÓNICA

Diseño de un sistema de ciberseguridad basado en Defense in Depth para protección del sistema de información de una empresa minera, 2021

TESIS

Para optar el título profesional de Ingeniero(a) Electrónico(a)

AUTOR(ES)

Collantes Maza, Alfredo Miguel

ORCID: 0009-0000-0353-4778

Ramos Vilela, Jessica Roxanna

ORCID: 0009-0001-1302-9246

ASESOR

Cuadrado Lerma, Luis Alberto

ORCID: 0000-0001-9689-3461

Lima, Perú

2021

Metadatos Complementarios

Datos del autor(es)
Collantes Maza, Alfredo Miguel
DNI: 42206180
Ramos Vilela, Jessica Roxanna
DNI: 43816626

Datos de asesor
Cuadrado Lerma, Luis Alberto
DNI: 10448199

Datos del jurado
JURADO 1
González Prado, Julio Cesar
DNI: 07702235
ORCID: 0000-0003-0384-7015

JURADO 2
Rodriguez Alcázar, José Luis Antonio
DNI: 08242196
ORCID: 0000-0003-2238-3017

JURADO 3
Rojas Tuya, Santiago Fidel
DNI: 09861770
ORCID: 0000-0001-9689-3461

Datos de la investigación
Campo del conocimiento OCDE: 2.02.01
Código del Programa: 712026

DISEÑO DE UN SISTEMA DE CIBERSEGURIDAD BASADO EN DEFENSE IN DEPTH PARA PROTECCIÓN DEL SISTEMA DE INFORMACIÓN DE UNA EMPRESA MINERA, 2021

INFORME DE ORIGINALIDAD

13%	13%	1%	4%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	repositorioacademico.upc.edu.pe Fuente de Internet	2%
2	www.welivesecurity.com Fuente de Internet	1%
3	repositorio.ug.edu.ec Fuente de Internet	1%
4	e-spacio.uned.es Fuente de Internet	1%
5	revistaesecurity.com Fuente de Internet	1%
6	www.360itgo.com Fuente de Internet	1%
7	es.scribd.com Fuente de Internet	<1%
8	www.infosecuritymexico.com Fuente de Internet	<1%

DEDICATORIA

A mis padres, hermana y abuela, que me han apoyado desde siempre. Desde pequeño me enseñaron la importancia del trabajo y dedicación, no solo con palabra sino con ejemplo, gracias a ellos que siempre me impulsan a seguir adelante. Esta culminación a seguir adelante. Esta culminación de todo es también parte de ellos y para ellos.

Alfredo Collantes Maza

Esta tesis está dedicada a Dios, a mis padres y hermana por ser mi pilar y acompañarme en cada paso que doy en este largo camino llamada vida. A Diego, mi esposo, por ser quien me reta cada día y me impulsa a ser un mejor profesional. A Cooper, que me acompañó en el proceso del desarrollo de esta tesis.

Jessica Ramos Vilela

AGRADECIMIENTO

Agradecemos a nuestro asesor, Luis Cuadrado, quien nos apoyó en el desarrollo de este proyecto. A la empresa minera, por habernos brindado la información que necesitábamos para realizar esta tesis. A todas personas que estuvieron presente durante esta etapa que ahora podemos dar por concluida y a Dios por guiarnos en todo momento.

Alfredo Collantes y Jessica Ramos

ÍNDICE GENERAL

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN

Actualmente, vivimos en confinamiento debido a la presencia del Covid-19, siendo el trabajo remoto la respuesta que han encontrado las empresas para la continuidad de la producción. Por tal, se ha creado un nuevo desafío para la ciberseguridad que es el brindar nuevas políticas de seguridad a la información crítica e importante.

El presente trabajo propuso una solución de ciberseguridad basada en *Defense in Depth* para la empresa objeto de estudio con la finalidad de asegurar la autenticación y control del acceso de terminales a la red interna independientemente del tipo de conexión (alámbrica o inalámbrica) a sus repositorios y/o sistemas de información, navegación a internet y mejorar la interconexión e intercambio de información entre la operación minera con las demás sedes de lima y provincias.

De esta manera, se logró plantear un sistema robusto que detecte cualquier amenaza a la información crítica y/o a la continuidad de los servicios de la empresa causando impacto negativo en la reputación de la empresa, perdida de ventas y retraso de procesos y tiempos de entrega que en el caso de la operación minera conllevaría serios problemas que pondrían en riesgo la continuidad de la misma y sus operaciones en general.

PALABRAS CLAVE: Ciberseguridad, Seguridad de la información, Defense in depth, ciberdelincuencia, Autenticación, TACACS+, Ransomware, Esquema AAA.

ABSTRACT

Currently, we live in confinement due to the presence of Covid-19; remote work has become the answer that companies have found for the continuity of production. Therefore, a new challenge appeared for cybersecurity, which is to provide new security policies to critical and important information.

The present thesis proposed a cybersecurity solution based on Defense in Depth for the company under study. In order to ensure the authentication and control of terminal access to the internal network regardless of the type of connection (wired or wireless) to its repositories and/or information systems, internet navigation and improve the interconnection and exchange of information between the mining operation with the other headquarters in Lima and the provinces.

Therefore, it was possible to propose a robust system that detects any threat to critical information and the continuity of the company's services. These threats could cause a negative impact on the company's reputation, loss of sales and delays in processes and delivery times that in the case of the mining operation it would entail serious problems that would put its continuity and its operations in general at risk.

KEY WORDS: Cybersecurity, Information Security, Defense in depth, cybercrime, Authentication, TACACS +, Ransomware, AAA Scheme.

INTRODUCCIÓN

La solución propuesta en el proyecto se centra en abordar la necesidad de la operación minera de proteger su información y el acceso a la misma mediante una provisión de nuevo *hardware* y *software* complementario que se integre de manera eficaz con el ya existente.

El proyecto se desarrolla a lo largo de 4 capítulos. En el capítulo 1, se establece el problema general y los problemas específicos sobre los cuales se desea trabajar y brindar una mejora y solución. Asimismo, se establecen en este capítulo el objetivo general y especifico, que tiene como resultado brindar un diseño propuesto de ciberseguridad basado en *Defense in Depth*.

En el capítulo 2, se describe la evolución histórica de la ciberdelincuencia y su crecimiento en el transcurso de los años, aprovechando el trabajo remoto y el avance tecnológico se ha convertido en una gran amenaza para las empresas. De esta manera, establecemos y presentamos el estado actual de la tecnología en cuanto a ciberdelincuencia, seguridad informática y seguridad de la información.

En el capítulo 3, se desarrolla el diseño de ciberseguridad basado en *Defense in Depth*. Esta solución toma en cuenta los requerimientos de seguridad de la información y la infraestructura de red actual de la empresa objeto del estudio, con la finalidad de brindarle una solución integral que no requiera reemplazar algún equipo ya existente.

Finalmente, en el capítulo 4 se presenta los aspectos administrativos, en el cual presentamos un cronograma de actividades simulado y analizamos el costo de inversión del diseño propuesto.

CAPITULO I: PLANTEAMIENTO DEL PROBLEMA

1.1. Descripción y Formulación del Problema General y Específicos

Los tres pilares que toda empresa requiere para sostener sus servicios críticos son: hardware, software y datos. Siendo este último uno de los más importantes, el cual requiere ser protegido contra daños o robos para evitar pérdida de información esencial que impacte en las operaciones de la compañía. Bajo esta premisa es crucial tener siempre un enfoque adecuado y sobre todo actualizado respecto a la seguridad de la información dado que la tecnología está siempre en constante evolución.

La presente investigación propone el diseño de un sistema de ciberseguridad basado en *Defense in Depth* con la finalidad de poder abordar los problemas actuales de vulnerabilidad de información que presenta una operación minera en la región de Cajamarca.

En los últimos años y debido a la emergencia sanitaria generada por el COVID -19 se ha incrementado el acceso remoto y el trabajo desde casa desde diversos dispositivos (laptops, celulares, tablets, etc.), todos estos nuevos escenarios de trabajo remoto han traído como consecuencia el aumento de la vulnerabilidad a los ataques cibernéticos ocasionando pérdidas en términos de ventaja competitiva, financiera, comercial y legal. Por ejemplo, tal como dijo Manuel Viera, presidente de la cámara minera de Chile en una conferencia realizada el en 2021: “Sabemos que los ataques pueden afectar a los sistemas administrativos de compras y licitaciones; al sistema de comercialización; además de ocasionar accidentes en los sistemas de control automáticos, a través de los hackeos, entre otros” (Guía minera de Chile, 2021). Adicionalmente menciona también que todo es trae consecuencias negativas como interrupciones operativas, un funcionamiento defectuoso de los equipos, robo de propiedad intelectual y secretos empresariales, perdido y/o eliminación de data de carácter privado y confidencial, tiempo de inactividad del proceso relacionados con las áreas afectadas y finalmente cuantiosas pérdidas financieras en el caso de los procesos mineros en particular.

En resumen, para cumplir con los requerimientos técnicos planteamos una solución de ciberseguridad que consiste en la provisión *hardware y software* de acuerdo a cada sección (autenticación y control de acceso a red y seguridad perimetral Internet y LAN (Centro de Datos y Operación Minera) que proveerá la autenticación y el control de acceso de terminales a la red interna, asegurando el

cumplimiento de las políticas de seguridad definidas. La infraestructura propuesta está basada en una solución de Cisco y VMWARE que permitirá el acceso de los terminales a través de la conexión alámbrica o inalámbrica.

1.1.1. Problema General

¿Cómo diseñar un sistema de ciberseguridad basado en *Defense in Depth* para protección del sistema de información de una empresa minera?

1.1.2. Problema Específicos

a. ¿Cuáles son los problemas de vulnerabilidad de información que generan la innovación tecnológica y el trabajo remoto?
b. ¿Cuáles son los requerimientos de seguridad de información que tiene la empresa minera?

1.2. Objetivo General y Específicos

1.2.1. Objetivo General

Diseñar un sistema de ciberseguridad basado en *Defense in Depth* para protección del sistema de información de una empresa minera.

1.2.2. Objetivos Específicos

a. Identificar los problemas de vulnerabilidad de información que generan la innovación tecnológica y el trabajo remoto.
b. Evaluar los requerimientos de seguridad de información que la empresa minera presenta.

1.3. Delimitación de la Investigación: Teórica, Espacial y Temporal

Esta investigación se llevará a cabo en una operación minera que se encuentra en la región de Cajamarca, a más de 3,000 metros de altitud. Se decidió acotar el período de estudio entre mayo 2021 hasta setiembre 2021.

El presente estudio involucra el análisis de las vulnerabilidades que toda empresa enfrenta en la actualidad debido al crecimiento de los ciberataques y la posición de la operación minera frente a este escenario y sus políticas de seguridad, la cual nos servirá de base para el desarrollo de la solución de ciberseguridad propuesta.

1.4. Justificación e Importancia

1.4.1. Justificación

a. Justificación tecnológica

La evolución constante de la tecnología hace imprescindible buscar la manera de poder hacer frente a estos cambios tecnológicos tratando en lo posible de actualizar las herramientas de control de información o de

cambiarlas de ser necesario. Es también importante pensar en que existen casos en que por ejemplo bases de datos y/o información se encuentran desprotegidas dado que en el momento que fueron creados los protocolos de seguridad eran suficientes o simplemente era impensable la necesidad de proteger esta información por considerarse innecesario o inviable siquiera pensar que alguien pudiera acceder a ella haciendo uso de la tecnología existente en ese momento.

De acuerdo a un estudio de IBM, la presencia de los *ransomware* se ha incrementado en los últimos años alcanzando casi el 40% de los mensajes SPAM en el 2016. Según Limor Keseem, asesor ejecutivo de seguridad de IBM Security, los ciberdelincuentes aprovechan nuestra dependencia de los dispositivos y de la digitalización de recuerdos, información financiera y secretos comerciales; por lo cual, se requiere de una vigilancia renovada para protegernos de estos métodos de extorsión.

Acorde con el estudio Estado del Riesgo Cibernético en Latinoamérica en tiempos del COVID- 19 realizado por Marsh, líder en consultoría, brokerage de seguros y administración de riesgo, y Microsoft, más del 30% de las empresas latinoamericanas han recibido un intento de ciberataque, el 31% de los ataques se han realizado durante la pandemia del COVID -19, siendo phishing la principal amenaza. Los ataques cibernéticos en el Perú se han incrementado en un 242% entre el antes y después de la pandemia, sólo en febrero del 2020 se registraron 787,774, para marzo del mismo año la cifra ascendió a 2,7 millones.

Cabe mencionar que el análisis esta investigación para brindar la mejor solución de ciberseguridad consideró la infraestructura de red (*hardware*) actual de la organización objeto de estudio, la cual está basada en una solución al 100% en equipamiento de la marca Cisco. Además, como nos menciona el Gerente de IT en la entrevista brindada la empresa considera de vital importancia centralizar el soporte en un operador para reducir el tiempo de repuesta y fuga de información.

b. Justificación Económica

No solo la tecnología para prevenir estos ataques se ha incrementado a través de los años, sino también las modalidades de ataque. Tal como dijo Brian Dye, ex presidente senior de seguridad informática de Symantec el software

antivirus está muerto (ESET, 2017). Argumentando que los ciberdelincuentes se aprovechan de las vulnerabilidades que aún eran desconocidas por los desarrolladores y fabricantes de estos programas de antivirus.

Inga Beale, CEO de Lloyds, señaló que los ciberataques les han costado a las empresas del mundo un aproximado de USD 400 mil millones en 2015 (ESET, 2017).

Una empresa PYME requiere de 33,700 euros para resolver un problema de seguridad como fuga de datos o ciberataques según un informe de Kaspersky citado por el Incibe.

Según la organización objeto de estudio, cuando un fabricante integra todos los componentes de red está se centraliza el soporte evitando pagar por más de un equipo de soporte o especialistas. Además, permite un crecimiento ordenado, sin dejar de lado, las actualizaciones de software de los equipos; los cuales al ser del mismo fabricante evita la desactualización y/o compatibilidad con los otros componentes. Este escenario sería diferente si se tratase de diferentes fabricantes.

1.4.2. Importancia

Entre las funciones principales de un sistema de ciberseguridad se encuentran categorizar y proteger el acceso a la información ante posibles ciberataques, siendo esta necesidad aún más relevante hoy en día en tiempos de confinamiento y pandemia causados por el COVID-19, dado que el acceso remoto a redes corporativas de empresas es mucho mayor y demanda un esfuerzo adicional el control y seguridad de la información.

CAPÍTULO II: MARCO TEÓRICO

2.1. Antecedentes del Estudio de Investigación

Teóricamente, el primer hacker registrado de la historia fue Nevil Maskelyne, quien logró interceptar en 1903 la primera transmisión de telégrafo inalámbrico, exponiendo así las vulnerabilidades del sistema desarrollado por Guillermo Marconi. Posteriormente fue el ciberdelincuente de nombre John Draper, quien logró realizar llamadas telefónicas gratis pudiendo engañar a la central haciendo uso de un silbato que se obsequiaba en las cajas de cereales de "Cap'n Crunch". (OPTIV, 2020).

Ya en los años 70 surge el primer malware de la historia moderna: Creeper, se trataba de un programa que se copiaba a sí mismo y que mostraba el mensaje: *"I'm a creeper, catch me if you can!"*. Es la respuesta. Este acto nace también el primer antivirus llamado Reaper, el cual se encargaba específicamente de buscar al virus y eliminarlo. En los años 80 el *malware* se volvió más común, esto trajo como consecuencia que también los antivirus se hicieran más eficientes. Optiv (2020) nos también que dice ya por el año 1986 Markus Hess y cómplice fueron arrestados en Alemania Occidental por haber hackeado el Laboratorio Nacional Berkely y vender la información robada a la KGB. Paso Seguido en 1986 aparece el conocido Morris Worm (gusano Morris), el hizo caer el internet primitivo de aquella época conocido también como ARPANET, demostrando así que cada vez los virus se vuelven más problemáticos y en respuesta a esto nace la primera compañía dedicada a los antivirus.

Finalmente, alrededor de 1995, en Europa se forma un comité de expertos en delitos informáticos para proteger a la sociedad frente a la ciberdelincuencia. En el año 2001, se aprobó y firmó el Convenio de Budapest, que hoy en día es integrado por 56 países.

A lo largo de los años, la ciberseguridad ha sufrido una evolución progresiva. Esto se genera en respuesta a las necesidades de defensa ante ataques informáticos a las distintas entidades y empresas con finalidades como el robo y venta de información, bases de datos, encriptación de información, etc.

Es en esta eterna lucha entre atacantes y defensores informáticos que nace la ciberseguridad, quien es la llamada a la protección de la información digital de los sistemas. Es por esta razón que la ciberseguridad es muchas veces considerada dentro de la seguridad de la información.

En los dos últimos años, el mundo se ha enfrentado a muchos cambios y nuevos retos debido a la crisis provocada por el coronavirus. Esto ha implicado en algunos casos

una nueva forma de trabajo desde casa que antes era muy limitada o simplemente impensable hasta antes de todos los acontecimientos que se dieron a raíz de la pandemia. Todo esto hizo del trabajo remoto algo más habitual y común, lo cual trajo consigo nuevos desafíos de seguridad que hasta este momento no habían sido siquiera planteados en algunos casos.

Según el informe (ESET, 2021) la nueva normalidad que trajo el COVID-19 generó en los responsables de ciberseguridad la necesidad de replantearse el esquema de seguridad y/o modificarlo de acuerdo a los nuevos requerimientos de las empresas para su correcto funcionamiento pudiendo así implementar el teletrabajo o trabajo desde casa de manera segura. Esto implicó por ejemplo cambios de prioridades de acceso, establecimiento de nuevas condiciones y protocolos de seguridad, re asignación de niveles de seguridad, etc.

A todo esto, hay que sumarle que el hacer estos cambios de manera correcta y óptima implican no solo en muchos casos un gasto de dinero para el cual no estaban preparados los presupuestos de las empresas sino también un tiempo de demora para el desarrollo, modificación y ajuste de los sistemas en general.

ESET (2021, p04) en su informe Seguridad de la información menciona: “Por ejemplo también que para el 76% de los ejecutivos y responsables en la toma de decisiones, el presupuesto para el área de seguridad se mantuvo o se redujo con respecto a años anteriores, y el 81% aseguró que los recursos con los que cuentan para seguridad resultan insuficientes”.

Si bien es cierto antes de la pandemia ya se hablaba de una alta tendencia de ciberataques en general, esta tendencia se mantuvo e incluso se hizo más común en algunos casos, según estudio de Ciberseguridad en América latina de 2021 de ESET se tiene por ejemplo los siguientes datos:

Los códigos maliciosos son la principal preocupación (64%) y la primera causa de incidentes de seguridad (34%) en las empresas latinoamericanas.

De acuerdo con la telemetría de ESET, las empresas en Brasil (19%) fueron las más afectadas por el malware según el total de las detecciones en Latinoamérica durante 2020, seguidas por las de México (17,5%) y Argentina (13,3%).

El número de ataques de fuerza bruta a los servicios de acceso remoto como RDP creció 704%, mientras que los registros para usuarios únicos aumentaron 196% durante 2020 en Latinoamérica.

El malware para la minería de criptomonedas aumentó su actividad hacia finales de 2020 en concordancia con el aumento en el valor de las criptodivisas. Tailandia (17,9%) fue el país con mayor porcentaje de detecciones, seguido de Perú (10,1%) y Ecuador (5,1%).

Con base en la telemetría de ESET, las empresas de Brasil (26,4%) fueron las más afectadas por casos de phishing durante 2020, seguidas por las empresas de Perú (22,8%) y México (12%).

Hoy en día, las redes de empresas incluyen redes domésticas en las cuales la seguridad informática o ciberseguridad es o simplemente nula o en su defecto muy limitada en comparación a los protocolos de seguridad implementados en una empresa grande compuesta de cientos de usuarios todos trabajando en una misma red a la sombra de servidores, protocolos de seguridad, restricción de accesos, permisos de usuarios, antivirus, etc.

Hemos de pensar que anteriormente a la crisis ocasionada por el COVID-19 los ámbitos hogar y oficina estaban en el 99% de los casos casi separados o su interacción era prácticamente nula, salvo para leer y contestar e-mails corporativos (ESET, 2021).

A día de hoy es necesario tener en muchos casos acceso a información de vital importancia para la empresa de manera remota desde todos estos nuevos puestos de trabajo desde casa, también llamados home office.

Es en este ámbito donde ya no solo juega un papel importante el factor de la ciberseguridad y la seguridad de la información sino también el factor humano con relación a la ciberseguridad, es también un reto el informar y explicar a los empleados el correcto uso de los nuevos accesos y privilegios que tienen ahora a la información desde la comodidad de sus hogares, información que antes era impensable que saliera de las oficinas.

2.1.1 Antecedentes Internacionales

Yerequi, D. (2018) en su tesis titulada Ciberseguridad aplicada a la e-democracia: análisis criptográfico y desarrollo de una metodología práctica de evaluación para sistemas de voto electrónico remoto y su aplicación a las soluciones más relevantes; para titularse como Ing. De Producción y computación en la Universidad de Leon, España; en sus conclusiones manifiesta que: En el caso en particular del voto electrónico remoto (VER) a los peligros habituales de cualquier actividad on-line se suman unos

requerimientos más exigentes de seguridad y un fuerte efecto llamada para potenciales atacantes por la trascendencia de lo que está en juego.

Villalba, A. (2015) en su tesis titulada La ciberseguridad en España 2011 – 2015 una propuesta de modelo de organización; para titularse como Dr. ciencias políticas y sociología en la universidad nacional de educación a distancia, España; en sus conclusiones manifiesta que Estados Unidos ha sido el país pionero al confeccionar la primera estrategia de seguridad nacional, en 1987, en el marco de una reforma integral de la seguridad y la defensa en el país que duró cuatro años y en la que intervino el Senado y la Cámara de Representantes de modo conjunto, dando lugar al Acta Goldwater-Nichols, que generó las bases del planeamiento estratégico moderno en Estados Unidos, inspirado en una serie de pensadores estratégicos, que adaptaron el modelo de Maquiavelo de la "razón de Estado" y de la búsqueda de raíces del "fenómeno guerra" de Clausewitz.

Aguirre, A. (2017) en su tesis titulada Ciberseguridad en Infraestructuras Críticas de Información en la Universidad de Buenos Aires, Argentina; en sus conclusiones manifiesta que Si bien esta problemática (de ciberseguridad) ha sido afrontada en ciertos sectores como el bancario, el comercio electrónico y las telecomunicaciones, se detecta un nivel de concientización bajo en otras verticales esenciales de la economía y por lo tanto, se vislumbra un largo camino a recorrer para lograr un adecuado nivel de protección del ciberespacio.

2.1.2 Antecedentes Nacionales

García, J; Huamani, S (2019) en su tesis titulada Modelo de gestión de riesgos de seguridad de la información para pymes en el Perú; para titularse como Ing. Electrónica en la Universidad Peruana de Ciencias Aplicadas, Perú; en sus conclusiones manifiestan que Los resultados obtenidos permitieron la reducción del riesgo de seguridad de la información dentro de la Pyme sobre los activos más críticos, se lograron identificar los componentes de una gestión de riesgos, y se propusieron controles e indicadores para que la Pyme pueda mejorar con respecto al riesgo y mantener un constante monitoreo del mismo.

Aguilar, A; Meléndez R, (2019) en su tesis titulada Modelo de referencia para identificar el nivel de madurez de ciberinteligencia de amenazas en la dark

web; para titularse como Ing. Electrónica en la Universidad Peruana de Ciencias Aplicadas, Perú; en sus conclusiones manifiestan que Tener la visibilidad de en un escenario adicional como la web oscura representa una estrategia de ciberseguridad más madura y llevar a la empresa de un nivel "normal" a un nivel "avanzado", lo cual permitirá mejorar sus proceso relacionados.

Beteta, J; Narva De la Cruz, M (2018) en su tesis titulada Análisis de la preparación de las organizaciones Mapfre Perú Seguros y Kallpa Corredora de Seguros ante las amenazas de seguridad de la información en el medio empresarial y que podrían impactar en sus operaciones de negocio; para titularse como Licenciado en Administración de Empresas en la Universidad Peruana de Ciencias Aplicadas, Perú; en sus conclusiones manifiestan que se invierte en seguridad de la información en las empresas grandes como es el caso de la aseguradora Mapfre Perú, debido a que es consciente que mantiene múltiples bases de datos, sistemas, aplicaciones con información sensible para el negocio que realiza; y de sufrir algún tipo de pérdida, secuestro o daño la información podría impactar severamente en términos operativos, financieros, legales y de reputación. Lo cual no ocurre en las empresas pequeñas como Kallpa corredora de seguros debido a que sus procesos y servicios de negocio son menos complejos y/o de menor ámbito respecto a la aseguradora, sin embargo, también maneja información sensible y requiere se implemente una gestión de seguridad de la información con sus respectivos controles.

2.2.Estructura Teórica y Científica que sustenta el Estudio

2.2.1. Ciberseguridad

La ciberseguridad o seguridad informática es la que se encarga de los distintos métodos, técnicas y procesos que buscan almacenar, distribuir y proteger la información en su versión digital, se puede considerar entonces que la ciberseguridad se encuentra dentro de la seguridad de la información (Romero,2018). Los términos de ciberseguridad y seguridad de la información se diferencian porque la primera incluye también tecnologías o prácticas ofensivas para atacar a sus adversarios, mientras que la segunda solo debe ser usado para aspectos defensivos.

Aguilera (2011, p09) define: “La seguridad informática es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable”.

2.2.2. Defense in Depth

Tal como señala (Gomez 2011, p51) podemos definir Defense in Depth de la siguiente manera: “Es un principio que consiste en el diseño e implementación de varios niveles de seguridad dentro del sistema informático de la organización”.

Defense in Depth se define simplemente como tener diversos niveles de controles de seguridad en más de una de las 3 áreas fundamentales de seguridad, siendo estas áreas el control administrativo, el control físico y el control técnico.

Se trata de un arreglo multicapas en el que si un mecanismo de seguridad falla automáticamente se activa la siguiente capa o protocolo para detener el ataque. Es también conocido comúnmente como *“castle approach”* pues al igual que un antiguo castillo medieval es necesario sortear diversos obstáculos y/o trampas si es que se quiere entrar en el usando la fuerza.

Si lo pensamos un poco nos daremos cuenta de que *Defense in Depth* se asemeja mucho por ejemplo a la seguridad física que se tiene en un edificio o recinto importante al cual se necesita acceder diaria o periódicamente según las necesidades de cada visitante. Cada edificio tendrá entonces su propio sistema de control de ingreso de personal y vigilantes compuesto por varias etapas y/o capas, algunas podrían parecer incluso redundantes, pero tiene una finalidad específica que los hace necesarios para evitar visitantes no deseados o intentos de robo de bienes o documentos importantes, por ejemplo.

Un acceso físico a una embajada tendría por ejemplo algunos de estas capas:

En el caso de empleados:

- Acceso mediante una tarjeta de empleado con un código asignado previamente.
- La entrada tendrá un pórtico detector de metales por el cual es inevitable pasar para poder ingresar.
- Es necesario escanear la tarjeta frente a un lector el cual contrasta con una base de datos por horario si es que el empleado está intentando entrar en el horario de trabajo que le corresponde.

- Un hecho el ingreso al lobby nos dirigimos al ascensor el cual se activa nuevamente con la tarjeta del empleado y le habilita el piso que le corresponda según su función.
- Una vez en el piso se puede ingresar a su oficina pasando nuevamente su tarjeta de empleado.

En el caso de Visitantes o personas que necesitan el acceso solo por un día para realizar un trámite o alguna solicitud:

- Acceso mediante una cita previa solicitada online indicando el día, hora y motivo de la visita.
- Es necesario presentar el código de verificación que se obtuvo al momento de solicitar la cita online.
- La entrada tendrá un pórtico detector de metales por el cual es inevitable pasar para poder ingresar.
- Dado que en el código están los datos del visitante y su motivo de visita este puede ser direccionado al piso o lugar que le corresponda según sus requerimientos.

Como vemos, si quisiéramos podríamos hacer cada vez más y más complejo el acceso y variar en función a las necesidades y riesgos de seguridad que presente el edificio en el caso de ambos ejemplos.

Uno de los primeros elementos básicos que encontramos como primera línea de defensa será el análisis de tráfico de red. Son los *firewalls* los llamados prevenir el acceso no autorizado a una red bloqueando o permitiendo según sea el caso basándose en protocolos o reglas de seguridad previamente establecidas.

Paso seguido encontraremos a los ya conocidos *software* Antivirus los cuales son críticos para la protección contra malware y virus.

En el análisis de Integridad de la data se verifica el checksum de los archivos. El checksum corresponde a la representación matemática de un archivo, esto le indica al sistema datos valiosos del mismo como por ejemplo la frecuencia del uso de ese archivo.

Este valor puede ser contrastado con una base de datos de virus o código malicioso para descartar alguna infiltración, por ejemplo, si el *checksum* de un archivo le resulta único o desconocido al sistema, este puede marcar dicho archivo como sospechoso o malicioso. El análisis de datos puede revisar

también por ejemplo la IP de la cual se está intentando acceder para asegurarse de que se trata de una fuente de acceso confiable o autorizada.

El análisis de comportamiento se activa por ejemplo en caso de que el *firewall* y/o las distintas protecciones de intrusión fallen en detectar o detener la intrusión. En esta etapa se envían alertas o se toman incluso acciones de control y ejecución para evitar que la brecha de seguridad se siga expandiendo, para que el sistema sepa cómo debe reaccionar en caso a un "comportamiento extraño" es necesario definir previamente cual será el "comportamiento normal" de sistema y sus funciones habituales.

Desde el primer instante en que se duplica la cantidad de procesos de seguridad y/o verificación o se aumentan las "capas de seguridad" las probabilidades de tener una brecha importante de seguridad se reducen considerablemente.

Si por ejemplo un hacker se infiltrara en un sistema que consta de varias capas de Seguridad no solo le tomaría mucho más tiempo tratar de acceder a la información que desea, sino que al ser tan complejo el sistema de seguridad está alerta y le proporciona tiempo valioso a los administradores de red para poder defenderse del intruso antes de que logre hacer un daño irreparable a la base de datos, por ejemplo.

Capas esenciales en un mecanismo que posee *Defense in Depth* deben incluir como mínimo:

- *Passwords* robustos y complejos
- Software Antivirus
- Gateway de seguridad: es una solución que, mediante la detección y filtrado del tráfico web, con técnicas de *antimalware,* URL *filtering* y detección de *sites* maliciosos protegen la navegación a internet
- Firewall: programas de *software* o dispositivos de *hardware* que filtran y examinan la información que vienen a través de su conexión a Internet. Representan la primera línea de defensa porque pueden evitar que un programa malicioso o un atacante obtengan acceso a su red y a su información.
- Malware: Es un término que abarca cualquier tipo de *software* malicioso diseñado para dañar o explotar cualquier dispositivo, servicio o red programable. Los delincuentes cibernéticos generalmente lo usan para

extraer datos que pueden utilizar como chantaje hacia las víctimas para obtener ganancias financieras.

- Patch Management: Es una solución relativamente pequeña para una vulnerabilidad de seguridad o un error en un componente de *software*. Los proveedores de *software* trabajan continuamente para solucionar problemas en su producto y luego proporcionan rápidamente a los usuarios una actualización importante de la versión o un parche.
- Backup y recovery de data
- Seguir la normativa de "darle all usuario la cantidad mínima de permisos posibles para que puedes realizar su trabajo"

A medida que las compañías crecen y son ellas sus necesidades, es también necesario expandir y/o mejorar las capas de seguridad, por ejemplo:

- Aplicar el uso de 2 factores de autenticación (2FA) o multifactor de autenticación (MFA): es el proceso de autenticación donde se combinan dos de los tres posibles factores de autenticación. Los posibles factores de autenticación son:
    - Algo que el usuario sabe (contraseña, número de identificación personal(PIN) o respuesta a una pregunta secreta)
    - Algo que el usuario tiene (por ejemplo, un token, teléfono móvil, USB, llavero, etc)
    - Algo que el usuario es (por ejemplo, reconocimiento de voz o rostro, biometría de comportamiento, huella digital, retina o escaneo del iris)
- Hacer uso de sistemas de prevención y detección de intrusiones
- Segmentación de red
- Encriptación de data: es una de las herramientas de seguridad más empleadas para proteger información sensible, ocultándola.
- Prevención de pérdida de data

2.3.Definición de Términos Básicos

- Amenazas a la información: Definido por Gómez (2011, p60) como: "Cualquier evento accidental o intencionado que pueda ocasionar algún daño en el sistema informático, provocando pérdidas materiales, financieras o de otro tipo a la organización".

- Autenticación: La autenticación es algo que usualmente se piensa que es únicamente o principalmente aplicable a los usuarios y sus identidades y data, pero no es siempre este el caso. No se busca verificar un usuario, ya que la autenticación no siempre está relacionada con estos, en muchos casos se quiere saber si un cambio o un dato es correcto, no se debe cometer el error en pensar que solamente las personas necesitan este proceso, este puede ser para cualquiera, un sistema, un dispositivo o una persona (Castro, 2018).
- Ciberdelincuencia: Palabras como ciberataques, ciberdelincuentes forman parte de nuestro vocabulario a raíz del uso de las nuevas tecnologías para cometer ataques cibernéticos contra gobiernos, negocios e individuos. Estos delitos no conocen fronteras, ni físicas, ni virtuales, causan importantes daños y suponen peligro muy real para las víctimas de todo el mundo. La ciberdelincuencia crece exponencialmente y los ciberdelincuentes son cada vez más ágiles explotan las nuevas tecnologías y adaptan sus ataques utilizando nuevos métodos y cooperan entre sí de manera nunca antes vista hasta ahora.
- Checksum: Es una larga cadena de letras y números que actúan como una especie de huella digital de un archivo o conjunto de archivos para indicar el número de bits incluidos en la transmisión. Si el valor del *checksum* es diferente del original puede alertar que el archivo ha sido manipulado o dañado. A partir de esto, el receptor puede investigar qué salió mal o intentar volver a descargar el archivo.
- DdoS (Denegación de servicio distribuido en español): es básicamente un ataque que tiene entre sus principales objetivos el lograr inhabilitar un servidor. Esto se puede lograr mediante diversas formas como, por ejemplo: agotamiento de los recursos del sistema, saturación de ancho de banda, etc. Otra manera común de ataque es por ejemplo enviar un volumen muy grande de solicitudes a la vez al recurso web con la finalidad de saturarlo y superar su capacidad de respuesta, esto hace que el recurso web se vuelva lento o simplemente deje de funcionar debido a que su capacidad de respuesta se ve superada por la cantidad tan grande de solicitudes (Karspersky, 2021).
- Hackers: Tal como señala (Gomez, 2011) el termino hacker es acuñado a una persona que posee grandes y profundos conocimientos en informática e internet, así como lenguajes de programación.

- Información: Dentro de la norma (ISO 27000:2018, p12) encontramos lo siguiente: “La información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia necesita estar adecuadamente protegida”, asimismo se aclara que la información puede ser material, digital o representada en forma de conocimiento, experiencia o *know how* por parte de los trabajadores o empleados que laboran desempeñando distintas en la empresa.
- Firmas IPS (Sistema de prevención de intrusos) basado en firmas es un sistema que básicamente cuenta con una base de datos de firmas, que en este caso se tratan de patrones conocidos de amenazas y/o ataques a la seguridad. El sistema luego se encarga de realizar una detección haciendo uso de comparaciones de esta base datos en búsqueda de coincidencias y patrones, de esta manera puede establecer si existe una posibilidad real de ataque (INCIBE,2020).
- Metro LAN: Nos referimos a una versión reducida de lo que sería una Macro LAN dado que una Metro LAN permite conexiones entre sedes de una misma área (comúnmente una misma provincia a diferencia de una Macro LAN en la cual se puede establecer conexiones a nivel nacional. Al respecto, Cepeda K., Edison A. (2006) en su tesis titulada Implantación de la red Metrolan Netuno en la Universidad central de Caracas, Venezuela; manifiesta que “Una red Metro LAN está diseñada para proveer servicios de interconexión entre dos usuarios de redes LAN separa dos geográficamente, utilizando el estándar Ethernet como protocolo central”.
- Políticas de Seguridad: Son declaraciones y reglas formales ya establecidas en una empresa, las cuales deben de cumplirse para garantizar un correcto funcionamiento del sistema informático. Asimismo, la (ISO 27000:2018, p7) nos dice: “Son intenciones y direcciones expresadas formalmente por la gerencia”.
- RADIUS: Podemos entender el esquema de radius como un servidor que se encarga de controlar los diferentes los accesos de los usuarios a una red de datos. Gomez (2011. p477) lo define como: “Un protocolo de Autenticación que se basa en la figura de un servidor centralizado de autenticación, encargado de autenticar conexiones remotas de forma segura”. Cabe mencionar también que Radius tiene la tare de verificar tanto el nombre de usuario como su respectiva contraseña. En caso el acceso sea verificado y

autorizado es radius quien se encarga de asignar una IP privada al dispositivo del usuario.

- Replicación de Datos: Comúnmente se habla de replicación de una base de datos como una manera de forma de incrementar tanto el rendimiento como la disponibilidad de la base de datos en sí. La replicación permite que ciertos datos de una base de datos en concreto sean almacenados y replicados en más de un sitio logrando con esto una mejora en el funcionamiento de las consultas globales hechas a la base de datos (Elmasri & Navathe, 2002). Por otro lado, replicación asincrónica se trata de actualizar las modificaciones en una réplica para luego encargarse más delante de la actualización de las demás copias o replicas.
- Seguridad de la Información: Castro (2018, p13) nos dice lo siguiente respecto a la seguridad de la información: "La seguridad de la información no se preocupa solo por el medio informático, se preocupa por todo aquello que pueda contener información, en resumen, esto quiere decir que se preocupa por casi todo". Esto quiere decir que, la seguridad de la información engloba las medidas y actividades que intentan proteger los activos de información, no solo en el ámbito digital sino con que abarca todo aquello que contenga información, sea de forma digital, física o en forma de ideas o conocimientos de personas que pertenecen a la organización.
- Sniffers:Al respecto Gomez (2011.p196) nos dice los siguiente: "Los Sniffers son individuos que se dedican a rastrear y tratar de recomponer los mensajes que circulan por redes de ordenadores en internet".
- TACAS y TACACS+ (Terminal Access Controller Access – Control System): Gomez (2011. p477) lo define de la siguiente manera: "Un protocolo similar a Radius, que emplea TCP para la transmisión de datos en lugar de UDP. El protocolo TACAS+ es una versión mejorada que separa la función de autenticación de usuarios de la función de autorización".
- Virus Informáticos: Están diseñados para copiarse a sí mismo y propagarse a otros dispositivos tanto como sea posible. Los virus informáticos proliferan infectando aplicaciones y el correo electrónico, y pueden transmitirse mediante medios extraíbles, sitios web infectados, archivos adjuntos de correo electrónico e incluso los *routers* de red.

a. Ransomware: Se define según Borghello (2009. p18) como: “Aplicaciones orientadas a “secuestrar” el sistema operativo o documentos del usuario para luego cobrar una “recompensa” por su recuperación”.

b. Troyanos: Permiten que un *hacker* (ciberdelincuente) se apodere completamente de su computadora y ejecute programas como si realmente estuvieran usando su teclado y mouse.

c. Phishing: Se puede entender, según lo explicado por Lara y Albán (2017. p18) como “Las personas consiguen información confidencial mediante el envío de un correo electrónico en el que engañan al beneficiario pidiéndole sus datos o claves para actualización de datos”.

- Vulnerabilidad: representa una debilidad en un sistema informático. Así, una vulnerabilidad es cualquier debilidad en el sistema informático que pueda permitir a las amenazas causarle daños y producir perdidas en la organización (Gomez, 2011).

CAPÍTULO III: DISEÑO METODOLÓGICO

3.1.Tipo de la investigación

Según lo explicado por Sampieri (2006. p103) “Los estudios descriptivos miden, evalúan o recolectan datos sobre diversos conceptos (variables), aspectos, dimensiones o componentes del fenómeno a investigar”. En nuestro caso, el enfoque de nuestra investigación busca analizar, profundizar y entender el comportamiento y posición de la empresa minera frente a las vulnerabilidades que la innovación tecnológica y el trabajo remoto originan.

Acorde con Sampieri (2006. p208) “Las investigaciones que recopilan datos en un momento único y cuyo propósito es describir variables y analizar su incidencia en un momento dado es un diseño de investigación transeccional o transversal”. Este es el diseño que realizaremos en esta investigación.

Para ello, se desarrolló un marco teórico para cada una de las variables que hemos identificado y que se requieren para esta investigación. Además, describiremos los controles de seguridad más conocidos que se implementan para reducir las amenazas internas.

El desarrollo de la investigación considera la siguiente metodología:

- Fase 0 - Planeación
  - Recopilación de información, permisos correspondientes.
  - Elaboración del marco teórico acorde a los parámetros encontrados en la investigación.
- Fase 1 - Estado Actual
  - Identificar los requerimientos de la empresa minera.
  - Entender los objetivos del negocio, retos actuales de seguridad y planes a futuro.
  - Revisar la arquitectura y capacidad actual de seguridad de la empresa minera.
- Fase 2 - Evaluación de Capacidades
  - Identificar los componentes de red y sus limitaciones.
  - Identificar riesgos, amenazas y políticas.
  - Identificar las capacidades de mitigación actual.
- Fase 3 - Diseño de Capacidades
  - Identificar capacidades de seguridad requeridas por cada componente de red.
- Fase 4 - Diseño de Arquitectura

- Generar el diagrama de la arquitectura de seguridad deseada.

3.2. Nivel de Investigación

El enfoque de nuestra investigación es de tipo descriptiva y transversal porque desarrollamos un marco teórico para cada una de las variables identificadas y describiremos los controles de seguridad más conocidos que se implementan para reducir las amenazas internas.

Además, busca enunciar los riesgos de seguridad que en la actualidad la empresa presenta y brindar una solución de red según sus necesidades.

Asimismo, para el análisis de tiempo, utilizaremos un Diagrama de Gantt en el que se especificó el esquema de trabajo y las actividades que contempla el desarrollo de la solución. El desarrollo del proyecto se realizará basados en una implementación tradicional considerando que se cuenta con un alcance definido, la complejidad propia del proyecto y la cantidad de dependencias que se tiene para su desarrollo que no permite brindar entregas continuas.

Finalmente, para el análisis económico revisaremos los indicadores más utilizados para evaluar la viabilidad de un proyecto.

3.3. Anteproyecto

3.3.1. Rubro de la Empresa

La organización objeto de estudio es una empresa minera cuya operación está ubicada a más de 3,000 metros de altitud en la región de Cajamarca, que cuenta con certificaciones internacionales en medio ambiente (ISO 14001), seguridad y salud (ISO 45001) y seguridad de la información (ISO 27001), siendo la última la más importante para nuestra investigación. Además, la empresa minera ha sido reconocida a nivel nacional e internacional por el buen desempeño en su gestión.

3.3.2. Estructura actual de la red de la empresa

Los equipos de red de la organización objeto de estudio son de un solo fabricante, CISCO. Además, un integrador le brinda servicio de voz, móvil, conectividad y *hosting* en dos centros de datos ubicados en Lima.

Su arquitectura de red que está diseñada en un esquema de alta disponibilidad en cada una de sus sedes. Así mismo, cuenta con un esquema de replicación entre la operación minera y un centro de datos, esta brinda alta disponibilidad les brinda replicación de storage, nivel de videoconferencia y voz IP.

La replicación entre los centros de datos es a través de una Metrolan dedicada de uso exclusivo y una red SAN, siendo la réplica síncrona. La replicación entre la operación minera y los centros de datos es de forma bidireccional.

Para nuestro análisis solo vamos a considerar la operación minera y los dos centros de datos, no consideraremos su sede principal y sus sedes remotas.

3.4. Solución Propuesta

El diseño propuesto consiste en la combinación de hardware y software centralizado en el modelo SAFE. Este servicio proveerá la autenticación y el control de acceso de terminales a la red de la operación minera, asegurando el cumplimiento de las políticas de seguridad definidas. Es decir, este servicio hace posible controlar que solamente los terminales que cumplan con todas las políticas de seguridad (autenticación, versión de software, antivirus, etc.) sean los únicos que puedan ingresar a la red. En cuanto a la infraestructura y hardware utilizados para llevar a cabo esta tarea se ha optado por una solución haciendo uso de Cisco y VMWare. Actualmente se cuenta en la empresa minera con aproximadamente 1000 dispositivos de red distribuidas en las diferentes sedes a través de conexión alámbrica e inalámbrica, razón por la cual se consideran estos 1000 dispositivos para el dimensionamiento de la solución. Dado que la empresa ya posee equipos y soluciones Cisco hemos optado por una solución que involucre la menor cantidad de cambios de estos componentes de red ya existente y también pensando en que el hecho de tener un solo integrador o marca responsable del mantenimiento de la red es una gran ventaja dado que los tiempos de respuesta se agilizan enormemente y no es necesario depender de terceros para la solución de problemas evitando así de paso también problemas de compatibilidades entre equipos de distintos fabricantes que podrían generar en algunos casos una inversión considerable si es que se tienen que renovar o comprar muchos equipos nuevos solo para que se puedan integrar con los equipos nuevos sugeridos en la solución.

3.4.1. Solución de Autenticación y Control de Acceso

La solución planteada considera el diseño de Cisco ISE para el control de acceso a la red, TACACS+ para gestión segura de los equipos de comunicación (ver Tabla 1) e implementación de Cisco Stealthwatch (ver Tabla 2) para la red de la empresa objeto de estudio. El Cisco ISE en el marco de control de acceso a red será implementado bajo un escenario distribuido entre la operación minera y centro de datos 01, este diseño considera implementar los

componentes de Cisco ISE de: administración, monitoreo y control de políticas de acceso en alta disponibilidad y para el servicio TACACS+ implementado en el Centro de Datos 01.

La solución se encuentra en el centro de datos 01, en caso de contingencia el usuario local de cada equipo de comunicación tomará acción sobre el esquema AAA.

Tabla 1: Distribución de Servidores Cisco ISE

Operación Minera	Centro de Datos 01
Administration/Monitoring & Troubleshooting Note 01 (Virtual)	Administration/Monitoring & Troubleshooting Note 02 (Virtual)
Police Service Node 01 (Virtual)	Policy Service Note 02 (Virtual)
	Policy Service Node para Servicio TACAC+ (Virtual)
	Licencia de TACACS+

Fuente: Elaboración Propia

Tabla 2: Distribución de servidores virtuales Cisco Stealthwatch

Operación Minera	Centro de Datos 01
Flow Collector Virtual 2	Flow Collector Virtual 1
	Console Management
Cinco mil (5,000) licencias de flujos por segundos	

Fuente: Elaboración Propia

a. Detalle de función de los componentes:

- Administración (*PAN – Policy Administration Node*): La función de este componente en particular es permitir realizar todas las operaciones administrativas en Cisco ISE. Se ocupa de toda la configuración relacionada con el sistema y las configuraciones que se relacionan con la funcionalidad como la autenticación, autorización, auditoria, y así sucesivamente.

En el diseño planteado para la solución se contempla la implementación de dos servidores, uno ubicado en cada sede (operación minera y Centro de Datos 01). Además, se validó que la plataforma Cisco ISE es totalmente compatible con la infraestructura de red que cuenta actualmente la operación minera.

- Monitoreo (*Monitoring & Troubleshooting Node*): Es lo que le da en este caso la particularidad al Cisco ISE de poder desempeñar la función de

colector de registro y almacenar mensajes de registro de toda la administración y nodos de servicios de Políticas de ISE en su red. Es este componente en particular quien proporciona herramientas de monitoreo avanzadas y es quien a su vez el que permitirá dar solución a los incidentes de acceso.

Según lo planteado en el diseño se considera la implementación de dos servidores (embebido en los servidores PAN), uno por cada sede, bajo un escenario de alta disponibilidad entre los centros de datos de la Operación Minera y el Centro de Datos 01.

- Servicio de Políticas (*PSN – Policy Service Node*): Es este componente el encargado de proporcionar el acceso a la red, la postura, el acceso para invitados, aprovisionamiento de clientes, y los servicios de perfiles. Es el llamado a evaluar las políticas y tomara todas las decisiones. Además, se encuentra distribuido entre los centros de datos de la Operación Minera y el Centro de Datos 01.
- TACACS+: Permite la gestión segura de los equipos de comunicación mediante AAA (*Authentication, Authorization y Accounting*) a través del registro de las actividades de operadores y administradores de la plataforma de red. La solución propuesta en este caso se encuentra en el centro de datos central, en caso de contingencia el usuario local de cada equipo de comunicación tomará acción sobre el esquema AAA.

b. Detalle de licenciamiento:

- ISE: Es una solución de CISCO de control de acceso a la red (NAC) y una plataforma que se encarga de verificar el cumplimiento de políticas mediante las cuales se define e implementa políticas de control y de acceso en toda la red desde una plataforma central. Permite establecer reglas específicas predefinidas las cuales deciden automáticamente quien tiene acceso a la información y que parte de la información puede ver y/o editar según corresponda los privilegios del usuario previamente definidas. Adicionalmente a esto ISE le proporciona a la red las siguientes capacidades:
    - Autenticación, autorización y contabilidad integradas (AAA), es decir acceso a la creación de perfiles, administración de políticas, postura y servicios para huéspedes.

- Visibilidad continua en toda su infraestructura de red, con esto se logra ver en todo momento que dispositivos están en su red y en qué lugar de esta están ubicados.
- Flujos de trabajo automatizados y más importante aún visuales que le permiten encargarse y controlar la incorporación y administración de empleados e invitados conforme vayan ingresando a la red.
- Segmentación automatizada la cual le permite administrar fácilmente el acceso a los recursos de la empresa y restringir cualquier posible movimiento lateral de las amenazas mediante microsegmentación.
- Garantiza una identificación precisa del dispositivo conectado a la red, sensores de dispositivos integrados, escaneo de puntos terminales y un servicio de alimentación de perfil de dispositivo. Tanto los portales de invitados móviles como los de escritorio son completamente personalizables le permiten simplificar y optimizar la experiencia de sus usuarios, al mismo tiempo que le brindan protección.

Cabe mencionar que el ISE propuesto hace uso de la infraestructura de red actual existente para hacer cumplir las políticas de seguridad y de esta manera se puede lograr optimizar el sistema, logrando de esta manera obtener un mayor provecho de la inversión inicial que hizo la empresa al adquirir los componentes actuales que posee la red, dado que los equipos que funcionan actualmente en la red son compatibles con la tecnología de segmentación definida por software de Cisco TrustSec. Mediante esta tecnología podemos, por ejemplo:

- Lograr contener amenazas de red evitando el movimiento no autorizado en puntos finales de la red y evitando la propagación de malware.
- Podemos ser capaces de segmentar las redes de basándonos en el control de políticas de acceso basado en roles y la segmentación definida por software.
- Es posible aplicar políticas de forma coherente en cualquier punto de la red sin complicadas redes VLAN.

- Stealthwatch Flow Collector: Es el encargado de categorizar, monitorear, analizar e identificar el tráfico de red y las posibles amenazas para crear una inteligencia de seguridad integral tanto a nivel de red y host. Así mismo, se encuentra distribuido entre las sedes de la Operación Minera y el Centro de Datos 01.

- Stealthwatch Management Console: Es quien gestiona, coordina y configura todos los StealthWatch Flow Collector existentes para poder de esta manera establecer, asegurar y correlacionar de manera inteligente el comportamiento de la red de la empresa minera. Además, estará instalado en el Centro de Datos 01.

En cuanto a la solución propuesta se incluyen las siguientes características y licenciamiento: Stealthwatch opera utilizando datos de red para acelerar y mejorar de esta manera la detección de anomalías, la respuesta a incidentes y los análisis forenses en toda la red. Stealthwatch establece también una línea de base compuesta por parámetros preestablecidos de lo que se considera comportamiento y actividad normales en la red. Bajo este punto de referencia es que se identifica una anomalía en la red y es así como se puede diferenciar un comportamiento anómalo en la red el cual a su vez pueda significar un ataque. La solución propuesta hace uso de los flujos de tráfico para supervisar en todo momento todo el entorno y determinar si se están produciendo infracciones de políticas y de acceso a la red teniendo siempre como referencia los "parámetros normales" previamente establecidos.

La solución propuesta monitorea continuamente el tráfico en su totalidad dentro de la red para identificar patrones anómalos de tráfico que pueden señalar abuso del sistema y amenazas internas. Esto permite ayudar a identificar y defenderse contra el malware de día cero, las amenazas persistentes avanzadas (APT), los intentos de DDoS y otros ataques antes que causen daños.

A continuación, se detallan algunas de las características principales del Stealthwatch propuesto:

- Otorga una comprensión simplificada del comportamiento normal de la red mediante el uso de NetFlow
- Permite la posibilidad de tener una gran visibilidad en el perímetro de la red, el interior, el centro de datos y la nube privada y pública.
- Realiza un monitoreo continuo de dispositivos, aplicaciones y usuarios a través de sus redes distribuidas.
- Fácil integración con su infraestructura de red existente, Cisco Firepower y Cisco ISE.

En el Figura 1 presentamos un ejemplo del Dashboard en el que se puede realizar el monitoreo de alarmas para su seguimiento y control (Ver Figura 1),

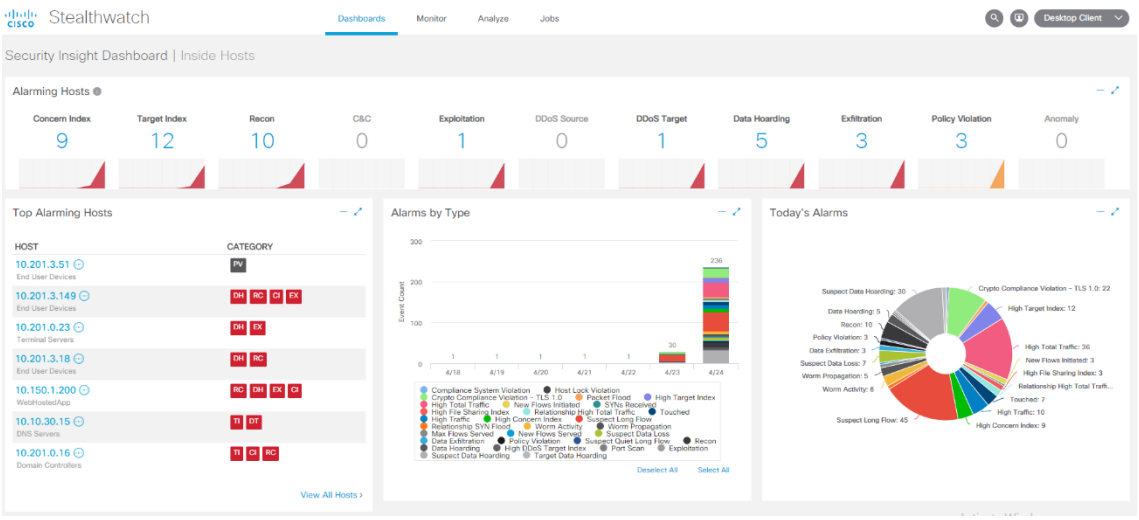


Figura 1: Security Insight Dashboard - Stealth watch

Fuente:https://www.cisco.com/c/dam/en/us/products/collateral/security/stealthwatch/stealthwatch-cte-test-drive-ins-lab-guide.pdf?dtid=osscdc000283

- MDM: De manera complementaria a la solución de Autenticación y Control de Acceso de ISE se adiciona un licenciamiento de una solución de MDM. El licenciamiento corresponde a 250 licencias VMware Workspace ONE Standard con soporte en la modalidad de producción (24x7), la cual se integra perfectamente con la solución de Autenticación y Control de Acceso propuesta de ISE/Stealthwatch.
- VMware Workspace One: Es una plataforma inteligente de espacio de trabajo digital con tecnología de VMware AirWatch mediante el cual puede administrar y suministrar cualquier aplicación en un dispositivo cualquiera de manera confiable y segura. Workspace ONE integra control de acceso, administración de aplicaciones y administración de terminales en múltiples plataformas. Cabe mencionar que Workspace ONE posee las siguientes características:
  - Administración de diversos dispositivos (plataformas: IOS, Android, Windows 7, 8 y 10, Windows phone, Symbian, Blackberry, Win, Apple Mac, Apple TV) en una sola consola, al mismo tiempo, así como diferente propiedad / uso (Cope, BYOD, Multiusuario).
  - Instalación de Airwatch Cloud Connector, que permite integración con: Syslog (Event log data), Corporate Networks, Email Management Exchange 2010 (PowerShell), EmailRelay (SMTP), Lotus Domino Web Service (HTTPS), Directory Services (LDAP/AD), BES – Blackberry, System Information and Event Management (SIEM).

3.4.2 Solución Perimetral Internet y LAN

Se considera para la solución planteada el diseño de un clúster Cisco FirePower 2130 para la protección perimetral de internet y un clúster Cisco FirePower 2120 para la protección perimetral de la granja de servidores ubicada en el Centro de Datos 01 con funcionalidades de firewall, control de aplicaciones, anti-malware y URL filtering para la protección perimetral de internet y funcionalidades de firewall, control de aplicaciones y URL filtering para la protección perimetral de la granja de servidores (ver Tabla 3). Ambos clústeres serán gestionados por la consola de gestión Cisco FMC 2500 que permite la actualización de firmas y nuevos ataques detectados por la nube de cisco que retroalimenta la solución de seguridad (TALOS).

Tabla 3: Distribución de Firewalls

DESCRIPCIÓN	CENTRO DE DATOS 01	CENTRO DE DATOS 02
PROTECCION MULTICAPA DE INTERNET	FPR2130-NGFW-K9 (Cisco Firepower 2130 NGFW Appliance, 1U, 1 x NetMod Bay)	FPR2130-NGFW-K9 (Cisco Firepower 2130 NGFW Appliance, 1U, 1 x NetMod Bay)
PROTECCIÓN DE CENTRO DE DATOS	FPR2120-NGFW-K9 (Cisco Firepower 2120 NGFW Appliance, 1U)	FPR2120-NGFW-K9 (Cisco Firepower 2120 NGFW Appliance, 1U)
GESTIÓN	FMC2500-K9 (Cisco Firepower Management Center 2500 Chassis)	

Fuente: Elaboración propia

a. Detalle de función de los componentes:

- Firewalls Perimetrales Internet (FPR2130-NGFW-K9): Protege el perímetro entre internet y la red de la empresa aplicando funcionalidades como firewall, control de aplicaciones, NGIPS, anti-malware y URL filtering. En el diseño planteado considera la implementación de dos Cisco FirePower 2130, uno por cada sede, bajo un escenario de alta disponibilidad entre los centros de datos 01 y 02.
- Firewalls Perimetrales para Centro de Datos (FPR2120-NGFW-K9): Protege el perímetro entre la granja de servidores y la red de la empresa aplicando funcionalidades como firewall, NGIPS, control de aplicaciones y URL filtering. En el diseño planteado se considera la implementación de dos Cisco FirePower 2120, uno por cada sede.

- Consola de Gestión (CISCO FMC 2500): Es la consola de gestión que se instalará en el Centro de Datos 01 y que manejará los dos (02) clúster FPR-2130-NGFW-K9 y FPR-2120-NGFW-K9 a implementar. La plataforma tiene la capacidad de manejar 60 millones de eventos y cuenta con 1.8TB de almacenamiento para eventos.

b. Detalle licenciamiento:

- Cisco TALOS: Se trata de una división de investigación e inteligencia frente a amenazas de Cisco, donde un grupo de expertos de seguridad proporciona una mayor protección a la comunidad de Internet y a los clientes, productos y servicios de Cisco. Esta división de investigación se encarga de detectar, analizar y proteger frente a amenazas para lograr esto hacen uso de datos de telemetría obtenidos de la red de Cisco los cuales incluyen miles de millones de peticiones web y de e-mails; millones de muestras de malware; datos de fuentes *open source* y millones de intrusiones de red. Talos Intelligence permite a Cisco proteger a sus clientes con mayor velocidad y eficiencia, dado que le es posible identificar las amenazas rápidamente.
- Cisco Firepower NGIPS: Permite tener automatización, flexibilidad y escalabilidad, permitiendo mediante el ajuste automático de las funciones IPS garantizar que las firmas IPS que se tengan en uso reflejen la realidad de su entorno, es decir escanea el tráfico de red de manera pasiva para identificar no solo lo que se cree que se tiene en el entorno sino lo que verdaderamente se tiene allí. Como ejemplo podemos pensar en una empresa que piensa que utiliza Microsoft Windows de manera exclusiva cuando en la práctica existen sistemas Linux en su red desconocidos para el área de TI los cuales también requieren protección. La tecnología de Cisco Firepower NGIPS incluye también inteligencia de seguridad con análisis de DNS, IP, y datos de URL. En la Figura 2 se muestra el esquema básico de este componente (Ver Figura 2).

Figura 2: Esquema Básico de Cisco Firepower

Fuente: Cisco Firepower

- Cisco Advanced Malware Protection (AMP): Mediante AMP se rastrea, descubre y bloquea la progresión del malware avanzado basado en la red. Cisco AMP *for Networks* está disponible con el Cisco Firepower NGFW propuesto en la solución y tiene la capacidad de integrarse con Cisco AMP Threat Grid con análisis estático y dinámico de malware.
- Cisco Application Visibility and Control (AVC): AVC usa en este caso el firewall de la aplicación L7 para identificar y controlar el acceso de los distintos usuarios existentes a más de 4000 aplicaciones aproximadamente.

  Cabe mencionar que Cisco AVC aplica también políticas móviles, sociales y otras de uso aceptable. Como ejemplo, puede hacer que las aplicaciones de las distintas redes o medio sociales más populares sean de solo lectura para cumplir con las regulaciones o normativas aplicables dentro de la empresa.
- Cisco Firepower Management Center: Otorga en este caso una administración centralizada de funciones de seguridad de red para múltiples NGFW físicos y virtuales. La idea es gestionar y correlacionar la inteligencia de los sensores de amenazas adicionales, incluidos los Cisco Firepower NGIPS y Cisco AMP para sensores de redes, y la defensa contra amenazas de Cisco Firepower. Además, permite la contención de amenazas rápida automática a través de la integración con el Cisco ISE propuesto en la solución. El centro de administración de Firepower de Cisco nos proporciona en este caso amplia inteligencia y manejo sobre los usuarios, las aplicaciones, los dispositivos y las amenazas que existen

en su red. Luego utilizara esta base de datos de información recopilada para analizar las vulnerabilidades de la red y proporcionar una respuesta adaptada de los eventos de seguridad ya conocidos. Puede tanto administrar funciones básicas de firewall como también controlar aplicaciones, investigar y remediar brotes de malware con facilidad.

3.4.3. Desarrollo de la arquitectura de Seguridad: Defense in Depth

El diseño de Ciberseguridad que proponemos está basado en Defense in Depth para brindar protección por niveles y/o capas según las políticas de seguridad que se defina. En cisco, el modelo que sigue este principio es el SAFE y es el que se eligió para este diseño porque permite abordar los requerimientos de la organización sujeto a estudio antes descritos dado que, mediante el empleo de la teoría de juegos con bloques de construcción enfocados en amenazas, y las mejores prácticas para defenderse contra ellos.

La idea detrás de esto es poder usar modelos simples en conjunto para poder centrarse en desafíos complejos. Se basa en el principio básico de descomponer algo complejo en varias piezas o trozos con la finalidad de simplificarlo en lo posible y abordarlo desde una o varias perspectivas distintas.

SAFE es un modelo y método de seguridad utilizado para asegurar el negocio. Se centra en las amenazas y mejores prácticas para defenderse de ellos. Además, utiliza conceptos simples para enfocarse sobre las complejidades de hoy, para estar preparados para los retos del mañana.

Este modelo es flexible a las necesidades de cada organización independiente de su tamaño. Personaliza y brinda la mejore arquitectura de seguridad para asegurar los objetivos del negocio teniendo en cuenta la política de seguridad de la organización utilizando los siguientes pasos:

- Identificar objetivos del negocio.
- Dividir la red en piezas manejables.
- Establecer un criterio para el éxito del negocio.
- Categorizar riesgos, amenazas y políticas.
- Construir la solución de seguridad.

Existen tres fases de construcción de la solución de seguridad y son las siguientes:

- Fase de capacidad: Haciendo uso de los objetivos del negocio, riesgos, políticas, justificando cuales capacidades de seguridad son requeridos en base a estos.

- Fase de arquitectura: Se hace uso de las capacidades justificadas y se las organiza en una arquitectura lógica.
- Fase de diseño: Teniendo ya la arquitectura definida se crea un diseño que se complete con una lista de productos, configuración, servicios y costos.

SAFE proporciona la clave para simplificar la ciberseguridad en Lugares Seguros en la red (PIN) para infraestructura y Dominios de Seguridad (Ver Figura 3).

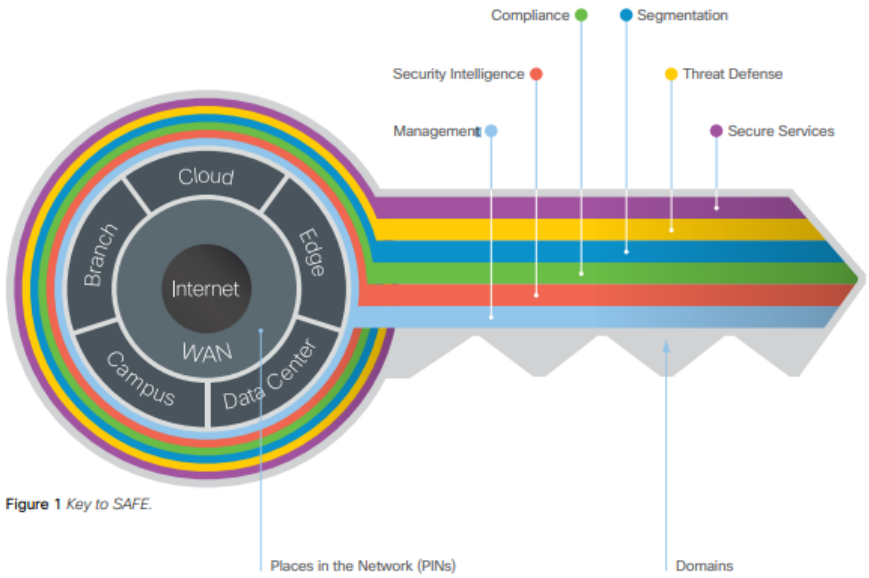


Figure 1 *Key to SAFE.*

Figura 3: Llave para SAFE

Fuente: Cisco https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/safe-overview-guide.pdf

La llave de SAFE se usa para mostrar ubicaciones y funciones operacionales que se usan comúnmente para ayudar a defenderlos. Es una herramienta principalmente de navegación. Se enfoca en resumir las principales áreas de ciberseguridad y cada componente tiene información adicional y detalles dentro el programa SAFE. Las secciones que siguen aclaran las capacidades funcionales necesarias para abordar las principales amenazas en cada lugar en el Red y en cada dominio de seguridad.

a. Lugares de Red (PIN-Places in the Network)

SAFE simplifica la seguridad de la red al proporcionar una guía de solución usando los Lugares en la Red (PIN) (Ver Figura 4). Estos son: Sucursales (*Branch*), Campus, WAN, Centro de Datos (*Data Center*), Perímetro Seguro (*Edge*), Nube (*Cloud*).

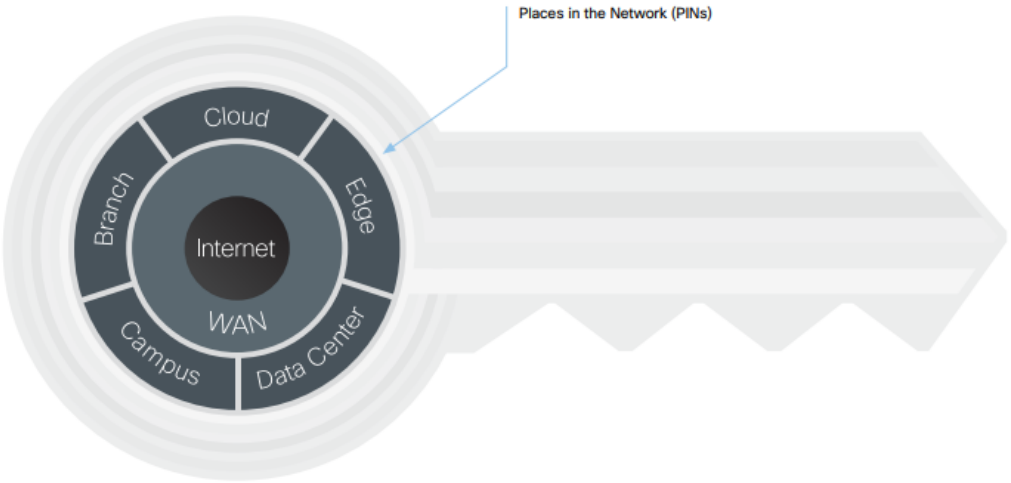


Figura 4: Lugares en la Red (PIN)

Fuente: Cisco(https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/safe-overview-guide.pdf)

- Sucursales Seguras (*Secure Branch*): Son las ramas suelen ser las menos seguras, porque son las menos controladas. Las principales amenazas mitigadas en este lugar son:
  - Endpoint Malware (POS Malware)
  - Actividad maliciosa de cliente no autorizado
  - Explotaciones de infraestructura inalámbrica.
- Campos Seguros *(Secure Campus)*: Son uno de los principales objetivos de los ataques porque contienen grandes poblaciones de usuarios con una variedad de tipos de dispositivos y tradicionalmente pocos controles de seguridad internos por la gran cantidad de zonas (subredes y VLAN), la segmentación segura es difícil. Las principales amenazas mitigadas en este lugar son:
  - Phishing
  - Explotaciones basadas en la web
  - Malware
  - Acceso a la red no autorizado
  - Pérdida de datos
- Centro de Datos Seguros (Secure Data center): Los centros de datos contienen la mayoría de activos de información y propiedad intelectual. Estos son los objetivos principales de todos los ataques y por lo tanto requieren el más alto nivel de esfuerzo para asegurar. Los centros de datos contienen cientos a

miles de servidores físicos y virtuales segmentados por tipos de aplicación, zonas de clasificación de datos y otros métodos. Creando y manejando apropiadamente reglas de seguridad para controlar el acceso que pueden ser extremadamente complejo. Las principales amenazas mitigadas son:

- Pérdida de datos
- Propagación de Malware
- Acceso a la red no autorizado (compromiso de la aplicación)

- Perímetro Seguro (*Secure Edge*): El perímetro es el PIN de mayor riesgo porque es el principal punto de entrada para el tráfico público desde Internet y el punto de la salida primaria para el tráfico corporativo hacia Internet. Al mismo tiempo, es el recurso del negocio más crítico en la economía actual basada en Internet. Las principales amenazas mitigadas son:
  - Vulnerabilidades del servidor Web
  - DDoS (*Distrinued denial of Service*)
  - Pérdida de datos
- Nube Segura (*Secure Cloud*): La mayoría de los riesgos de seguridad en la nube provienen de la pérdida de control, la falta de confianza, el acceso compartido y la información oculta. Los acuerdos de nivel de servicio (SLA) son la herramienta principal para que las empresas dicten el control de las capacidades de seguridad seleccionadas en los servicios basados en la nube. Se deben usar auditorías independientes de certificación y evaluación de riesgos para mejorar la confianza. Las principales amenazas mitigadas son:
  - Vulnerabilidades del servidor Web
  - Virus y Malware
  - Pérdida de datos
- WAN Segura: Conecta todas las ubicaciones de la compañía juntas para proporcionar un único punto de control y acceso a todos los recursos. Administrar las políticas de seguridad y calidad del servicio (QoS) para controlar la comunicación puede ser excepcionalmente difícil y complejo. Las principales amenazas mitigadas son:
  - Propagación de Malware
  - Acceso a la red no autorizado
  - WAN sniffing

Para el diseño de esta investigación se han identificado los siguientes PIN:

- Campus: Operación minera
- Branch: otras sedes de la empresa minera incluyendo los domicilios de los colaboradores debido al trabajo remoto.
- WAN
- EDGE
- Data Center: Centro de Datos 01 y Centro de Datos 02
- Cloud: Perímetro internet

b. Dominios de Seguridad

Los dominios seguros representan el lado operativo de la llave. La seguridad operacional está dividida por función y las personas en la organización que son responsables de ellos. Cada dominio tiene una clase de capacidades de seguridad y aspectos operacionales que deben ser considerados (Ver Figura 5).

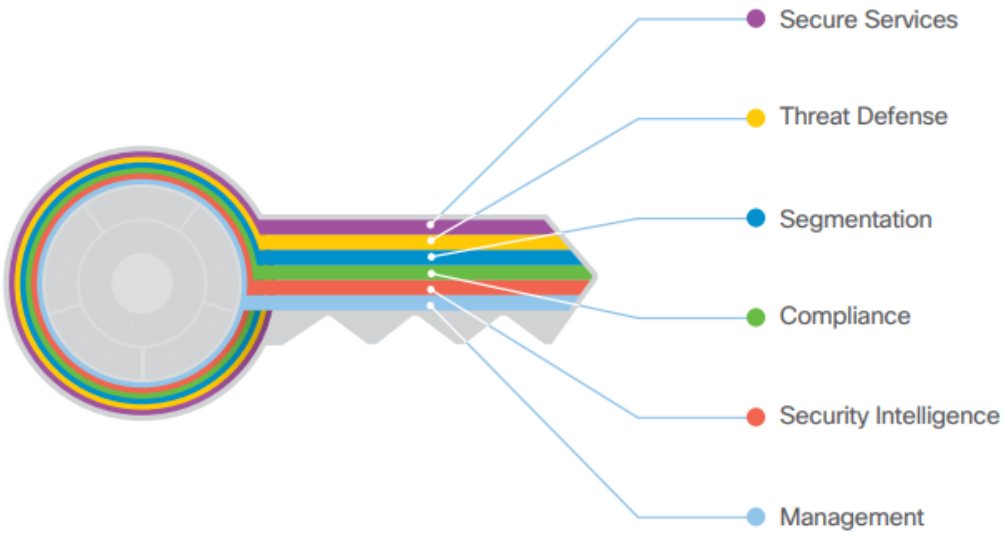


Figura 5: Modelo SAFE - Dominios de Seguridad

Fuente: Cisco (https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/safe-overview-guide.pdf)

A continuación, vamos a detallar cada una de los dominios de seguridad:

- Management: La gestión de dispositivos y sistemas, que usan servicios centralizados, es fundamental para lograr la implementación de políticas, administración de cambios en el flujo de trabajo y la capacidad de mantener los sistemas con parches. La administración coordina las políticas, los objetos y las alertas. La Figura 6 muestra la progresión de las capacidades de seguridad utilizadas para las operaciones de Management (Ver Figura 6).

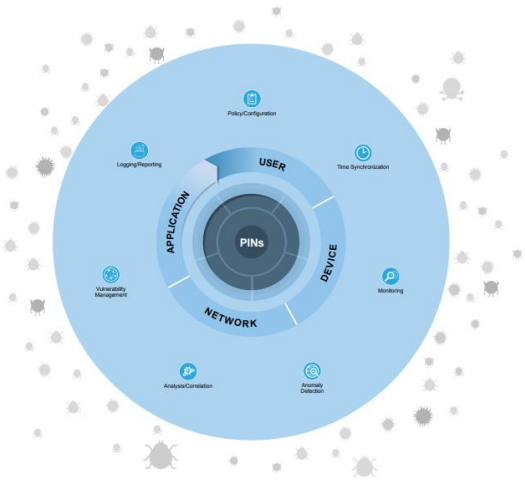


Figura 6: Management Domain Capabilities

Fuente: Cisco (https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/safe-overview-guide.pdf)

- Security Intelligence: Proporciona detección global de amenazas y malware emergente. Permite que una infraestructura cumpla las políticas de forma dinámica a medida que aumenta la reputación de nuevas amenazas, brindando una protección de seguridad precisa y oportuna. La Figura 7 muestra la progresión de las capacidades de seguridad utilizadas para las operaciones de Security Intelligence (Ver Figura 7).

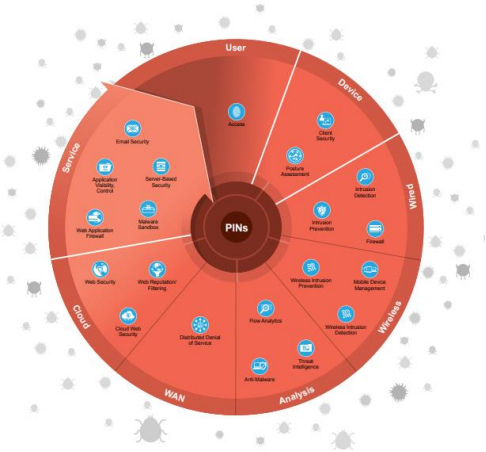


Figura 7: Security Intelligence Capabilities

Fuente: Cisco (https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/safe-overview-guide.pdf)

- Compliance: Aborda las políticas internas y externas. Muestra cómo los múltiples controles pueden estar cumplirse con una única solución. Ejemplo: auditoría HIPAA, PCI, SOX. Cabe mencionar que la gerencia de IT de la organización sujeto a estudio pasa alrededor de 14 auditorías en el año; entre

ellas, SOX. La Figura 8 muestra la progresión de las capacidades de seguridad utilizadas para las operaciones de Compliance (Ver Figura 8).

Figura 8: Compliance Capabilities

Fuente: Cisco (https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/safe-overview-guide.pdf)

- Segmentation: Establece límites para los datos y los usuarios. A través de la segmentación manual logra una combinación de direccionamiento de red, VLAN y firewalls para la aplicación de políticas. Aprovecha la infraestructura para hacer cumplir las políticas automatizadas y escalables. La Figura 9 muestra la progresión de las capacidades de seguridad utilizadas para las operaciones de Segmentation (Ver Figura 9).

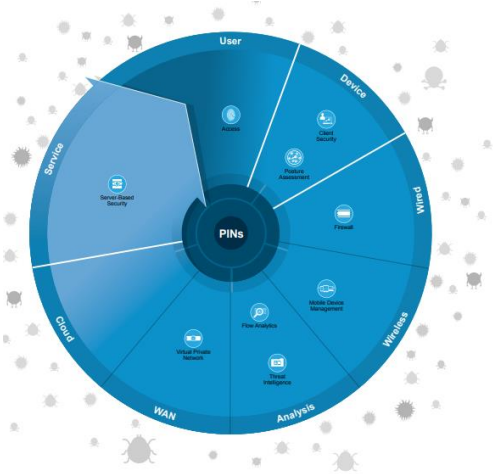


Figura 9: Segmentation Capabilities

Fuente: Cisco (https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/safe-overview-guide.pdf)

- Threat Defense: Proporciona visibilidad de los ciberataques y ciberamenazas más evasivas y peligrosas. Utilizando la telemetría del tráfico de la red, la

reputación y la información contextual, permite la evaluación de la naturaleza y riesgo potencial de la actividad sospecha para que pueda tomar medidas correctivas. La Figura 10 muestra la progresión de las capacidades de seguridad utilizadas para las operaciones de Threat Defense (Ver Figura 10).

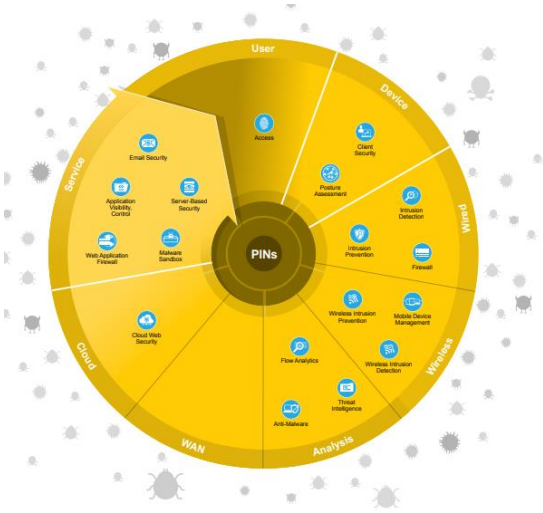


Figura 10: Threat Defense Capabilities

Fuente: Cisco (https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/safe-overview-guide.pdf)

- Secure Services: Proporcionar tecnologías como control de acceso, redes privadas virtuales y cifrado. Este dominio incluye protección para servicios inseguros como aplicación, acceso inalámbrico y comunicación unificada (colaboración). La Figura 11 muestra la progresión de las capacidades de seguridad utilizadas para las operaciones de Secure Services (Ver Figura 11)

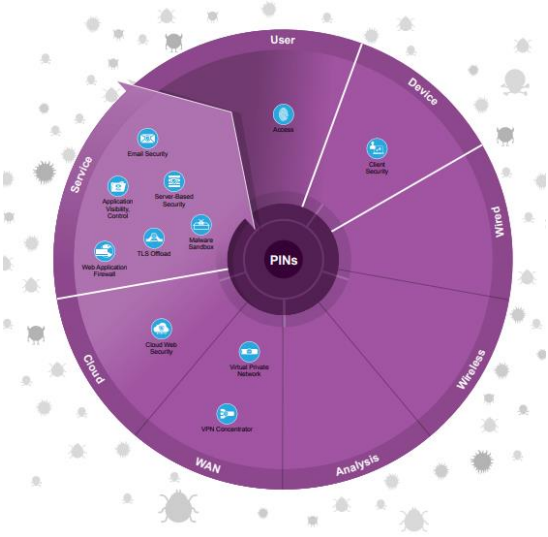


Figura 11: Secure Services Capabiilities

Fuente: Cisco (https://www.cisco.com/c/dam/en/us/solutions/collateral/enterprise/design-zone-security/safe-overview-guide.pdf)

3.5. Diseño Propuesto

3.5.1. Estructura de la arquitectura propuesta

La solución propuesta consiste en integrar a través del método SAFE (basado en el principio de Defense in Depth) la solución de autenticación y control de acceso (para proteger el acceso remoto a la red interna) y la solución Perimetral de Internet y LAN (proteger las conexiones alámbricas e inalámbricas).

A continuación, presentaremos la arquitectura que proponemos tanto para cada Centro de Datos (activo/ stand –by) y la operación minera (Ver Figura 12 y 13).

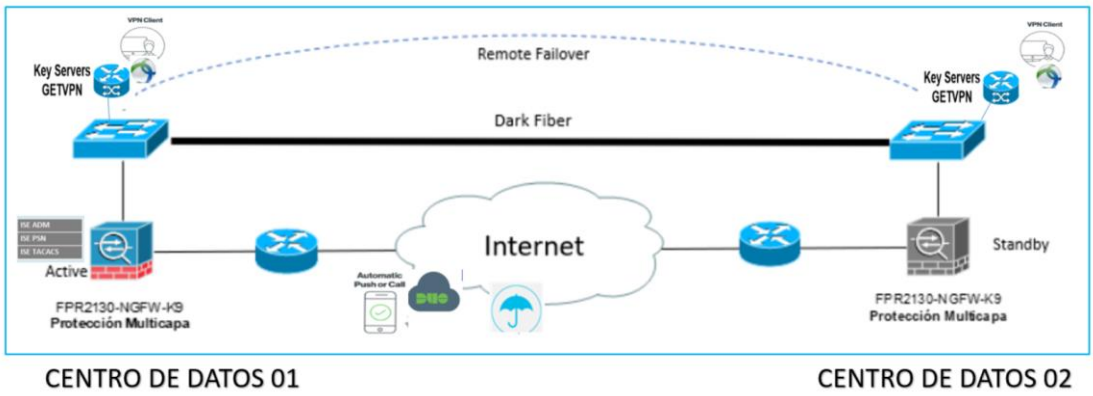


Figura 12: Arquitectura Ciberseguridad - Centro de Datos

Fuente: Elaboración Propia

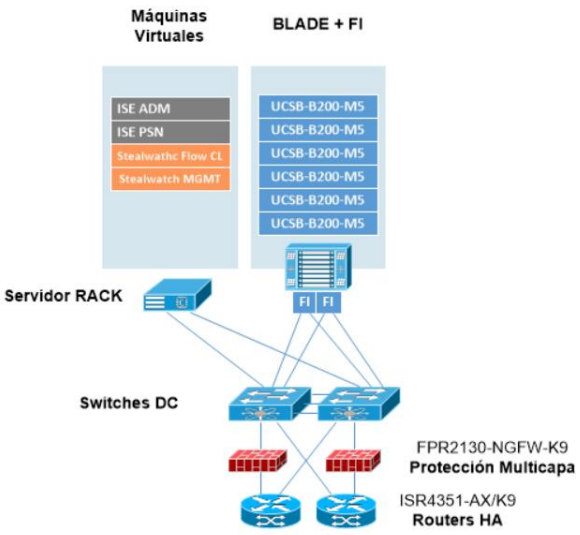


Figura 13: Arquitectura Ciberseguridad - Operación Minera

Fuente: Elaboración propia

La Figura 14 muestra la solución Perimetral de Internet y LAN de Centro de Datos y Operación Minera, esta propuesta muestra la estructura de red en los Centros de Datos y en la operación minera. Resaltando que los equipos de Firepower de los Centros de Datos 01 y 02 están en alta disponibilidad (Activo/stand by), lo cual permitirá la redundancia de acceso a los sistemas críticos de la empresa sujeta a estudio (Ver Figura 14).

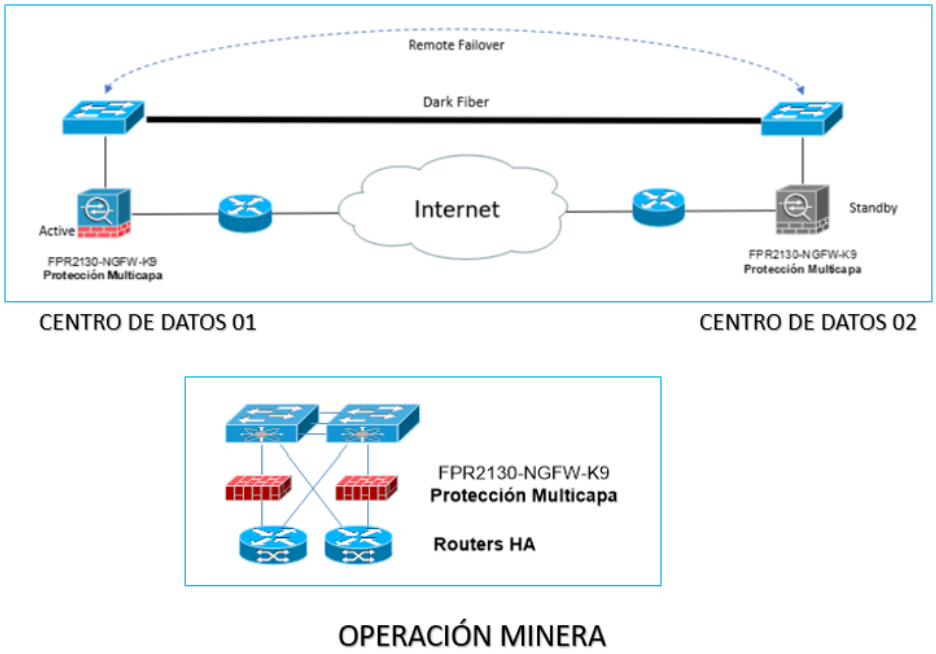


Figura 14: Solución Perimetral de Internet y LAN

Fuente: Elaboración propia

A continuación, presentamos la solución de Autenticación y Control de Acceso para la organización sujeta al estudio (Ver Figura 15). Los puntos optimizados son:

- Dispositivos endpoints protegidos:
  - AnnyConnect: Habilita acceso seguro a la red de la organización
  - Umbrella: Protección en la capa DNS
  - AMP: Protección, detección contra malware
- Doble factor de autenticación (Password + Token)
- Evaluación de postura de equipos
- Dos dispositivos en Alta Disponibilidad (Activo / Stand –by)
- Soporte activo 7 x24

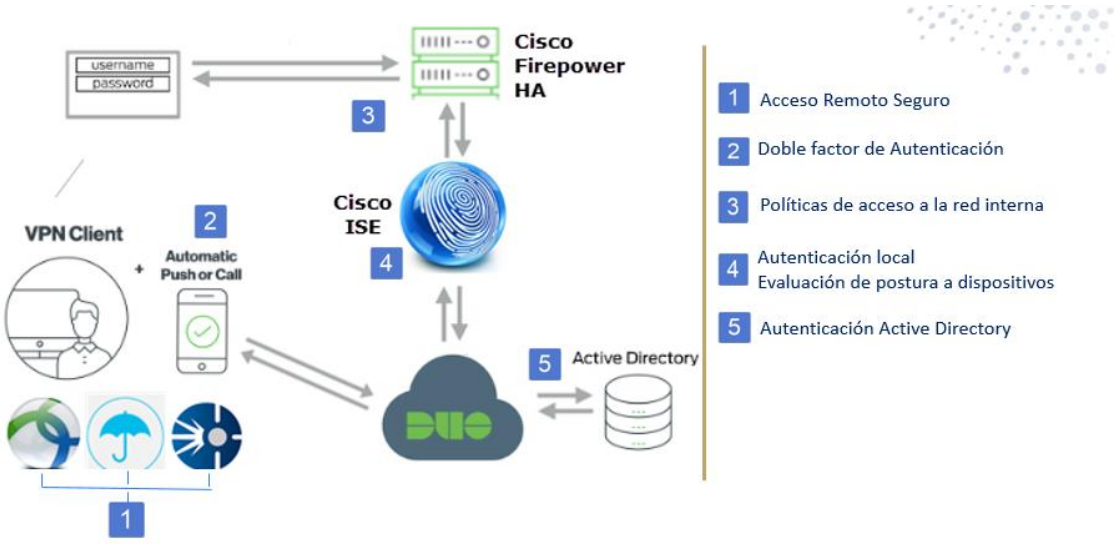


Figura 15: Solución de Autenticación y Control de Acceso

Fuente: Elaboración propia

3.5.2. Casos de Alta Disponibilidad

En las Figuras 16 se muestra el proceso de autenticación de usuarios, este proceso de realiza entre las diversas sedes remotas, la Operación Minera y el Centro de Datos 01(Ver Figura 16).

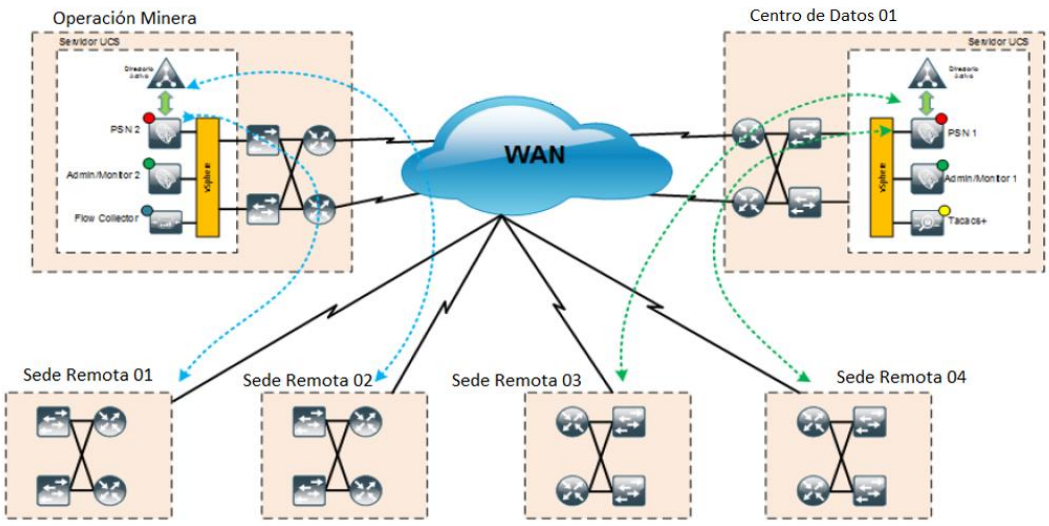


Figura 16; Diagrama de Autenticación de Usuarios

Fuente: Elaboración propia

En la figura 17 se muestra el caso la operación minera se vea afectada, la autenticación de los usuarios no se verá afectada y se realizará a través del Centro de Datos 01 (ver Figura 17). De esta manera se activa el mecanismo

de contingencia correspondiente de manera eficaz y fiable de control de acceso y autenticación.

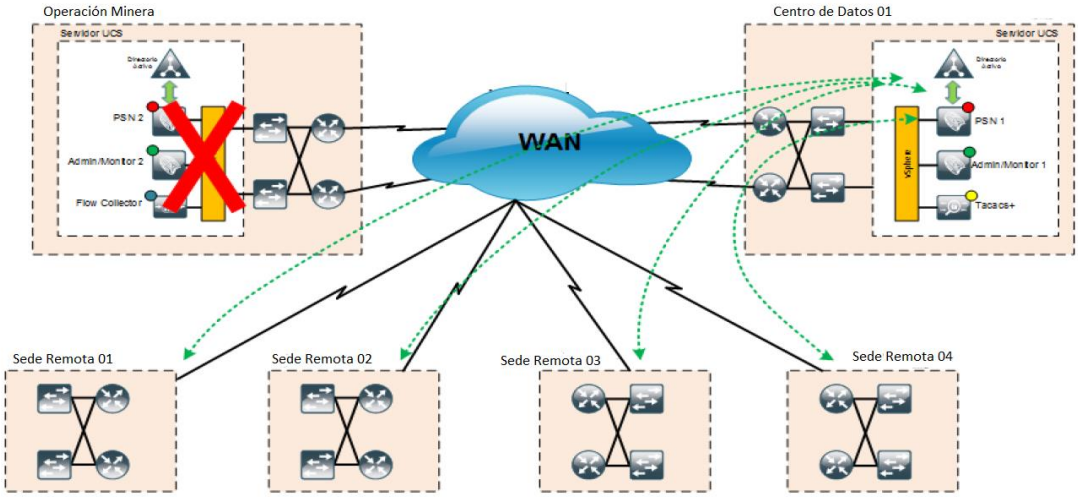


Figura 17: Diagrama de Alta Disponibilidad - Autenticación de Usuarios

Fuente: Elaboración Propia

En este escenario presentado en las Figuras 16 y 17, se contemplan la autenticación de las sedes remotas 01 y 02 puede realizarse desde la sede Operación Minera; mientras que las sedes remotas 03 y 04, lo hacen por el Centro de Datos 01. En ambos casos el proceso de autenticación es similar, haciendo primero uso de políticas ISE las cuales serán definidas previamente por el administrador de red, se hace uso también de un flow collector y de TACACS+ así como de la solución VMWare en ambos casos (Operación minera y Centro de Datos 01). En este caso de contingencia podemos observar como mejora fundamental que en caso se requiera, el Centro de Datos 01 está en la capacidad suficiente de asumir la tarea entera de autenticación de las demás sedes remotas mientras se solucionan y/o se revisa lo ocurrido y la gravedad de la brecha de seguridad ocurrida en la sede operación minera.

En la Figura 18 se muestra el diagrama el flujo de tráfico a través de los perímetros de seguridad de cada Centro de Datos y la Operación Minera (Ver Figura 18).

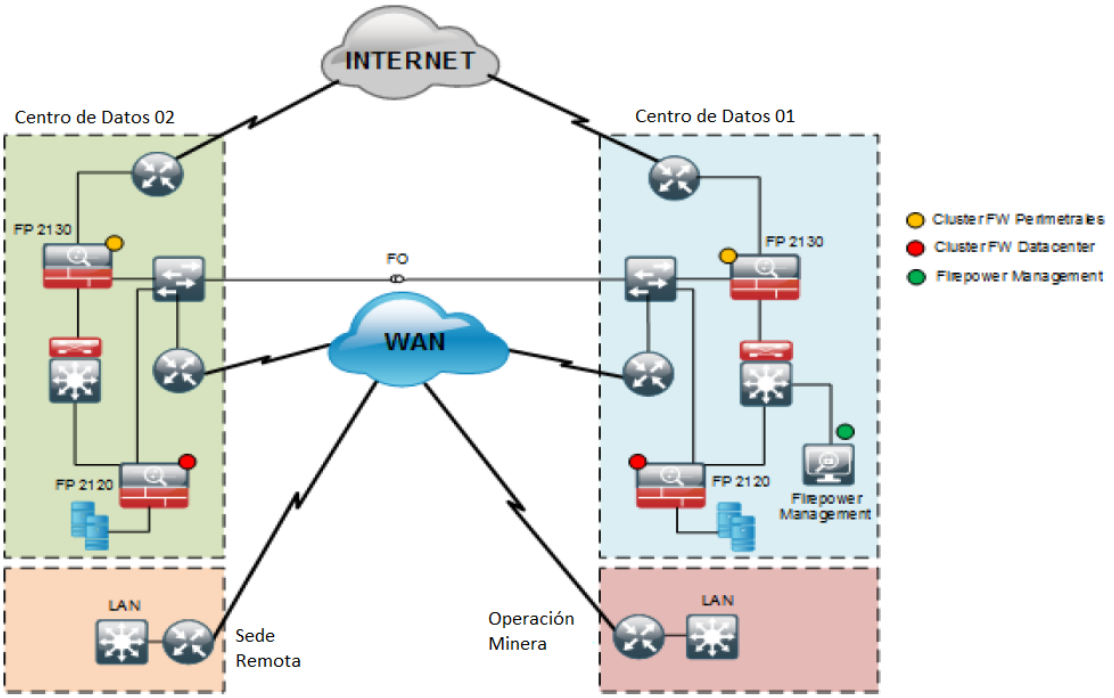


Figura 18: Diagrama de Flujo de Tráfico - Seguridad

Fuente: Elaboración Propia

En las Figuras 19, 20 y 21 muestran el diagrama del flujo de tráfico que se tendrá en caso uno de los equipos de seguridad Firepower sufra un ataque o se ve interrumpido su funcionamiento. De esta manera el tráfico es redirigido para poder seguir realizando las actividades necesarias con normalidad mientras se hace un análisis de seguridad respecto a lo sucedido con el funcionamiento de los equipos Firepower afectados. Anteriormente a esto no era posible y/o era hecho de manera deficiente. Asimismo, el diagrama muestra que la alta disponibilidad del servicio se mantendría a pesar de que uno de los equipos Firepower se vea afectado o incluso si ambos fueran comprometidos debido a alguna brecha de seguridad o algún fallo o desperfecto físico del equipo en sí.

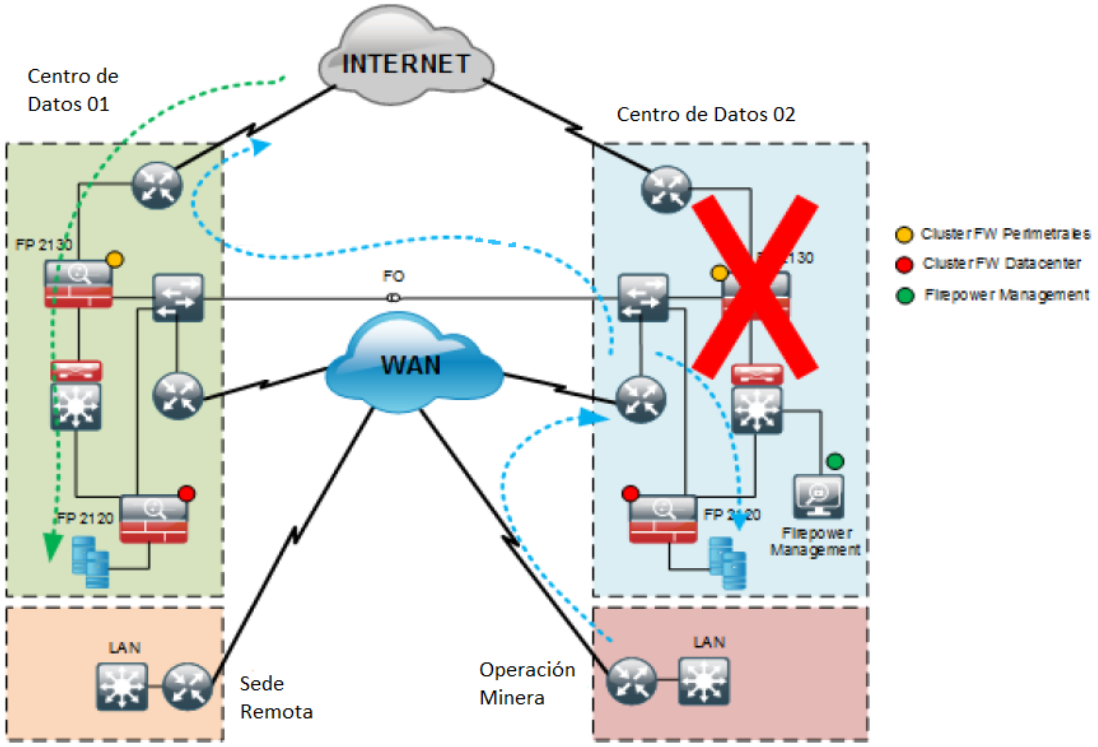


Figura 19: Diagrama de Contingencia 01 del Flujo de Tráfico del Centro de Datos 01- Seguridad

Fuente: Elaboración propia

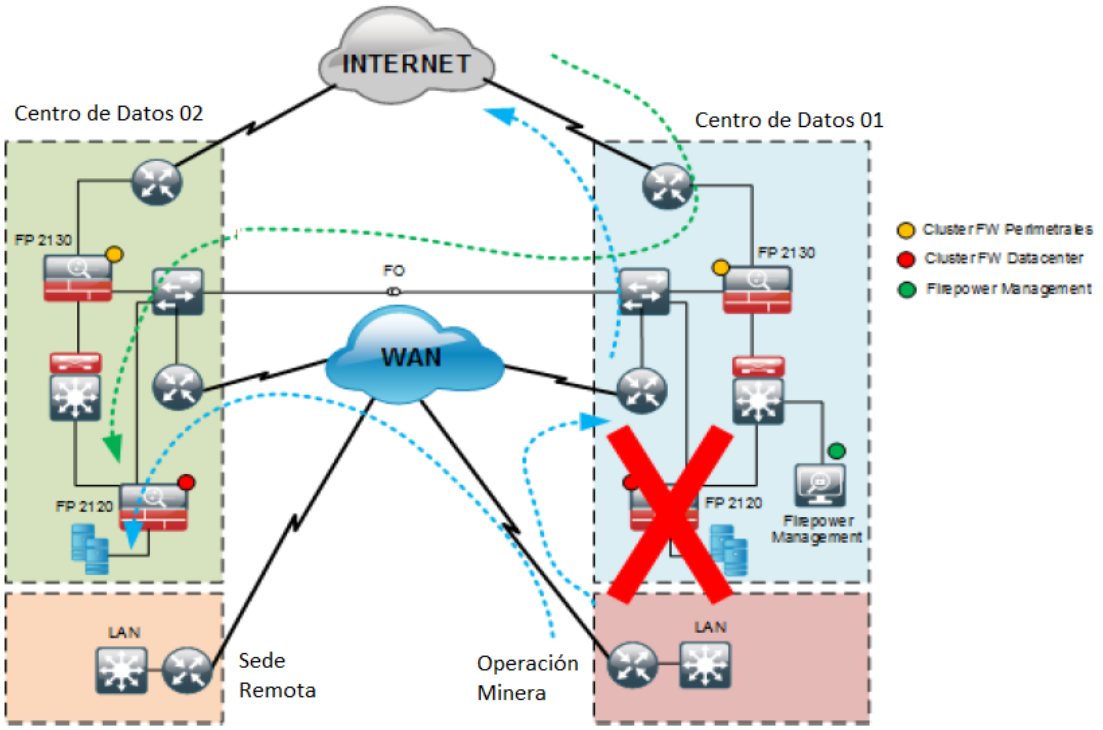


Figura 20: Diagrama de Contingencia 02 del Flujo de Tráfico del Centro de Datos 01 – Seguridad

Fuente: Elaboración propia

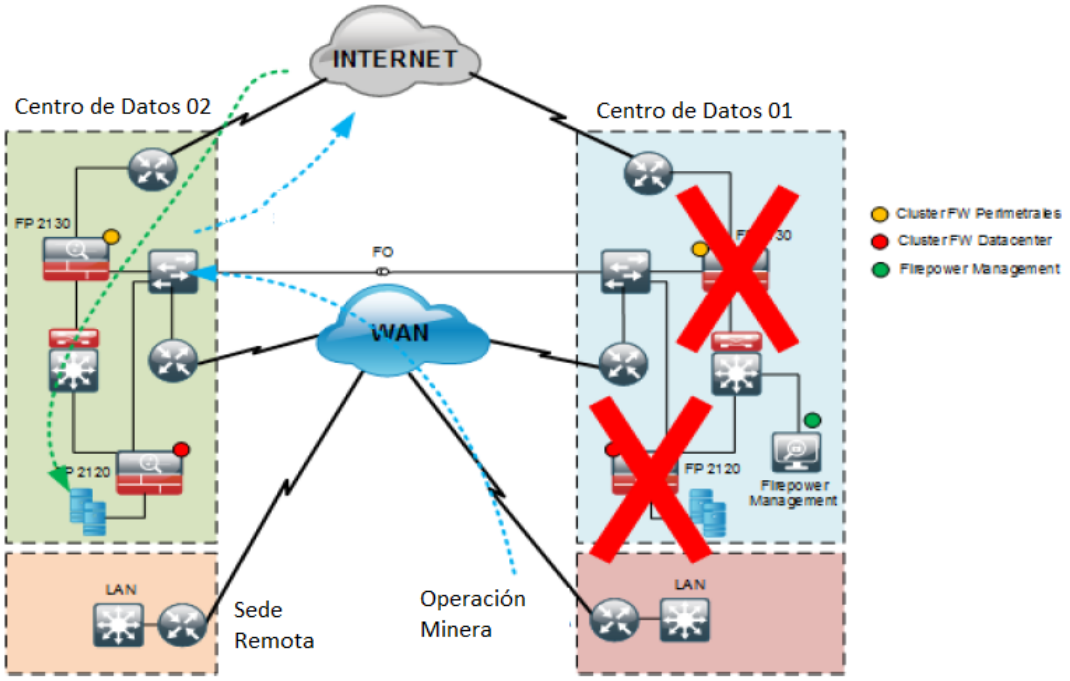


Figura 21: Diagrama de Contingencia del Flujo de Tráfico a través del Centro de Datos 02 – Seguridad

Fuente: Elaboración Propia

3.5.3. Implementación

Para implementar el diseño propuesto de manera ordenada, se sugiere tomar como base la metodología PMO y dividirlo en 05 fases: inicio, planeamiento, ejecución, seguimiento y cierre. Las tareas principales para la ejecución e implementación del proyecto se pueden enumerara de la siguiente forma:

- Planificación y coordinación de reuniones con la organización sujeto a estudio.
- La construcción de un cronograma del proyecto, en el capítulo 04 se indica el que planteamos para la ejecución del diseño propuesto.
- Es necesario también mantener una comunicación siempre fluida con la empresa minera para informar de los avances de la implementación, integración y/o puesta en marcha de los servicios con forme se vayan anexando al sistema existente.
- Escalar cualquier asunto relacionado con las actividades del proyecto de progreso con los interesados internos y externos (Operación Minera y fabricante).

- Planificación general del proyecto y de control para garantizar el calendario de reuniones de finalización del proyecto. Proponemos realizar reuniones diarias (15 minutos, asistentes: jefe de proyecto de la empresa integrador y minera) y semanales (30 minutos – asistentes: equipos de configuración y especialistas y jefe de proyecto de la empresa integrador y minera). Estas reuniones permitirán agilizar la solución de cualquier inconveniente que se presente en el desarrollo del proyecto.
- Luego del cierre de cada etapa del proyecto será necesario hacer una evaluación del sistema y su correcto funcionamiento antes de pasar a la siguiente etapa. Esto se repetirá etapa por etapa hasta terminar de implementar el proyecto en su totalidad.

CAPÍTULO IV: ASPECTOS ADMINISTRATIVOS

4.1.Cronograma de Actividades

Para el analizar el período de tiempo que tomaría la implementación de la solución propuesta presentamos un diagrama Gantt. Este contiene la estructura de ejecución del proyecto según la metodología PMO.

Según la simulación realizada la implementación de esta solución de ciberseguridad es de 149 días útiles. Cabe mencionar que se ha considerado un escenario ideal en el que no existen retrasos por entrega de equipos, factores internos o ajenos al proyecto, etc. Además, que las fechas presentadas son referenciales.

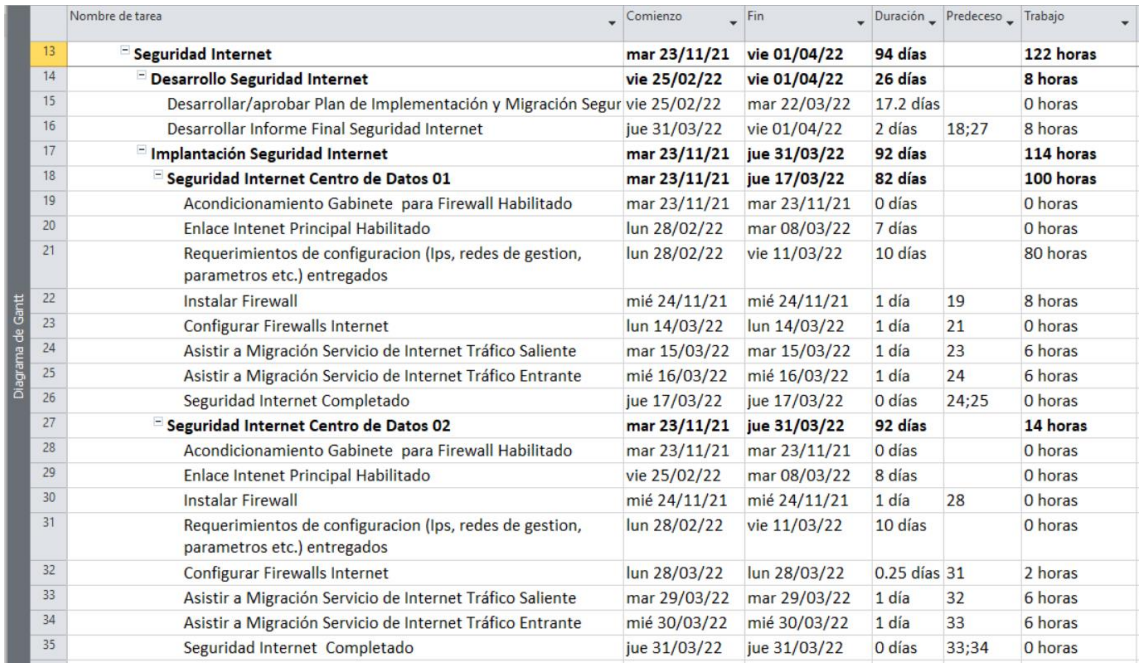
El cronograma de actividades la presentaremos en tres gráficos: En el primer gráfico, Figura 16 presentamos la estructura macro de la implementación y se muestra que la ejecución de esta solución se realizará en 310 horas hombre y que se desarrollaría en 149 días útiles (Ver Figura 16). En el segundo gráfico, Figura 17, realizamos un acercamiento a la etapa de ejecución y a una de sus dos principales fases: Seguridad de Internet (Ver Figura 17). En el tercer gráfico, Figura 18, presentamos la segunda fase de la etapa de ejecución: Seguridad LAN (Ver Figura 18).

Diagrama de Gantt

	Nombre de tarea	Comienzo	Fin	Duración	Predeceso	Trabajo
2	**Gestión del Proyecto: Solución de Ciberseguridad**	**lun 13/09/21**	**vie 08/04/22**	**149 días**		**310 horas**
3	**Inicio**	**lun 13/09/21**	**lun 13/12/21**	**66 días**		**10 horas**
4	Inicio del Proyecto	lun 13/09/21	lun 13/09/21	0 días		0 horas
5	Registrar OC de Equipos	lun 13/12/21	lun 13/12/21	1 día		2 horas
6	Registrar OC Servicios	vie 12/11/21	mar 16/11/21	3 días		6 horas
7	Realizar Kick Off del Proyecto	vie 26/11/21	vie 26/11/21	1 día		2 horas
8	**Planificación**	**lun 29/11/21**	**lun 29/11/21**	**1 día**		**4 horas**
9	Desarrollar Cronograma del Proyecto	lun 29/11/21	lun 29/11/21	1 día	7	4 horas
10	**Ejecución**	**vie 19/11/21**	**vie 01/04/22**	**96 días**		**288 horas**
11	Llegada de Equipos	vie 19/11/21	vie 19/11/21	0 días		0 horas
12	Adquirir Servicios Locales para Instalación y Configuración	vie 26/11/21	vie 26/11/21	1 día		2 horas
13	**Seguridad Internet**	**mar 23/11/21**	**vie 01/04/22**	**94 días**		**122 horas**
36	**Seguridad LAN**	**mar 15/02/22**	**mar 15/03/22**	**21 días**		**164 horas**
51	**Cierre**	**vie 19/11/21**	**vie 08/04/22**	**100 días**		**8 horas**
52	Certificación Servicios	vie 19/11/21	vie 19/11/21	1 día	6CC	8 horas
53	Fin del Proyecto	vie 08/04/22	vie 08/04/22	0 días	10;13;36	0 horas

Figura 22:Diagrama Gantt: Estructura Macro de la Implementación

Fuente: Elaboración Propia

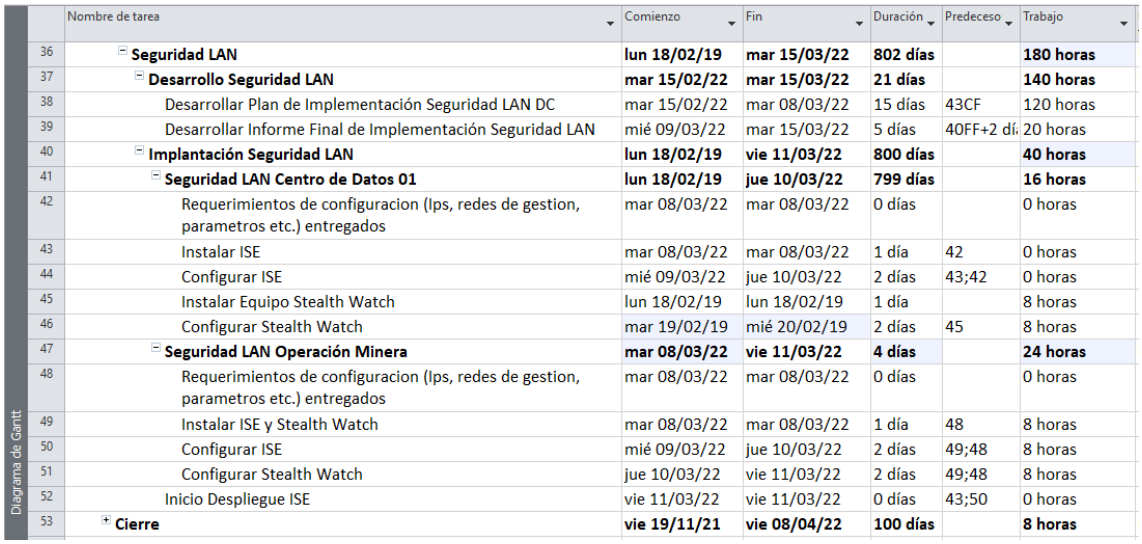


	Nombre de tarea	Comienzo	Fin	Duración	Predeceso	Trabajo
13	**Seguridad Internet**	**mar 23/11/21**	**vie 01/04/22**	**94 días**		**122 horas**
14	**Desarrollo Seguridad Internet**	**vie 25/02/22**	**vie 01/04/22**	**26 días**		**8 horas**
15	Desarrollar/aprobar Plan de Implementación y Migración Segur	vie 25/02/22	mar 22/03/22	17.2 días		0 horas
16	Desarrollar Informe Final Seguridad Internet	jue 31/03/22	vie 01/04/22	2 días	18;27	8 horas
17	**Implantación Seguridad Internet**	**mar 23/11/21**	**jue 31/03/22**	**92 días**		**114 horas**
18	**Seguridad Internet Centro de Datos 01**	**mar 23/11/21**	**jue 17/03/22**	**82 días**		**100 horas**
19	Acondicionamiento Gabinete para Firewall Habilitado	mar 23/11/21	mar 23/11/21	0 días		0 horas
20	Enlace Intenet Principal Habilitado	lun 28/02/22	mar 08/03/22	7 días		0 horas
21	Requerimientos de configuracion (Ips, redes de gestion, parametros etc.) entregados	lun 28/02/22	vie 11/03/22	10 días		80 horas
22	Instalar Firewall	mié 24/11/21	mié 24/11/21	1 día	19	8 horas
23	Configurar Firewalls Internet	lun 14/03/22	lun 14/03/22	1 día	21	0 horas
24	Asistir a Migración Servicio de Internet Tráfico Saliente	mar 15/03/22	mar 15/03/22	1 día	23	6 horas
25	Asistir a Migración Servicio de Internet Tráfico Entrante	mié 16/03/22	mié 16/03/22	1 día	24	6 horas
26	Seguridad Internet Completado	jue 17/03/22	jue 17/03/22	0 días	24;25	0 horas
27	**Seguridad Internet Centro de Datos 02**	**mar 23/11/21**	**jue 31/03/22**	**92 días**		**14 horas**
28	Acondicionamiento Gabinete para Firewall Habilitado	mar 23/11/21	mar 23/11/21	0 días		0 horas
29	Enlace Intenet Principal Habilitado	vie 25/02/22	mar 08/03/22	8 días		0 horas
30	Instalar Firewall	mié 24/11/21	mié 24/11/21	1 día	28	0 horas
31	Requerimientos de configuracion (Ips, redes de gestion, parametros etc.) entregados	lun 28/02/22	vie 11/03/22	10 días		0 horas
32	Configurar Firewalls Internet	lun 28/03/22	lun 28/03/22	0.25 días	31	2 horas
33	Asistir a Migración Servicio de Internet Tráfico Saliente	mar 29/03/22	mar 29/03/22	1 día	32	6 horas
34	Asistir a Migración Servicio de Internet Tráfico Entrante	mié 30/03/22	mié 30/03/22	1 día	33	6 horas
35	Seguridad Internet Completado	jue 31/03/22	jue 31/03/22	0 días	33;34	0 horas

Diagrama de Gantt

Figura 23:Diagrama Gantt: Seguridad Perimetral Internet

Fuente: Elaboración Propia



	Nombre de tarea	Comienzo	Fin	Duración	Predeceso	Trabajo
36	**Seguridad LAN**	**lun 18/02/19**	**mar 15/03/22**	**802 días**		**180 horas**
37	**Desarrollo Seguridad LAN**	**mar 15/02/22**	**mar 15/03/22**	**21 días**		**140 horas**
38	Desarrollar Plan de Implementación Seguridad LAN DC	mar 15/02/22	mar 08/03/22	15 días	43CF	120 horas
39	Desarrollar Informe Final de Implementación Seguridad LAN	mié 09/03/22	mar 15/03/22	5 días	40FF+2 dí	20 horas
40	**Implantación Seguridad LAN**	**lun 18/02/19**	**vie 11/03/22**	**800 días**		**40 horas**
41	**Seguridad LAN Centro de Datos 01**	**lun 18/02/19**	**jue 10/03/22**	**799 días**		**16 horas**
42	Requerimientos de configuracion (Ips, redes de gestion, parametros etc.) entregados	mar 08/03/22	mar 08/03/22	0 días		0 horas
43	Instalar ISE	mar 08/03/22	mar 08/03/22	1 día	42	0 horas
44	Configurar ISE	mié 09/03/22	jue 10/03/22	2 días	43;42	0 horas
45	Instalar Equipo Stealth Watch	lun 18/02/19	lun 18/02/19	1 día		8 horas
46	Configurar Stealth Watch	mar 19/02/19	mié 20/02/19	2 días	45	8 horas
47	**Seguridad LAN Operación Minera**	**mar 08/03/22**	**vie 11/03/22**	**4 días**		**24 horas**
48	Requerimientos de configuracion (Ips, redes de gestion, parametros etc.) entregados	mar 08/03/22	mar 08/03/22	0 días		0 horas
49	Instalar ISE y Stealth Watch	mar 08/03/22	mar 08/03/22	1 día	48	8 horas
50	Configurar ISE	mié 09/03/22	jue 10/03/22	2 días	49;48	8 horas
51	Configurar Stealth Watch	jue 10/03/22	vie 11/03/22	2 días	49;48	8 horas
52	Inicio Despliegue ISE	vie 11/03/22	vie 11/03/22	0 días	43;50	0 horas
53	**Cierre**	**vie 19/11/21**	**vie 08/04/22**	**100 días**		**8 horas**

Diagrama de Gantt

Figura 24:Diagrama Gantt: Seguridad Perimetral LAN

Fuente: Elaboración Propia

4.2.Análisis de Costos

Para analizar el costo del diseño propuesto, se debe tener como premisa que todos los activos de la infraestructura de red actual de la organización sujeto a estudio, son compatibles y no requiere ser reemplazados. Por tanto, nos centraremos únicamente en los componentes de hardware y software de la solución.

4.2.1. Capital Expenditures (CAPEX)

Para determinar el costo de inversión de la solución propuesta, se ha divido en dos tablas el detalle de los componentes de hardware y software que brindaran

la seguridad perimetral de Internet y la seguridad LAN (autenticación y control de acceso). En la Tabla 4. se presenta el hardware, mientras que en la Tabla 5. el software o licencias.

Tabla 4: Lista de componentes de Hardware

COMPONENTE		CANT.
PROTECCION MULTICAPA DE INTERNET - CENTRO DE DATOS 01		
FPR2130-NGFW-K9	Cisco Firepower 2130 NGFW Appliance, 1U, 1 x NetMod Bay	1
PROTECCION MULTICAPA DE INTERNET - CENTRO DE DATOS 02		
FPR2130-NGFW-K9	Cisco Firepower 2130 NGFW Appliance, 1U, 1 x NetMod Bay	1
PROTECCIÓN DE CENTRO DE DATOS 01		
FPR2120-NGFW-K9	Cisco Firepower 2120 NGFW Appliance, 1U	1
PROTECCIÓN DE CENTRO DE DATOS 02		
FPR2120-NGFW-K9	Cisco Firepower 2120 NGFW Appliance, 1U	1
GESTIÓN		
FMC2500-K9	Cisco Firepower Management Center 2500 Chassis	1

Fuente: Elaboración Propia

Tabla 5: Lista de componentes de Software

Componente: Software	CANT.
SEGURIDAD LAN: AUTENTICACIÓN Y CONTROL DE ACCESO	
Licencia Airwatch (VMWARE)	250
Licencia Stealtwatch (flujo de tráfico: 5,000)	1
Licencia ISE	250
Licencia Firewall	4
Licencia VPN	250
Licencia MDM	250
SEGURIDAD INTERNET: PROTECCIÓN MULTICAPA Y CENTRO DE DATOS	
Licencia DUO	250
Licencia AMP	250
Licencia Umbrella	250

Fuente: Elaboración Propia

De la tabla anterior, considerar lo siguiente:

- La licencia Stealtwatch captura el tráfico que generar todos los componentes de red que la empresa, es por ello que su estimación se basa en un flujo de tráfico que para este estudio se consideró de 3,000 (dato brindado por la empresa).
- Cada firewall requiere de una licencia, es por este motivo que se han considerado 04 licencias.
- Para las otras licencias, se considera una licencia por usuario. Para este caso, hemos considerado 250 usuarios, que es la cantidad de colaboradores en planilla de la empresa.

La solución que centraliza la infraestructura de red actual y los nuevos componentes de seguridad es el método SAFE basado en *Defense in Depth*.

La solución de ciberseguridad que proponemos contempla los componentes de seguridad (*hardware y software*) y el método SAFE. Para el cálculo de inversión se consultó a la empresa Telefónica del Perú para que nos brinde los costos aproximados, los cuales presentamos en la Tabla 6

Tabla 6: Cuadro de presupuesto CAPEX

DESCRIPCIÓN	Importe USD
COMPOMENTES: HARDWARE & SOFTWARE	
Software & Hardware (incluye instalación de la solución, soporte del fabricante por 04 años)	$311,500.75
SOLUCIÓN INTEGRADORA	
Método SAFE	$90,123.00
TOTAL CAPEX	$401,623.75

Fuente: Elaboración Propia

De la tabla anterior se determina que el importe de inversión es de $401,623.75, el cual nos servirá para determinar el ROI.

4.2.2. Operacional Expenditures (OPEX)

Consideramos como OPEX al monitoreo y soporte técnico (primer y segundo nivel). En la Tabla 7, presentamos el costo mensual de un ingeniero residente, considerando un contrato a 03 años que es soporte que nos brinda el fabricante. Para determinarlo, consultamos con la empresa Telefónica del Perú.

Tabla 7: Cuadro de presupuesto OPEX

OPEX	Importe USD
Ingeniero residente de Soporte seguridad NAC, Seguridad perimetral y servidores virtuales 7x24. • Soporte y monitoreo del COS. (security operation center)	$4,650.00
TOTAL (Mensual)	**$4,650.00**
TOTAL OPEX (36 meses)	**$167,400**

Fuente: Elaboración Propia

4.2.3. Retorno de inversión (ROI)

Para evaluar si el diseño propuesto es una buena inversión para la empresa, consultamos al Gerente de IT el importe aproximado que perdería la empresa si sus servicios críticos se vieran afectados y tuvieran que detener la operación, nos indicó que la perdida diaria es aproximadamente de USD $1,000,000.

Si el costo total de la solución propuesta es de USD $569,023.75 y asegura la continuidad de la operación. Podemos determinar que es rentable para la empresa debido que la inversión solo representa el 56% de la perdida diaria que tendrían al sufrir un ciberataque.

CONCLUSIONES

1. Este trabajo de investigación se ha elaborado durante el contexto de pandemia por la presencia de COVID -19 que sumado a la innovación tecnológica y el trabajo remoto permitieron incrementar la presencia de vulnerabilidades y amenazas por los ataques de ciberseguridad a través de virus informáticos como: phishing, troyanos, ransomware, y malware. En este punto, la empresa objeto de estudio considera importante generar una cultura de seguridad para todos para cuidar no solo la información de la empresa sino también la personal y busca concientizar la presencia de las amenazas cibernéticas.
2. Durante el proceso de análisis para el diseño de este trabajo de investigación, se identificó que la empresa objeto de estudio requiere reforzar el acceso seguro a la red por parte de sus colaboradores e invitados, mejorar la seguridad perimetral internet y LAN (correo electrónico, navegación a internet, entre otros) e implantar mecanismos de seguridad interna para el acceso a la granja de servidores repartidos en dos centros de datos ubicados en Lima.
3. Este estudio presenta el diseño de un sistema de ciberseguridad basado en Defense in Depth para la empresa objeto de estudio. Esta estrategia basada en un principio de capas permite flexibilizar y customizar la solución para cubrir su necesidad de controlar el acceso a la red interna según perfil, usuario y empresa, entre otros requerimientos como el de considerar la infraestructura de red actual.
4. Un factor clave de éxito para la gestión de la seguridad informática es identificar cuáles son los puntos vulnerables y servicios críticos que presenta la infraestructura de red. Conociendo como se encuentra la red se puede utilizar las tecnologías emergentes a nuestro favor para prevenir y reducir a nulo las vulnerabilidades.
5. Las empresas que son conscientes que mantienen múltiples sistemas, aplicaciones con información sensible para el negocio y presentan hiperconectividad invierten en soluciones de ciberseguridad para incrementar la seguridad de la información. De sufrir algún tipo de pérdida secuestro o daño de la información podría impactar al estado financiero, reputación de la empresa y términos legales como operativos.

RECOMENDACIONES

1. Es importante que toda empresa que busca reforzar su seguridad de la información realice campañas de concientización y sensibilización con el respaldo de la directiva para informar a todos los colaboradores acerca de los controles de acceso y explicarles los diferentes medios por los que pueden ser víctimas de robo de información tanto personal como laboral.
2. Es fundamental que las empresas realicen simulaciones de ciberataques para identificar los activos más vulnerables y qué tipo de conexión tienen para establecer políticas de seguridad, así generar un historial que permitan analizar un caso o identificar compartimientos de accesos foráneos.
3. Se recomienda priorizar la inversión en seguridad de inversión y/o solución de ciberseguridad en los procesos claves del negocio.
4. Al implementar una solución de ciberseguridad, se aconseja documentar correctamente las reglas, políticas y controles de acceso de cada uno de los componentes de seguridad en guías de controles base que permitirá tener una línea base para futuros cambios y se generará así un historial de cambios.

REFERENCIAS BIBLIOGRÁFICAS

Borghello, C. (2009). Crimeware: el crimen del Siglo XXI. Recuperado de: https://www.welivesecurity.com/wpcontent/uploads/2014/01/crimeware_crimen_siglo_xxi.pdf [Consulta: 29, Junio, 2021]

Corletti, A. (2017). Ciberseguridad [Libro en línea]. [Consultado: 28, Junio, 2021] Disponible en: http://www.ieee.es/Galerias/fichero/OtrasPublicaciones/Nacional/2018/Libro-Ciberseguridad_A.Corletti_nov2017.pd.pdf

ELMASRI, R. & NAVATHE, S. (2002) Fundamentals of database systems. 3ra Edición Addison Wesley

ESET (2017, Marzo 22) La economía de la ciberseguridad: cuál es el verdadero valor del antivirus [Consultado: 29, Junio, 2021]
Disponible en: https://www.welivesecurity.com/la-es/2017/03/22/economia-de-la-ciberseguridad/

ESET (2021, Junio 11) ESET Security Report 2021. [Consultado: 29, Junio, 2021] Disponible en: https://www.welivesecurity.com/wp-content/uploads/2021/06/ESET-security-report-LATAM2021.pdf

Gómez, A. (2011). Enciclopedia de la seguridad informática. (2 ed.). RA-MA EDITORIAL. Recuperado de: https://www.ra-ma.es/libro/enciclopedia-de-la-seguridad-informatica-2a-edicion_48115/

Hernandez Sampieri, R; Metodología de la Investigación (4ta ed.). MC Graw Hill.

INCIBE (2020, Octubre 9) ¿Qué son y para qué sirven los SIEM, IDS e IPS [Consultado: 10, Septiembre, 2021] Disponible en: https://www.incibe.es/protege-tu-empresa/blog/son-y-sirven-los-siem-ids-e-ips

KASPERSKY (2021, Julio 10) Trojan-DdoS [Consultado: 08, Septiembre, 2021] Disponible en: https://www.kaspersky.es/resource-center/threats/ddos-attacks

MARSH (2020, Octubre 27) Estado del Riesgo Cibernético en Latinoamérica en tiempos de COVID-19. [Consultado: 29, Junio, 2021] Disponible en: https://coronavirus.marsh.com/mx/es/insights/research-and-briefings/webinar-cyber-risk-in-latin-america-in-times-of-covid19.html

OPTIV; (2020) *A visual history of cybersecurity*. [Consultado: 29, Junio, 2021] Disponible en: https://www.optiv.com/insights/discover/downloads/visual-history-cybersecurity

Romero Castro, M.I.; Introducción a la seguridad informática y el análisis de vulnerabilidades [Libro en línea]. [Consultado: 28, Junio, 2021] Disponible en: https://www.3ciencias.com/wp-content/uploads/2018/10/Seguridad-inform%C3%A1tica.pdf

ANEXOS

Anexo 1: Matriz de Consistencia Interna

TITULO: DISEÑO DE UN SISTEMA DE CIBERSEGURIDAD BASADO EN DEFENSE IN DEPTH PARA PROTECCIÓN DEL SISTEMA DE INFORMACIÓN DE UNA EMPRESA MINERA, 2021				
PROBLEMA GENERAL	OBJETIVO GENERAL	VARIABLES E INDICADORES	POBLACION Y MUESTRA	METODOLOGÍA
¿Cómo diseñar un sistema de ciberseguridad basado en defense in depth para protección del sistema de información de una empresa minera?	Diseñar un sistema de ciberseguridad basado en defense in depth para protección del sistema de información de una empresa minera.	1. Ciberseguridad 2. Sistema de información 3. Defense in depth	Población: Empresa Minera	Tipo: Descriptivo Diseño: Transeccional o transversal
PROBLEMA ESPECIFICO	**OBJETIVO ESPECIFICO**	**VARIABLES E INDICADORES**	**POBLACION Y MUESTRA**	**METODOLOGÍA**
¿Cuáles son los problemas de vulnerabilidad de información que generan la innovación tenológica y el tramajo remoto ?	Identificar los problemas de vulnerabilidad de información que generan la innovación tecnológica y el trabajo remoto.	1. Vulnerabilidad 2. Innovación tecnológica 3. Trabajo remoto	Población: Empresa Minera	Tipo: Descriptivo Diseño: Transeccional o transversal
¿Cuáles son los requerimientos de seguridad de información que tiene la empresa minera?	Evaluar los requerimientos de seguridad de información que la empresa minera presenta.	1. Seguridad de información	Población: Empresa Minera	Tipo: Descriptivo Diseño: Transeccional o transversal

Anexo 2: Matriz de Operacionalización de Variables

VARIABLE	DEFINICION	DIMENSIONES	INDICADORES
Ciberseguridad	La ciberseguridad o seguridad informática es la que se encarga de los distintos métodos, técnicas y procesos que buscan almacenar, distribuir y proteger la información en su versión digital, se puede considerar entonces que la ciberseguridad se encuentra dentro de la seguridad de la información (Romero,2018). Los términos de ciberseguridad y seguridad de la información se diferencian porque la primera incluye también tecnologías o prácticas ofensivas para atacar a sus adversarios, mientras que la segunda solo debe ser usado para aspectos defensivos.	Vulnerabilidades Ataques informaticos o ciber ataques Virus informaticos	Norma Internacional de seguridad de información y metodología PMO
Defense in Depth	Defense in Depth se define simplemente como tener diversos niveles de controles de seguridad en más de una de las 3 áreas fundamentales de seguridad, siendo estas áreas el control administrativo, el control físico y el control técnico. Se trata de un arreglo multicapas en el que si un mecanismo de seguridad falla automáticamente se activa la siguiente capa o protocolo para detener el ataque. Es también conocido comúnmente como "castle approach" pues al igual que un antiguo castillo medieval es necesario sortear diversos obstáculos y/o trampas si es que se quiere entrar en el usando la fuerza.	Información y activos críticos Control de acceso Autenticación	Norma Internacional de seguridad de información y metodología de diseño PMO