"Responsabilidad con pensamiento positivo"

UNIVERSIDAD TECNOLÓGICA ISRAEL

TRABAJO DE TITULACIÓN EN OPCIÓN AL GRADO DE: INGENIERO EN ELECTRÓNICA DIGITAL Y TELECOMUNICACIONES

TEMA:

Implementación de una red LAN con acceso WAN, en la empresa GMS, administrada de acuerdo con la norma establecida por el Instituto SANS - *SysAdmin Audit, Networking and Security Institute*

AUTOR:

YANARA JEZABEL SIMBAÑA SIMBAÑA

TUTORES:

Mg. David Patricio Cando Garzón
Tutor técnico

Mg. Flavio David Morales Arévalo
Tutor Metodológico

QUITO, ECUADOR

2020

CERTIFICACIÓN TUTOR METODOLÓGICO

UNIVERSIDAD TECNOLÓGICA ISRAEL APROBACIÓN DEL TUTOR

En mi calidad de tutor del trabajo de titulación certifico:

Que el trabajo de titulación **"Implementación de una red LAN con acceso WAN, en la empresa GMS, administrada de acuerdo con la norma establecida por el Instituto SANS - SysAdmin Audit, Networking and Security Institute"**, presentado por la **Srta.Yanara Jezabel Simbaña**, estudiante de la carrera de Electrónica Digital y Telecomunicaciones, reúne los requisitos y méritos suficientes para ser sometido a la evaluación del Tribunal de Grado, que se designe, para su correspondiente estudio y calificación.

Quito, febrero del 2020

TUTOR

……..

Mg. Flavio Morales

UNIVERSIDAD TECNOLÓGICA ISRAEL

APROBACIÓN DEL TUTOR TÉCNICO

En mi calidad de tutor del componente práctico certifico:

Que el trabajo de titulación "Implementación de una red LAN con acceso WAN, en la empresa GMS, administrada de acuerdo con la norma establecida por el Instituto SANS - *SysAdmin Audit, Networking and Security Institute*", presentado por la Srta. Yanara Jezabel Simbaña Simbaña, estudiante de la carrera de Electrónica Digital y Telecomunicaciones, reúne los requisitos y méritos suficientes para ser sometido a la evaluación del Tribunal de Grado, que se designe, para su correspondiente estudio y calificación.

Quito, febrero del 2020

TUTOR

……..

Mg. David Cando

AGRADECIMIENTO

Mi agradecimiento a mis padres Nancy y Samuel quienes fueron el pilar fundamental de esta etapa, por haber depositado su confianza, amor y anhelo.

El inmenso agradecimiento a mis segundos padres Laura y Vicente quienes siempre me han cuidado y me han ayudado.

Mi más profundo agradecimiento a mi compañero de vida Carlos por su gran apoyo en las buenas y en las malas, por levantarme y darme ánimos cada día, por enseñarme que nada es imposible.

A mis amigos que han sido como hermanos por los ánimos, risas y llantos en cada día de mi vida estudiantil.

Mi sincero agradecimiento a mis tutores Mg. David Cando y Mg. Flavio Morales por su apoyo, su guía, liderazgo y confianza dentro y fuera de las aulas de clase.

DEDICATORIA

Mi tesis la dedico con todo mi amor y cariño a mis padres por su gran apoyo, paciencia y tolerancia en esta etapa estudiantil, a mis abuelitos quienes fueron un pilar fundamental en mi vida, mi dedicación a mi compañero de vida quien ha sido un apoyo y ayuda incondicional en mi vida universitaria, a mis amigos quienes siempre me brindaron ánimos en todo momento.

TABLA DE CONTENIDO

LISTA DE FIGURAS

LISTA DE TABLAS

LISTA DE ANEXOS

RESUMEN

La seguridad de la información se ha convertido en el tema de moda, sin embargo, poco o nada se ha hablado de cómo iniciar la incorporación de los conceptos asociados desde la fase de diseño de las redes. Los especialistas actuales en este campo han sido formados de manera empírica, por la necesidad del mercado laboral, la exigencia de las empresas y la operación de estas.

La necesidad de evaluar los métodos de diseño se convierte en algo crucial, se evalúa un antes y un después de las redes diseñadas con base en seguridades y las que antes no consideraban esto.

En este proyecto de titulación, se plantea una alternativa de como cruzar la experiencia de miles de profesionales en seguridad de la información con la metodología de diseño de redes basada en capas, se utilizan los controles críticos listados por el instituto SANS y los sub-controles que permiten evaluar el cumplimiento de las recomendaciones y se demuestra, que al final se podrá tener una red funcional y segura.

La aplicabilidad de lo descrito se mide en la implementación de la red con esas consideraciones y como resultado, esto es efectivo y eficiente.

Al no tener una red segura, se consideran que las pérdidas ascenderían a miles o millones de dólares por entidad, a causa del cibercrimen que se detecta en promedio en una sola empresa.

Palabras clave: *redes seguras, diseño de redes con seguridad, CIS, SANS, controles de seguridad, subcontroles de seguridad.*

ABSTRACT

Information security has become the hot topic, however, little or nothing has become how to activate the conversion of the associated concepts from the design phase of the networks. Current specialists in this field have been empirically trained, due to the need of the labor market, the requirement of companies and their operation.

The need to evaluate design methods becomes crucial, a before and after of the changed networks based on securities and those that are not considered this is evaluated.

In this degree project, an alternative of how to cross the experience of miles of professionals in information security with the layer-based network design methodology is proposed, the critical controls listed by the SANS Institute and the sub-controls are required which allows to evaluate compliance with the recommendations and it is demonstrated that in the end you can have a functional and secure network.

The applicability of the described is measured in the implementation of the network with these considerations and as a result, this is effective and efficient.

Not having a secure network, losses amounting to miles or millions of dollars per entity will be considered, a cause of cybercrime that will be detected on average in a single company.

Keywords: *secure networks, secure network design, CIS, SANS, security controls, security sub-controls.*

INTRODUCCIÓN

ANTECEDENTES DE LA SITUACIÓN OBJETO DE ESTUDIO

Actualmente el avance tecnológico y la dependencia de los seres humanos de dispositivos que almacenen, procesen y compartan información se ha hecho habitual, en tareas comunes de la vida cotidiana como citas, agenda, conversaciones telefónicas, enviar mensajes o cartas que hoy día son electrónicas a través de e-mail, hasta tareas mucho más avanzadas como manejar la inteligencia de negocios de una empresa, guardar estadísticas de ventas, compras, comportamiento de usuarios, tendencias y demás, incluso la operación misma de muchas empresas es completamente digital y dependiente de equipos electrónicos capaces de interactuar entre ellos y ofrecer información procesada a los usuarios a través de enormes redes de datos, privadas de cada empresa, colaborativas entre dos o más empresas que comparten información ya sea por alianzas, ser clientes, proveedores o simplemente por poseer datos de interés.

La aparición de computadoras despertó el deseo de hablar de ellas y con ellas hablar cerca de personas y sitios web remotos, lo que dio origen a redes, clasificadas por su ubicación de operación, por ejemplo, redes de área local o generalmente llamadas redes LAN por sus siglas en inglés (*Local Area Network*), que protegen hogares, oficinas y edificios. Redes de lugares extendidos que podrían abarcar ciudades, naciones o incluso continentes, que se llaman redes WAN por sus siglas en inglés (*Wide Área Network*). Actualmente la interconexión más grande entre redes se conoce como INTERNET, lo cual es una de las más grandes fuentes de datos en el mundo.

De forma sencilla, rápida y a costos relativamente accesibles, un usuario o empresa puede conectarse a internet para aprovechar los beneficios de la globalización, leer, procesar, modificar, crear, eliminar y consumir los datos que otros usuarios o empresas ponen a disponibilidad de cualquiera o de grupos exclusivos o seleccionados.

Sin embargo, todas las posibilidades descritas añadieron riesgos inherentes a la existencia misma de redes, computadoras y las estadísticas que se comparten, guardan y procesan en ellos. Para este propósito, se requieren más y más expertos especializados en áreas muy precisas de información de tecnologías que son parte de las redes y que son

beneficiosas dentro de la seguridad de las redes mismas, además de los datos.

Algunas tesis se han escrito con diseños que señalan problemas de seguridad, tienen en cuenta la autenticación de usuarios y dispositivos o diseños jerárquicos, sin embargo, son bastante precisos u observan una versión comercial de los líderes dentro de la empresa de fabricación de equipos de comunicaciones y telecomunicaciones.

El instituto SANS - *SysAdmin Audit, Networking and Security Institute*, fundado con fines de lucro y cuyo objetivo ha sido reunir información sobre la seguridad de redes, equipos de comunicación como *routers*, switch, firewalls, aplicaciones, bases de datos, etc, ha desarrollado recomendaciones sobre 20 controles mínimos necesarios para administrar una red que ofrezca disponibilidad, integridad y confiabilidad en los datos que circulan, se almacenan y procesan.

Al no existir de forma nativa correlación directa en la metodología de diseño de redes y estos 20 controles mínimos se considera necesario investigar y desarrollar la metodología de diseño con esta consideración, implementar una red cuyas bases y consideraciones, estimaciones y cálculos se realicen con estos controles.

PLANTEAMIENTO Y JUSTIFICACIÓN DEL PROBLEMA

Por la cantidad de información que se encuentra disponible en las redes, la cantidad de usuarios y equipos que forman parte de estas y la creciente exponencial de nuevas tecnologías que se han desarrollado, los administradores y usuarios han encontrado ciertos inconvenientes.

Uno de los inconvenientes más comunes es que los administradores de red no disponen de inventarios actualizados, reales y en tiempo real de los equipos en las redes que ellos controlan, el *software*, procesos, servicios, vulnerabilidades, accesos o incluso registros para investigación de acciones realizadas con los equipos o la información.

Los diseños consideran la segmentación de las redes con VLAN, o redes virtuales que mantienen cierta información separada de usuarios que no deben tener acceso, sin embargo, no se consideran casos específicos de uso, puertos, protocolos, aplicaciones, tecnologías en

sí, sino que se permite o se deniega todo o ningún tráfico de red. Por lo que segmentar esto, en la actualidad se vuelve crucial.

Lo propio ocurre con la seguridad, no siempre conocen el software existente, el uso que los consumidores dan a los datos, a los recursos de red, a las comunicaciones propiamente, de modo que establecer puntos de vigilancia o tomar decisiones en tareas simples como ampliar la capacidad de los canales para mejorar la productividad o implementar soluciones software, hardware e incluso servicios nuevos se vuelve algo netamente intuitivo y dependiente del criterio de los administradores pero no sigue un lineamiento bien definido que garantice que con base en datos estadísticos de esa red, la decisión tomada permita alcanzar los objetivos planteados o tan solo no afecte a la operación o producción actual, muy pocas veces se considera el triángulo de la seguridad conformado en sus vértices por la disponibilidad, integridad y confiabilidad de la información.

Más de 375.000 especialistas en todas las áreas que comprenden las telecomunicaciones plantearon sus problemas y puntos de vista para solventarlos, de este modo, creados los 20 controles críticos, muchos administradores tratan de apegarse a ellos, lamentablemente encuentran dificultad al no encontrar referencias o metodologías de diseño y sobre todo de implementación de redes que engranen a estos controles.

Es entonces necesario investigar, diseñar e implementar una red que considere estos controles, se afianza así un precedente metodológico aplicable a cualquier realidad de negocio, empresa o red, indiferente de su uso, vertical de negocio o tamaño. Así como agnóstica a la marca o modelo de equipos a emplear.

OBJETIVO GENERAL:

- Implementar una red LAN con acceso WAN, en la empresa GMS, administrada de acuerdo con los 20 controles establecidos por el Instituto SANS - *SysAdmin Audit, Networking and Security Institute.*

OBJETIVOS ESPECÍFICOS:

- Definir las diferentes metodologías de diseño de redes y los controles críticos de seguridad establecidos por el instituto SANS para la administración, gestión de una red considerada como segura.
- Implementar la red diseñada.
- Analizar los resultados y establecer un resumen crítico de resultados y factibilidad de estandarización de la metodología particular empleada.

ALCANCE

El diseño cubrirá las capas de la 2 a la 7, tiene como referencia el modelo de capas de la ISO-OSI. Se añade para ciertos puntos al usuario como una capa 8, lo cual en la actualidad se ha convertido en un estándar de facto, considerar una nueva capa, que es el usuario final.

Implementar una red en la empresa GMS – Grupo Microsistemas Jovichsa S.A. que haya sido diseñada durante el desarrollo del presente trabajo de titulación, considera todo lo necesario a nivel de configuraciones, software y hardware con el objetivo de que los controles establecidos por el Instituto SANS sean aplicados para la administración y mejora continua.

Para la implementación se considerará como entregables:
- Cronograma.
- Alcance especifico detallado.
- Diagrama de red con el diseño.
- Informe que incluya VLAN, *Networking*, detalle de equipos y sus capacidades, canales, etc.
- Capturas y copias de las configuraciones de *switches* con detalles específicos de redes,

VLAN, puertos, asignaciones, etc, con información de las rutas, accesos, configuraciones generales, firewalls, así como excepciones, SIEM, inventarios, monitoreo y demás elementos que sean necesarios para cumplir los objetivos planteados. Por seguridad y confidencialidad las direcciones IP, VLAN, puertos pueden ser visibles en este documento.

Establecer mediante este ejercicio un precedente que permita adaptar este diseño a diferentes redes y escenarios, de mayor o menor tamaño, con más o menos servicios, siempre con cuidado en el mapeo o correlación a los controles de seguridad y recomendaciones.

DESCRIPCIÓN DE LOS CAPÍTULOS

Capítulo 1

Para tener la confiabilidad, velocidad y conectividad debe cumplir con controles de seguridad con ciertos requisitos para la red, esta debe ser escalable, adaptable y de fácil administración.

Para esto se considera la clasificación de las redes según la forma de establecer la comunicación, arquitectura de red, topología y los modelos de referencia OSI y modelo TCP/IP.

Adicional, se considera los servicios que la red presenta en las cuales los usuarios a menudo utilizan archivos compartidos, el uso diario de correo electrónico, el almacenamiento de datos y para esto todas las aplicaciones que hacen esto posible.

De esta manera se hace uso de controles de seguridad que se consideran como críticos por el instituto SANS.

El modelo debe ser jerárquico para ofrecer escalabilidad y considera las siguientes tres capas: capa de acceso, capa de distribución y núcleo, en la empresa por el tamaño se fusiona la capa de distribución y núcleo de acuerdo con recomendaciones de Cisco para estos ambientes.

Este diseño cuenta con la parte de acceso separada e independiente de fácil escalabilidad.

Capítulo 2

Los marcos metodológicos de investigación y técnicas para la recolección de la información se realizarán en campo, de la metodología a emplear y los controles de seguridad establecida, estos basados en entrevistas al personal de infraestructura de la empresa GMS, se documentará la información provista por el personal encargado, así como las expectativas a las cuales se debe alcanzar.

Los datos a ser procesados serán de forma manual con indicadores que permitan realizar el diseño adecuado y la toma de decisiones o evaluación de los puntos a tratar, se tendrá la calificación establecida por el instituto SANS con 6 puntos del 0 al 5, en el caso de no aplicar se aumentará un punto más como 6, de esta manera entregará un informe del nivel de madurez y esta será evaluado con los controles que establece el instituto SANS, se espera tener una red madura en seguridad y funcional a todo nivel en las capas desde la 2 hasta la capa 7 del modelo OSI para redes LAN y WAN.

La selección de controles aplicados a la empresa y un oficial de seguridad quien será una persona de la organización responsable de velar que los temas de seguridad sean cumplidos al momento de realizar una auditoría interna y externa de ser necesario para evidenciar la implementación y que estos se mantengan con los controles detallados en la investigación.

Capítulo 3

Para el diseño de la red debe considerarse de forma tradicional, basada en la topología deseada, el número de nodos y empleados, el número de subredes y VLAN, así como también los dispositivos y servicios que serán puestos al servicio de los consumidores y clientes de la red. Para este caso se considera los nuevos requisitos que proporciona la empresa auspiciante que se listan a continuación:

- Servicios de autenticación
- Servicios de almacenamiento y colaboración de archivos compartidos
- Software y hardware de seguridad ante ataques informáticos
- CRM o sistema de manejo y relacionamiento de clientes
- Software de ofimática y soporte de oficina
- Servicio de internet, aplicaciones y bases de datos
- Servicios de red a través de red cableada
- Cumplimiento de controles de seguridad acorde a recomendaciones del instituto SANS
- Se considerará para el diseño jerárquico, 2 capas, con la capa de núcleo y distribución fusionadas descrito con anterioridad.
- La implementación será realizada después de la obra civil, el sitio actual no se reutilizará.

El diseño partirá desde cero, sin embargo, se considerará los equipos existentes, en caso de poderse reutilizar.

Para llevar a cabo los controles y puesta en producción se requiere de lo siguiente:

- Grupo de monitoreo
- Grupo de operación
- Conectividad
- Borde
- Centro de datos
- DMZ: Se destinará esta sección a los servidores de operación que mantendrán los procesos importantes de negocio activos.

Entre ellos se tendrá:

- Servidor de autenticación
- Servidores de archivos
- Servicios Web
- Bases de datos
- Seguridad y apoyo: Este grupo de servidores tendrán el software y hardware virtual de apoyo para seguridad y cumplimiento de los controles

Análisis de controles con el diseño propuesto

Se realiza la revisión de los controles propuestos y se diseña el proyecto con alcance que incluye, productos o servicios, documentación, normativa, seguimiento, indicadores y como realizar una mejora continua.

Capítulo 4

Se documenta como se encuentra la red diseñada con los controles de seguridad que ha sido implementada, finalmente, se ha considerado 27 proyectos en total, que conllevan la implementación de soluciones y servicios acorde a las necesidades, mismas que han sido vistas en la propuesta, estos 27 proyectos cubren 19 de los 20 controles existentes y se elimina el control de 15, referente a seguridad de redes Wireless o comunicaciones inalámbricas, ya que no se provee este servicio en la red.

Cabe indicar que no se consideraron para la implementación todos los controles con un proyecto independiente ya que varios controles pueden ser atacados con un proyecto, porque muchas soluciones comerciales tratan de abarcar varias brechas de seguridad, así como un control puede requerir más de un proyecto por los diversos subcontroles que tiene.

Los siguientes servicios han sido considerados de forma recurrente para cumplir con los

controles, subcontroles y tener una red madura respecto a seguridad informática y garantizar disponibilidad, confiabilidad y confidencialidad de los datos.

Mediante servicios de respuesta a incidentes, se ha establecido lo necesario para la preparación antes de que ocurran incidentes de seguridad de la información o ataques. Para establecer los puntos que entregarán información para las investigaciones, para esto se debe considerar los elementos implementados como productos ya que se deben realizar trabajos sobre estos elementos. Posterior estos servicios permitirán contener, mitigar y erradicar cualquier amenaza de una forma rápida y que constituya el menor impacto posible a la operación.

Debe considerarse al menos los mayores tipos de ataques informáticos de los que son víctimas las organizaciones hoy en día.

CAPÍTULO 1.

FUNDAMENTACIÓN TEÓRICA

1.1 Diseño de redes

El diseño para implementar va de acuerdo con los problemas actuales de comunicación que tiene la empresa, para esto la red debe permitir que los usuarios cumplan con sus requisitos laborales, debe suministrar conectividad de usuario a usuario y de usuario a aplicación con una velocidad y confiabilidad razonable.

Para el diseño debe cumplir con ciertos requisitos:

- Esta red debe ser escalable es decir aumentar de tamaño sin que se hagan cambios importantes en el diseño general.
- La red debe ser adaptable, se considera futuras tecnologías, sin limitar nuevas tecnologías.
- Debe ser fácil de administrar para facilitar su administración y monitoreo, se debe asegurar estabilidad en el funcionamiento.

1.2 Clasificación de las redes según la forma de establecer la comunicación

Frecuentemente, las redes de área extendida WAN, proporcionan medios de transmisión a largas distancias y se extienden geográficamente por muchos o miles de kms. Estas se pueden clasificar en función de la forma en que se establece la comunicación en redes de dos tipos: redes de conmutación de circuitos y redes de conmutación de paquetes. Habitualmente las redes WAN conmutadas conectan redes LAN entre sí mediante dispositivos enrutadores.

Arquitectura de red: se puede definir como el conjunto de capas y protocolos que constituyen un sistema de comunicaciones. Cada capa o nivel es un consumidor de servicios ofrecidos mediante un conjunto de entidades.

1.3 Modelo de referencia OSI

Normativa internacional de la ISO. Compuesto de 7 capas, es un modelo para interconectar sistemas abiertos (OSI). Entre sus principales características:

- Está estructurado en 7 capas
- Utiliza protocolos normalizados internacionalmente
- Indica lo que cada capa debe hacer.

La figura 1.1 indica las 7 capas del modelo OSI

Figura 1.1. Modelo ISO/OSI de 7 capas.

Fuente: (Modelo OSI, 2019)

1.4 Modelo de referencia TCP/IP

Constituye actualmente la arquitectura de red más empleada en cualquier sistema de comunicaciones que requiera interconexión entre sistemas diversos. Conformado por 4 capas, como se aprecia en la figura 1.2.

Figura. 1.2. Modelo TCP/IP de 4 capas.

Fuente: (Modelo OSI, 2020)

1.5 Manejo de la topología

Física de la red, se considerará el manejo de la topología, tener presente las necesidades del administrador y requerimientos de las aplicaciones atados a los controles de seguridad que se pretende vincular con el proceso de diseño.

La topología física de una red es la disposición geométrica real de las estaciones de trabajo.

Según sea la distribución que se tenga pensada para el diseño de una red, se utilizada un tipo de topología específica.

Entre las principales topologías de red se tienen las siguientes:

1.5.1 Topología en anillo

Red más simple, donde los nodos se encuentran conectados como si fuera un anillo, estos forman un círculo entre ellos, así la información va en un sentido, teniendo como desventaja en el caso de tener un nodo fallido, se cae la red y deja de pasar la información por lo que esta topología es poco eficaz. (Rodríguez, 2017).

1.5.2 Topología de Árbol

Esta topología es más sencilla, las conexiones entre las estaciones de trabajo están en forma de árbol, se tiene similitud en tener una punta y una base, muy similar a la topología estrella y se basada en la topología de bus, si un nodo falla, no hay mucho impacto, pues entre los nodos tienen un cable principal llamado *backbone* (como redundancia) así lleva la información al resto de nodos y comparte un mismo canal de comunicación. Es más eficaz evitando la caída total de la red. (Rodríguez, 2017).

1.5.3 Topología de Bus

Basada en un cable central, este cable lleva la información a todas las estaciones de trabajo de la red en forma de ramificaciones, así la información va en secuencia hacia los nodos, la desventaja de esta topología es la distribución secuencial de los datos, si el cable se interrumpe, la red queda inutilizada, es poco útil actualmente. (Rodríguez, 2017).

1.5.4 Topología de Estrella.

Actualmente es muy utilizada ya que es muy eficiente, la información va desde el punto central hacia todos los nodos de la red, es como una especie de servidor local que administra los servicios compartidos y la información, así si un nodo falla, la red continua operando, en ciertas ocasiones también puede depender del funcionamiento del host. Es más eficaz ya que su principal ventaja es operar a pesar de fallas en los nodos. (Rodríguez, 2017).

1.5.5 Topología de Malla.

Denominada también como topología de trama. Estos se encuentran conectados entre sí, es un arreglo de interconexiones de nodos entre ellos. Es una topología muy utilizada entre las redes WAN. La información puede ir por diferentes caminos, si llega a fallar un nodo la operación sigue con normalidad.

En esta topología al tener todos los nodos conectados en malla permite transmitir la información por diferentes caminos de un nodo a otro, de esta manera se diferencia de las otras topologías al no necesitar de un servidor o nodo central como las topologías de árbol y estrella descritas anteriormente. (Rodríguez, 2017).

1.5.6 Topología Híbrida.

Es una combinación de dos o más topologías distintas, combina diferentes topologías y es una de las más utilizadas, esto con el fin de adaptarse a las necesidades del cliente, y brindar la conectividad de sus equipos, combina las topologías que desea, las cuales, deben ajustarse a la estructura física del lugar en donde estará la red y los equipos que se conectarán.

Esta topología es más confiable al combinar y permitir conexión y la transferencia de información a todos los nodos. (Rodríguez, 2017).

"Todos estos conceptos, ligados al funcionamiento de las redes, se los considerará dentro de los riesgos que son sobrellevados con los controles que la SANS y la experiencia que sus investigadores han propuesto". (Rodríguez, 2017).

"Además, se considera los diversos servicios que la red prestará a sus usuarios como el almacenamiento de datos, la compartición de archivos, correos electrónicos y las tecnologías que hacen esto posible". (Rodríguez, 2017).

Es necesario comprender que el proceso de diseño será modificado, esto acorde a los siguientes controles de seguridad que se consideran como críticos por el instituto SANS, el listado se muestra en la tabla 1.1:

Tabla. 1.1. Listado de controles de seguridad

Número	CONTROL
Control 1	Inventario de dispositivos autorizados y no autorizados
Control 2	Inventario de software autorizado y no autorizado
Control 3	Configuraciones de seguridad de hardware y software
Control 4	Evaluación continua de vulnerabilidades y remediación
Control 5	Uso controlado de privilegios administrativos
Control 6	Mantenimiento, monitoreo y análisis de auditoria de logs
Control 7	Protección de *email* y *web browser*
Control 8	Defensa de *malware*
Control 9	Limitación y control de puertos de red
Control 10	Capacidad de recuperación de datos
Control 11	Configuración de seguridad para dispositivos de red
Control 12	Defensa perimetral
Control 13	Protección de datos
Control 14	Control de acceso basado en la "necesidad de saber"
Control 15	Control de acceso *Wireless*
Control 16	Monitoreo y control de cuentas
Control 17	Evaluación de habilidades de seguridad y capacitación apropiada para llenar vacíos
Control 18	Seguridad de software de aplicaciones
Control 19	Gestión y respuesta a incidentes
Control 20	*Penetration tests* y ejercicios del equipo rojo

Fuente: (CERT-PY, 2014)

El diseño debe realizar de manera jerárquica, de tal forma que se cubra desde la capa más baja hasta el núcleo de la red como se indica en la figura 1.3.

Una red LAN jerárquica debe considerar las siguientes tres capas:

- Acceso: ofrece a los nodos y usuarios acceso directo de conexión a la red.
- Distribución: une las capas de acceso y ofrece conexión a los servicios.
- Núcleo: brinda conectividad entre las capas de distribución.

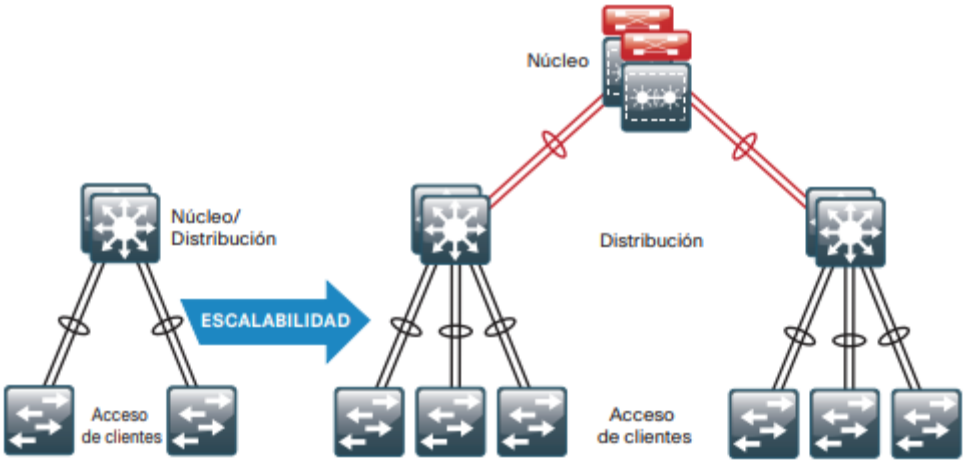


Figura. 1.3. Modelo de referencia que ofrece escalabilidad en un diseño jerárquico.

Fuente: (Cisco, 2014)

En la parte inferior la figura 1.4., considera como clientes a los usuarios o dispositivos de punto final.

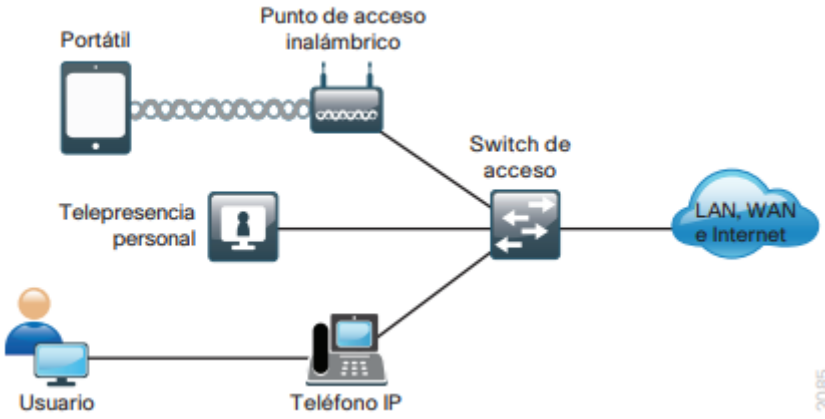


Figura. 1.4. Equipos de punto final que acceden a la red, a través de la capa de acceso.

Fuente: (Cisco, 2014)

Por las exigencias y el tamaño de la empresa GMS, se ha considerado fusionar la capa

de distribución y núcleo, acorde a una recomendación de Cisco para estos ambientes.

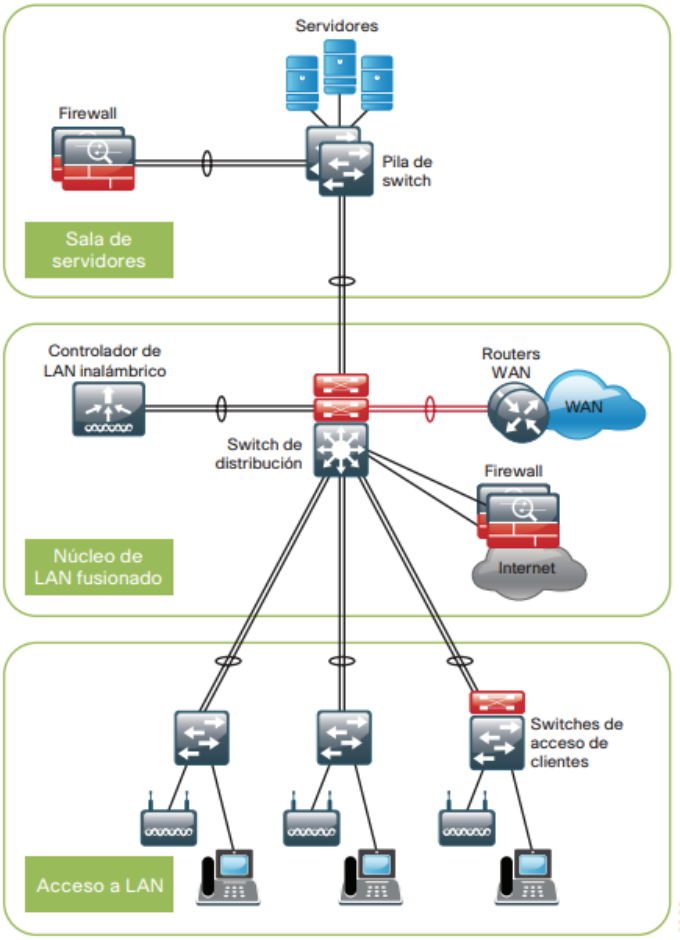


Figura. 1.5. Diseño en dos capas, con fusión de la capa de núcleo y distribución.

Fuente: (Cisco, 2014)

De acuerdo a lo que se muestra en la figura 1.5, este diseño permite contar con la parte de acceso separada, independiente y de fácil escalabilidad a la vez que se concentra la operación del núcleo y la distribución, reduce en número de elementos de red, para empresas pequeñas y medianas, sin perder control de comunicaciones, segmentación de redes, subredes, VLAN y uso de elementos de seguridad como cortafuegos o firewall, así como controladores de red inalámbrica administrados desde el punto de distribución en arreglos de varios puntos de acceso o AP, también mantiene independiente la parte de servidores, o redes que deban estar aisladas completamente ya sea por seguridad, funcionalidad o cumplimiento normativo. (SANS, 2017).

Para el diseño y conocimiento de la red se considera los siguientes conceptos:

- Red LAN: se denomina red de área local, con un alcance pequeño y muy común en edificios o departamentos, permite conexión de nodos y los usuarios pueden

compartir datos, archivos e incluso hacer uso de impresoras.

- Red WAN: con alta velocidad y gran cobertura geográfica, utiliza como medio de conexión fibra óptica y permite la conexión de dos nodos como si fueran parte de la misma LAN, su función es proporcionar el servicio de conmutación para transmitir los datos hasta alcanzar su destino.
- SWITCH DE ACCESO: facilitan la conexión de los dispositivos de nodo final a la red, los conmutadores de capa de acceso se conectan a los conmutadores de capa de distribución, estos implementan tecnologías de *routing*, calidad de servicio y seguridad.
- "SWITCH DE DISTRIBUCIÓN: brinda funciones de *switching*, *routing* y acceso a la red para que pueda conectarse el resto, otorga alta disponibilidad al usuario final ya que mediante conmutadores da redundancia y rutas de igual costo al núcleo. (Diseño de la LAN, 2020)
- "DMZ: Zona desmilitarizada situada entre la red interna y la red externa permite evitar problemas existentes para ejecutar programas o acceder a servicios puntuales desde el exterior. (Crespo, 2017)

- Servicios CSIRT: hace uso de servicios de respuesta a incidentes, están listos para dar respuesta a lo necesario para la preparación antes que ocurra el incidente de seguridad o ataques. Por esta razón se considera los elementos implementados como productos ya que se realiza trabajo bajo estos elementos. Posterior estos servicios permitirán contener, mitigar y erradicar cualquier amenaza de una forma rápida y que constituya el menor impacto posible a la operación. (IS IT SKULL, 2019).

CAPÍTULO 2.

MARCO METODOLÓGICO

Enfoque metodológico de la investigación: Es mixto, ya que se realizará una implementación en campo que abarca los conocimientos adquiridos durante la etapa de estudio, la etapa de investigación de la metodología a emplear y de los controles de seguridad establecidos.

2.1 Métodos empíricos y técnicas empleadas para la recolección de la información:

La metodología empleada para la recolección de información será basada en entrevistas con el personal de infraestructura de la empresa GMS, se documentará también la información más relevante provista por el coordinador del área de monitoreo, acorde al alcance planteado y las expectativas de los involucrados.

2.2 Formas de procesamiento de la información obtenida de la aplicación de los métodos y técnicas:

Los datos se procesarán de forma manual mediante la alimentación a matrices de datos con indicadores que entreguen información para el diseño, toma de decisión o evaluación de los puntos a tratar, también se realizará la aplicación de la metodología de calificación establecida por el instituto SANS, que establece un sistema de 6 puntos, comprende valores entre 0 y 5 puntos de la siguiente forma, considera adicional el valor 6, cuando no aplica a GMS el control establecido:

- No existente
- Inicial
- Repetible
- Definido
- Gestionado
- Optimizado

- No aplicable

Esto finalmente entregará un informe del nivel de madurez en lo relativo a la seguridad de la información que se tendrá en la red diseñada e implementada.

2.3 Metodología seleccionada:

Se hará uso de la metodología de evaluación de nivel de madurez que se establece en los controles del instituto SANS, de tal forma que la red será evaluada y calificada como se describe en el párrafo anterior, debe dar como resultado una red madura en seguridad y funcional a todo nivel en las capas que el diseño considera desde la capa 2 que es de acceso a la red hasta la capa 7 que es de aplicaciones, según el modelo ISO-OSI de equipos para redes de datos tanto LAN como WAN.

Para adecuar el diseño de red a lo establecido como parte de este trabajo de titulación se considera:

- 20 controles críticos de seguridad
- 150 subcontroles asociados a los 20 controles críticos de seguridad
- 7 atributos que debe tener cada subcontrol para ser considerado como aplicado
- 7 calificaciones a cada uno de los 6 atributos con un porcentaje de peso en la evaluación definido previamente

En la figura 2.1 se indica el *Framework* (Marco de referencia) para el diseño con la metodología seleccionada:

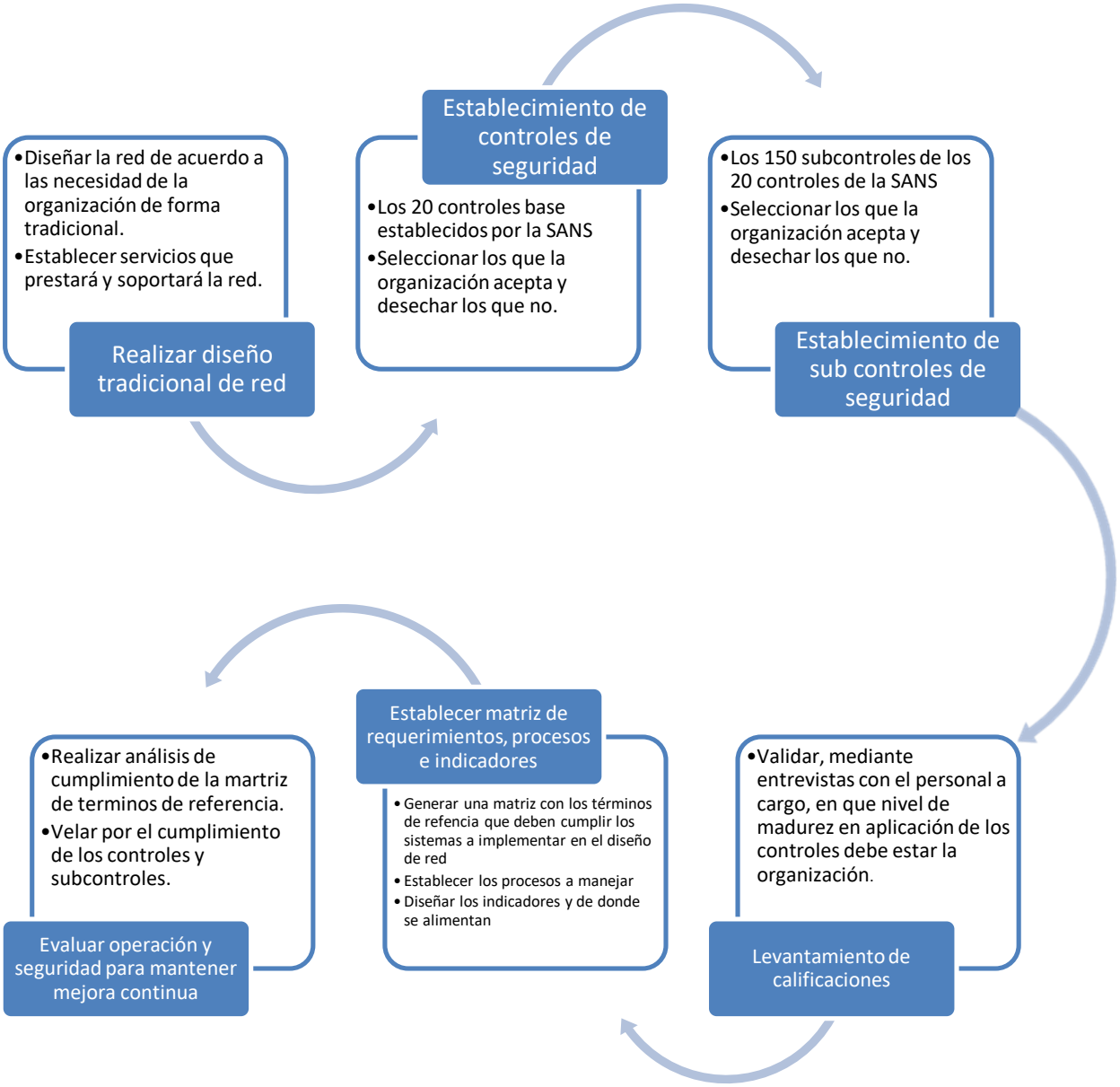


Figura.2.1 Marco de referencia

Fuente: Elaborado por el autor

2.4 Selección de controles aplicables a la empresa:

Antes de avanzar en el paso dos del *framework* de diseño que considera los controles propuestos, se debe considerar que en el diseño es prácticamente obligatorio que participe una persona de la organización con el rol de "OFICIAL DE SEGURIDAD"

Esta persona será la responsable de velar que los temas de seguridad sean cumplidos y

de acompañar a las empresas en auditorías internas y externas en donde sea necesario demostrar ya sea con evidencias o entrevistas como se implementó y mantener el modelo con los controles propuestos.

"Con esto se refuerza la teoría de que los riesgos asociados a los diseños que no consideran seguridad son demasiado altos y pueden poner en riesgo a los usuarios, la información e incluso la operación misma de las empresas". (Gallardo, 2017).

"Para esto, se emplea un estándar de facto en la industria de seguridad, conocido como el equipo azul y el equipo rojo, el equipo azul es el encargado de defender los activos y la información y el equipo rojo, es quien ataca, intenta vulnerar la seguridad a fin de descubrir las brechas en ejercicios controlados y cubrirlas antes que un externo o interno mal intencionado lo haga". (Gallardo, 2017).

Tras socializar los controles, se debe validar si la organización acepta implementar y cuáles no, debidamente justificados, esto se lo debe realizar mediante entrevista con el encargado del área, como responsable de la funcionalidad de operación. (Gallardo, 2017).

Levantamiento de calificaciones

Validar, mediante entrevistas que se muestran con el análisis de los subcontroles y controles, en qué nivel de madurez en aplicación de los controles debe estar la organización.

CAPÍTULO 3.

PROPUESTA

Para dar una propuesta se realiza primero un análisis de situación inicial con los productos, infraestructura, servicios y equipos que se tenía en la red antigua.

Levantamiento de información:

- 4 puestos de trabajo.
- 0 VLAN separadas e independientes.
- 0 DMZ
- Sin subred para servidores de apoyo, seguridad y cumplimiento de controles de seguridad
- Sin subred de pruebas completamente aislada.
- No se tiene alta disponibilidad en los elementos de red, comunicaciones y seguridad.
- Sin cumplimiento de los controles críticos recomendados por el instituto SANS
- Procedimientos base para inicio de operaciones.

Para la empresa GMS se pone a consideración la siguiente propuesta de diseño de red y de equipos, procedimientos y controles para el cumplimiento del *framework* propuesto:

3.1 Diseño tradicional de la red:

Para el diseño de la red debe considerarse de forma tradicional, basada en la topología deseada, el número de nodos y empleados, el número de subredes y VLAN, así como también los dispositivos y servicios que serán puestos al servicio de los consumidores y clientes de la red. Para este caso se considera los nuevos requisitos que proporciona la empresa auspiciante que se listan a continuación:

- Servicios de autenticación
- Servicios de almacenamiento y colaboración de archivos compartidos
- Software y hardware de seguridad ante ataques informáticos
- CRM o sistema de manejo y relacionamiento de clientes
- Software de ofimática y soporte de oficina

- Servicio de internet, aplicaciones y bases de datos
- Servicios de red a través de red cableada
- Cumplimiento de controles de seguridad acorde a recomendaciones del instituto SANS
- Se considerará para el diseño jerárquico, 2 capas, con la capa de núcleo y distribución fusionadas descrito con anterioridad.
- La implementación será realizada después de la obra civil, el sitio actual no se reutilizará.
- El diseño partirá desde cero, sin embargo, se considerará los equipos existentes, en caso de poderse reutilizar.

3.2 Establecer matriz de requerimientos, proyectos e indicadores

- Generar una matriz con los términos de referencia que deben cumplir los sistemas a implementar en el diseño de red
- Establecer los procesos a manejar
- Diseñar los indicadores y de donde se alimentan

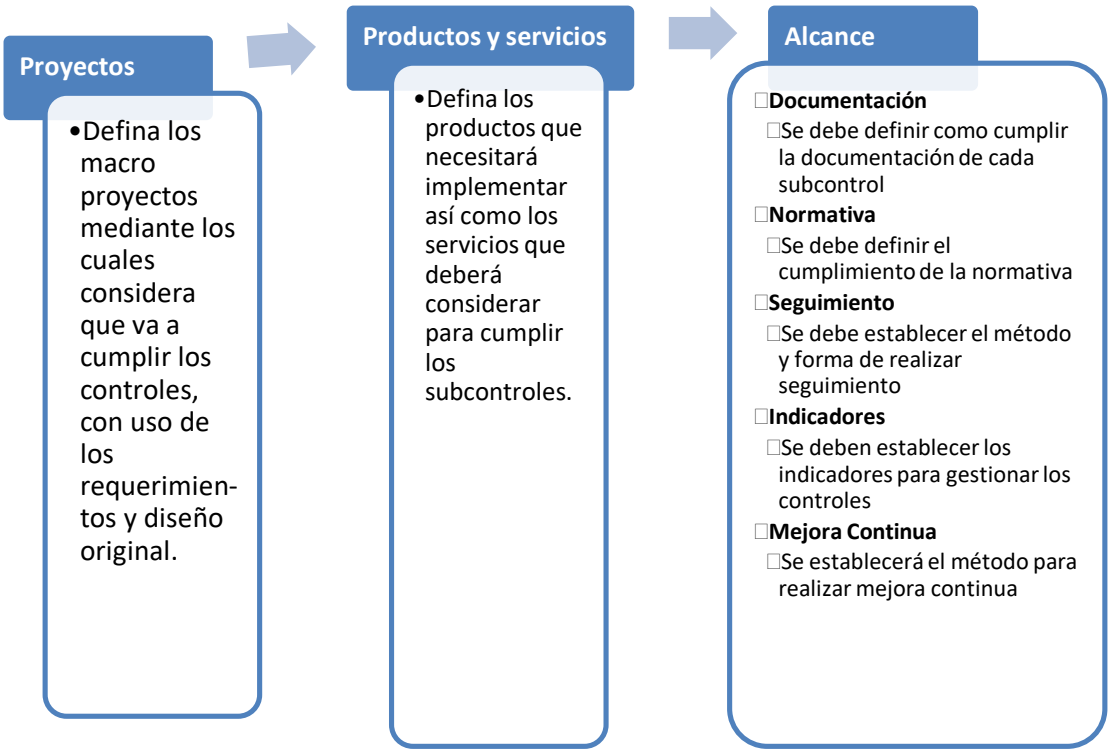


Figura. 3.1. Matriz

Fuente: Elaborado por el autor

3.3 Evaluar operación y seguridad para mantener mejora continua

- Realizar análisis de cumplimiento de la matriz de términos de referencia.
- Velar por el cumplimiento de los controles y subcentrales.
- De forma constante, la organización debe velar por el cumplimiento de lo establecido en esta metodología de diseño, con esto se garantizará un nivel de madurez alto, en cuanto a seguridad de la información.

Para ello, se propone que los resultados de los cálculos se midan de forma gráfica y que el documento anexo, auxiliar, desarrollado en Excel, de forma continua y que un custodio alimente el proceso.

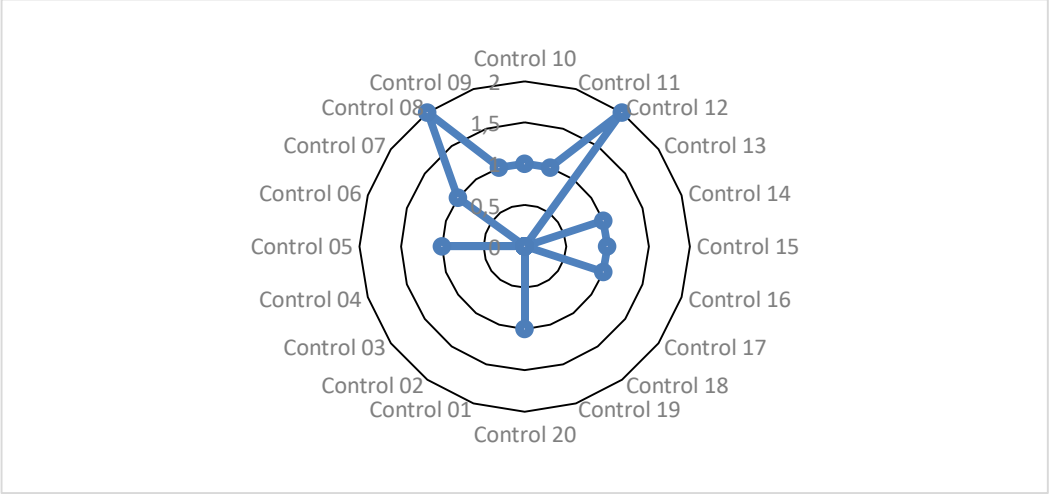


Figura. 3.2. Mapa de calor de cumplimiento de los controles de seguridad establecidos junto con el diseño de la red.

Fuente: Elaborado por el autor

3.4 Para llevar a cabo los controles y puesta en producción se requiere de lo siguiente:

3.4.1 Grupo de monitoreo:

Se propone realizar la implementación de puntos de red para 6 estaciones de monitoreo con posibilidad de crecer a 14, esto por disponibilidad de puntos de red, sin embargo, por disponibilidad de espacio físico se prevé un crecimiento de hasta 8 estaciones de monitoreo con acceso ethernet.

3.4.2 Grupo de operación:

Aquí se propone manejar las 12 estaciones de trabajo, por disponibilidad de puntos de red. Para las actividades de monitoreo, análisis y gestión propias del negocio.

3.4.3 Conectividad:

Para la conectividad se propone el uso de dos capas, conforme al modelo que se detalla en el capítulo anterior, reduce los costos, facilita el diseño y lo simplifica, costos.

Los equipos de monitoreo y operación estarán separados en VLAN diferentes, aunque compartirán el mismo equipo de conmutación, este equipo será de capa 2 estará en un armario en la oficina principal y contará con un equipo de la misma marca y modelo en redundancia.

El punto de núcleo será en el *datacenter*, en donde se ubicarán los equipos de borde y el conmutador de núcleo, que también tendrá redundancia, este equipo será de capa 3 por la necesidad de enrutar VLAN y cumplimiento de los controles de seguridad que se detallan más adelante en esta propuesta.

3.4.4 Borde:

Para los equipos de frontera se elegirá un firewall, que también estará en redundancia, con su respectivo equipo para alta disponibilidad.

Ambos equipos estarán conectados a dos servicios de internet independientes para balanceo de comunicaciones y alta disponibilidad de los servicios.

3.4.5 Centro de datos:

DMZ: Se destinará esta sección a los servidores de operación que mantendrán los procesos importantes de negocio activos.
Entre ellos se tendrá:

- Servidor de autenticación
- Servidores de archivos
- Servicios Web

- Bases de datos

3.4.6 Seguridad y apoyo:

Este grupo de servidores tendrán el *software* y *hardware* virtual de apoyo para seguridad y cumplimiento de los controles, así como el aprovechamiento de los recursos embebidos en los equipos de los partes de la red detalladas anteriormente.

Aquí se ubicará:

- Software de Inventario
- SIEM
- Analizador de vulnerabilidades
- Software de Seguridad
- Software para gestión de incidentes e inteligencia de seguridad
- Equipos para pruebas de penetración

Mismo que se detallan a continuación:

3.4.7 Controles propuestos de la SANS

 # 1. Inventario de dispositivos autorizados y no autorizados.

GMS debe administrar activamente todos los dispositivos de hardware en la red, de modo que solo los dispositivos autorizados tengan acceso y los dispositivos no autorizados puedan identificarse rápidamente y desconectarse antes de que inflijan daño o puedan acceder a datos confidenciales. (Gallardo, 2017).

 # 2. Inventario de software autorizado y no autorizado.

GMS debe administrar activamente todo el software en la red, por lo que solo se instala el software autorizado. Las medidas de seguridad como la inclusión de listas blancas de aplicaciones pueden permitir a las organizaciones encontrar rápidamente un software no autorizado antes de que se haya instalado o ejecutado. (Gallardo, 2017).

 # 3. Configuraciones seguras para hardware y software.

GMS necesita, realizar procesos de endurecimiento en las configuraciones de los activos de información, establecer, implementar y administrar la configuración de seguridad de

computadoras portátiles, servidores y estaciones de trabajo. Debe seguir una gestión de configuración estricta e implementar procesos de control de cambios para evitar que los atacantes exploten servicios y configuraciones vulnerables o que generalmente vienen en los dispositivos por defecto. (Gallardo, 2017).

 # 4. Evaluación continua de la vulnerabilidad y remediación.

GMS necesita evaluar de forma constante las vulnerabilidades sobre la red y los activos que forman parte de ella y tomar medidas continuamente sobre nueva información (por ejemplo, actualizaciones de software, parches, avisos de seguridad y boletines de amenazas) para identificar y remediar las vulnerabilidades que los atacantes podrían usar para penetrar en sus redes. (Gallardo, 2017).

 # 5. Uso controlado de privilegios administrativos.

"Este control requiere que las empresas utilicen herramientas automatizadas para monitorear el comportamiento del usuario y realizar un seguimiento de cómo se asignan y utilizan los privilegios administrativos para evitar el acceso no autorizado a los sistemas críticos, así como la manipulación mal intencionada con credenciales autorizadas para los efectos". (Gallardo, 2017).

 # 6. Mantenimiento, monitoreo y análisis de registros de auditoría.

GMS necesita recopilar, almacenar, administrar y analizar registros de eventos para detectar actividades aberrantes e investigar incidentes de seguridad, así como para reconstruir acciones realizadas por quienes operan la red, así como por quienes se benefician de sus funcionalidades, administradores y empleados. (Gallardo, 2017).

 # 7. Protecciones de correo electrónico y navegador web.

GMS debe asegurarse de que solo se utilicen navegadores web y clientes de correo electrónico totalmente compatibles en la organización para minimizar su superficie de ataque, así como implementar protección sobre los protocolos que emplean estas aplicaciones y garantizar que la circulación de datos en la red sea segura. (Gallardo, 2017).

 # 8. Defensa de *malware*

GMS debe asegurarse de que puedan controlar la instalación y ejecución de códigos maliciosos en múltiples puntos de la empresa. Este control recomienda el uso de herramientas automatizadas para monitorear continuamente estaciones de trabajo, servidores y dispositivos móviles con antivirus, antispyware, firewalls personales y funcionalidad IPS basada en host. (Gallardo, 2017).

 # 9. Limitación y control de puertos de red, protocolos y servicios.

"GMS debe detectar, monitorear y administrar permanentemente el uso de puertos, protocolos y servicios en dispositivos de red y equipos para minimizar las ventanas de vulnerabilidad disponibles para los atacantes". (Gallardo, 2017).

 # 10. Capacidad de recuperación de datos.

GMS debe asegurarse de que los sistemas y datos críticos se respalden adecuadamente con una frecuencia adecuada para que puedan recuperarse tan pronto como el negocio lo exija ante eventos o siniestros. También necesitan tener una metodología probada para la recuperación oportuna de datos. (Gallardo, 2017).

 # 11. Configuraciones seguras para dispositivos de red.

GMS debe establecer, implementar y administrar activamente la configuración de seguridad de los dispositivos de infraestructura de red, como cortafuegos y conmutadores, de forma segura, es decir, sin emplear configuraciones, accesos de usuarios y contraseñas por defecto, lo cual podría permitir a alguien mal intencionado acceder y alterar estas configuraciones en los dispositivos. (Gallardo, 2017).

 # 12. Defensa perimetral

GMS necesita detectar, administrar y controlar el flujo de información entre redes de diferentes niveles de confianza, con un enfoque analítico. Se ha revisado datos que podrían dañar la disponibilidad, confiabilidad o integridad de la información. La mejor defensa son las tecnologías que proporcionan una visibilidad y un control profundos

sobre el flujo de datos en todo el entorno, como la detección o prevención de intrusos, así como analítica de los paquetes a nivel profundo en las fronteras de la red. (Gallardo, 2017).

 # 13. Protección de Datos.

GMS debe usar los procesos y herramientas adecuados para mitigar el riesgo de la filtración de datos y garantizar la integridad de la información sensible. La protección de datos se logra mejor mediante la combinación de encriptación, protección de integridad y técnicas de prevención de pérdida de datos. (Gallardo, 2017).

 # 14. Acceso controlado basado en la necesidad de saber.

GMS necesita rastrear, controlar y asegurar el acceso a sus activos críticos, y determinar fácilmente qué personas, computadoras o aplicaciones tienen derecho a acceder a estos activos. (Gallardo, 2017).

#15. Control de acceso inalámbrico

GMS necesita contar con procesos y herramientas para rastrear y controlar el uso de redes de área local inalámbricas (LAN), puntos de acceso y sistemas de clientes inalámbricos. Todos los dispositivos inalámbricos conectados a la red deben coincidir con una configuración autorizada y un perfil de seguridad. (Gallardo, 2017).

#16. Control y monitoreo de cuenta.

Es fundamental que GMS administre activamente el ciclo de vida de las cuentas de usuario (creación, uso y eliminación) para minimizar las oportunidades de que los atacantes las aprovechen. Todas las cuentas del sistema deben ser revisadas regularmente, y las cuentas de los antiguos contratistas y empleados deben desactivarse tan pronto como la persona abandone la empresa. (Gallardo, 2017).

 # 17. Evaluación de habilidades de seguridad y capacitación adecuada para llenar vacíos.

GMS debe identificar el conocimiento específico y las habilidades que necesitan para fortalecer la seguridad. Esto requiere desarrollar y ejecutar un plan para identificar

brechas y solucionarlas a través de programas de políticas, planificación y capacitación. (Gallardo, 2017).

 # 18. Seguridad del software de la aplicación.

GMS debe administrar el ciclo de vida de seguridad de todo el software que utilizan para detectar y corregir las debilidades de seguridad. En particular, deben verificar regularmente que usen solo las versiones más actuales de cada aplicación y que todos los parches relevantes se instalen con prontitud. (Gallardo, 2017).

 # 19. Respuesta y manejo de incidentes.

GMS necesita desarrollar e implementar una respuesta adecuada a los incidentes, lo que incluye planes, roles definidos, capacitación, supervisión de la gestión y otras medidas que los ayudarán a descubrir ataques y contener el daño de manera más efectiva. (Gallardo, 2017).

 # 20. Pruebas de penetración y ejercicios de equipo rojo.

El control final requiere que GMS evalúe la fortaleza general de sus defensas (la tecnología, los procesos y las personas) así se pueden realizar pruebas de penetración externas e internas regulares. Esto les permitirá identificar vulnerabilidades y vectores de ataque que se pueden usar para explotar sistemas. (Gallardo, 2017).

El control 15, referente a seguridad para **comunicaciones inalámbricas**, no se considerará, dado que, en la red dimensionada, no se considera proveer este servicio, dado que por seguridad y sigilo de información y por petición de la empresa auspiciante no se proveerá este servicio.

3.4.8 Análisis de controles con el diseño propuesto:

En anexo 3. Se realiza la revisión de los controles propuestos y se diseña el proyecto con alcance que incluye, productos o servicios, documentación, normativa, seguimiento, indicadores y como realizar una mejora continua.

La propuesta ha sido entregada para consideración de quienes dirigirán la seguridad en

la compañía, esto se conformará por un comité de seguridad cuyos miembros serán la Gerencia General, la Presidencia Ejecutiva, la Gerencia de Servicios y el oficial de seguridad.

Socializado el diseño y aceptados los controles, subcontroles, procesos y métodos de evaluación, se realiza la implementación, para lo cual se debe considerar:

- Obra civil
- Adquisición de elementos
- Implementación de hardware y software base

3.4.9 Aspectos técnicos del producto

3.4.9.1 SIEM

Se requiere una plataforma de SIEM que sea capaz de procesar los logs de las siguientes plataformas:

En la tabla 3.1 se aprecia un formulario de levantamiento de información de plataforma SIEM

Tabla 3.1 Levantamiento de información de SIEM

Días de almacenamiento de logs			30			
	Ubicaciones					Kbytes
Type	**#1**	**#2**	**SUM**	**Logs al día**	**EPS**	**Bandwith**
Active Directory /LDAP / *Radius*	1	0	1	518.000	12	9.593
Antivirus/AntiSPAM	1	0	1	86.000	2	398
Application servers	1	0	1	86.000	2	995
Databases	1	0	1	172.000	4	1.194
DNS servers	1	0	1	1.728.000	40	12.000
Domain controllers	1	0	1	864.000	20	6.000
Firewalls DMZ/externo	1	0	1	2.600.000	60	18.056
Host intrusion detection systems	1	0	1	43.000	1	398
Network intrusion detectionsSystems	1	0	1	1.728.000	40	16.000
Switches	2	2	4	43.000	4	597
Unix / Linux Server	3	0	3	8.600	1	119
VPN terminators	1	0	1	43.000	1	299
Vulnerability scanner	2	0	2	8.600	0	199

Web servers	1	0	1	430.000	10	2.986
Windows server	9	0	9	172.000	36	28.667
TOTALS	27	2	**29**		**236,88**	100.687
MB/SEC					**MB**	0,10
DAILY GB					**GB**	4,05
STORAGE for LOG RETENTION					**TB**	0,119
					GB	121,528

Fuente: AlienVault an AT&T Company.

Se requiere una plataforma de SIEM que sea capaz de procesar:

- EPS (eventos por segundo): 237
- Ancho de banca: 0.1 MB
- Almacenamiento diario: 4.05 GB
- Almacenamiento mensual: 121,52 GB
- Almacenamiento anual: 1.4 TB
- Sensores: 2, uno por cada ubicación

Tráfico

VPN: el equipo debe poder manejar el tráfico de 50 VPN de clientes de la empresa auspiciante, actualmente se tienen 26 VPN, pero se espera un crecimiento alto.
Cada VPN transporta un tráfico que la empresa estima en 30 Mbps (indican que esto es por su experiencia en la red anterior), en la tabla 3.2 se visualiza el cálculo del análisis de equipos, usuarios y porcentajes de simultaneidad.

Tabla 3.2 Análisis de equipos, usuarios y porcentajes de simultaneidad.

Equipos	Totales	Usuarios simultáneos	Porcentaje en la hora pico
PC	12	8	66%
Servidores	10	10	100%
Monitores	8	8	100%

Fuente: Elaborado por el autor

Usuarios: el equipo debe soportar el tráfico de al menos 20 usuarios (12 pc y 8 monitores) y 10 servidores.

Por la operación de la red, se considera el peor escenario, medido en la hora pico, con las siguientes condiciones: se espera tener 3 turnos de los operadores, durante las 24 horas del día. Dos personas tendrán el día libre al mismo tiempo, se tendrá 10 personas en la red

en un día, 6 pantallas y 10 servidores activos todo el tiempo. La concurrencia de comunicaciones se calcula en un 66%, esto con base en la cantidad de usuarios que trabajan simultáneamente en una hora pico que representa los 2/3 de los totales. Por lo tanta la tabla 3.3 muestra el cálculo del tráfico total.

Tabla 3.3 Cálculo de tráfico total:

Servicios habilitados por usuario	Tráfico pico	PC (8 equipos)	Servidores (10)	Pantallas
VPN (6 por usuario activas en una hora)	180 Mbps	1440	0	0
Correo	0,5 Mbps	4	0	0
Navegación a internet	1 Mbps	8	8	8
VoIP (*softphones yealink*)	0,5 Mbps	4	0	0
Total		**1456 Mbps**	**8 Mbps**	**8 Mbps**

Fuente: Elaborado por el autor

Las VPN son empleadas por cada operador para monitorear redes de clientes a través de servicios gestionados de NOC, SOC y CSIRT. El correo electrónico es empleado para enviar notificaciones e interactuar con los clientes. La navegación para completar sus tareas operativas y cada estación de trabajo tiene instalado *sotfphones* para telefonía de VoIP.

Se requiere una plataforma que sea capaz de gestionar la seguridad perimetral de acuerdo con las siguientes características técnicas:

- ***Throughput* de red (tráfico a proteger)**: 1472 Mbps o 2.4 Gbps
- **Throughput de VPN:** 1440 Mbps o 1.4 Gbps
- **Puertos:** 4x1Gbps Eth**,** 2 para red interna, 2 para red WAN (se tiene redundancia en acceso a internet)

3.4.9.2 Protección de punto final

Se requiere contratar protección para:

- 10 servidores entre Windows y Linux
- 12 estaciones de trabajo Windows

3.4.9.3 Prevención de fuga de información

Se requiere contratar software de prevención de fuga de información que permita:

- **Compatibilidad:** con sistemas operativos Windows

- **Administración:** centralizada
- Auditoría
- Solución todo en uno (no diferentes componentes, servidor de DLP, base de datos, agentes, etc. Por facilidad de administración)

3.4.9.4 Cifrado de equipos

Se requiere cifrado con las siguientes características:

- **Algoritmo:** AES 256 bits
- **Administración:** Centralizada

3.4.9.5 Administración de parches y vulnerabilidades

Se requiere detección de vulnerabilidades y parchado con las siguientes características:

Compatibilidad: Sistemas operativos Windows

Detección: Vulnerabilidades de sistemas operativos y aplicaciones de escritorio

Corrección: Vulnerabilidades de sistemas operativos y aplicaciones de escritorio

Gestión: Centralizada, automática, programada o manual.

3.4.9.6 Gestión de usuarios

Se requiere una plataforma que permita la gestión de usuarios con las siguientes características:

Compatibilidad de administración: Sistemas operativos Windows

Compatibilidad de integración: Con los demás componentes de la red

3.4.9.8 Firewall para aplicaciones WEB

Se requiere una plataforma de WAF con la siguiente capacidad:

- **Tráfico web limpio**: 5 Mbps (capacidad asignada por la empresa al servicio WEB)

3.4.9.9 Gestor de contraseñas

Se requiere una plataforma de gestión de contraseñas con las siguientes características:

- **Compatibilidad de escritorio:** Sistemas operativos Windows
- **Compatibilidad con navegadores web:** Navegadores Google Chrome y Mozilla

Firefox

- **Compatibilidad con dispositivos móviles:** Android y iOS

3.4.9.10 Doble factor de autenticación

Se requiere una plataforma de doble factor de autenticación con las siguientes características:

- **Compatibilidad de integración:** Sistemas operativos Linux (Debian 3.5)
- **Compatibilidad con dispositivos móviles:** Android y iOS

3.4.9.11 Análisis de código fuente

Se requiere una plataforma de análisis de código fuente para el aplicativo web desarrollado que tenga las siguientes características:

- Análisis estático
- Análisis dinámico
- Tipo SaaS
- Análisis de librerías de terceros
- Sandbox

3.4.9.12 Patch panel

Debe tener las siguientes características:

Número de puertos: 24 (se usarán 12 para los puntos de red de los usuarios, 6 para los monitores y 6 quedarán libres por crecimiento, se espera tener 2 monitores más en el corto plazo)

- Conectores: RJ45 / ETH (toda la red es gigabit ethernet)
- Velocidad: 24x1Gbps

3.4.9.13 Switch

Se requiere switch con las siguientes características:

- **Capa:** 3
- **Número de puertos:** 24
- **Velocidad de puertos de conmutación:** 24x1Gbps
- **Enlaces troncales:** Si, 4
- **Velocidad de los enlaces troncales:** 10 Gbps ETH

- **Redundancia:** Si
- **Soporte para:** 802.1W o RSPT (*Rapid Spanning Tree Protocol*)
- **Administrable:** Si

3.4.10 Selección de productos

Para la selección de los productos se consideran las características de varias marcas o fabricantes de las mismas soluciones, como requerimiento se plantea que la solución pueda cubrir los controles y subcontroles de tal forma que se involucre el menor número de soluciones y se reduzcan los costos de adquisición, operación y mantenimiento, el manejo de diversas plataformas requiere más personal, por lo que debe ser optima la cantidad de sistemas que se involucran. De esta forma, una solución que cubra varias necesidades será una mejor opción. El último parámetro de evaluación es el costo, con el objetivo de minimizar el impacto en el presupuesto.

3.4.10.1 Selección de plataforma de SIEM

En la tabla 3.4 se consideran tres marcas de productos que pueden ser adquiridos y se evalúan los parámetros con base en los subcontroles:

Tabla 3.4 Comparativa de plataforma SIEM

Funcionalidades	ALIENVAULT	McAfee	LogRhythm	Justificación
SIEM	X	X	X	Necesario para el cumplimiento del control 6
Análisis de vulnerabilidades	X			Necesario para el cumplimiento del control 4
Inventario de activos	X		X	Necesario para el cumplimiento del control 1
Descubrimiento activo de activos	X		X	Necesario para el cumplimiento del control 1
Descubrimiento pasivo de activos	X		X	Necesario para el cumplimiento del control 1
Monitoreo de cuentas de usuario	X	X	X	Necesario para el

				cumplimiento del control 16
Monitoreo de integridad de archivos	X	X	X	Necesario para el cumplimiento del control 3
Monitoreo de integridad de sistema		X	X	Necesario para el cumplimiento del control 3
Cumplimiento normativo	X	X	X	Necesario para el cumplimiento del objetivo de negocio, mediante los reportes de cumplimiento normativo se puede evaluar la aplicación de ciertos subcontroles
Clasificación dinámica de activos por el software de red	X			Necesario para el cumplimiento del control 2
Inventario de software de red	X			Necesario para el cumplimiento del control 2
Monitoreo de logs de actividades realizados por usuarios administradores	X	X	X	Necesario para el cumplimiento del control 5
Monitoreo de errores en configuración de sistemas	X		X	Necesario para el cumplimiento del control 3
Monitoreo y detección de malas prácticas en la administración de sistemas	X		X	Necesario para el cumplimiento del control 3
Costo	Bajo	Medio	Alto	Debe entrar en el presupuesto

Fuente: Elaborado por el autor

El producto seleccionado para implementar es Alienvault, por el cumplimiento de los requerimientos y características.

3.4.10.2 Selección de plataforma de protección Endpoint

Como se aprecia en la figura 3.5 se consideran tres marcas de productos que pueden ser adquiridos y se evalúan los parámetros con base en los subcontroles:

Tabla 3.5 Comparativa para plataforma de seguridad de punto final

Funcionalidades	Sophos Central	ESET	BitDefender	Justificación
Protección centralizada cloud	X		X	Necesario para el cumplimiento del control 8
IPS basado en host	X	X	X	Necesario para el cumplimiento del control 8
Control de periféricos	X	X		Necesario para el cumplimiento del control 8
Protección en tiempo real	X	X	X	Necesario para el cumplimiento del control 8
Protección de navegación	X	X	X	Necesario para el cumplimiento del control 7
Protección de malware de correo electrónico	X	X	X	Necesario para el cumplimiento del control 7
Control de archivos por extensión	X	X	X	Necesario para el cumplimiento del control 7
Costo	Bajo	Medio	Alto	Debe entrar en el presupuesto

Fuente: Elaborado por el autor

Posterior a la evaluación el producto que cumple con los parámetros adecuados para protección de punto final es Sophos Central.

3.4.10.3 Selección de plataforma para la prevención de fuga de información

En la tabla 3.6 se consideran tres marcas de productos que pueden ser adquiridos y se evalúan los parámetros con base en los subcontroles:

Tabla 3.6 Comparativa de plataforma para DLP (*Data Loss Prevention*)

Funcionalidades	Sophos Enpoint DLP	McAfee DLP	Symantec DLP	Justificación
Identificación de aplicaciones por categoría	X		X	Necesario para el cumplimiento del control 2
Permiso o denegación de ejecución de aplicaciones	X	X	X	Necesario para el cumplimiento del control 2
Comprueba la integridad de los archivos	X			Necesario para el cumplimiento del control 8
Identificación de información sensible	X	X	X	Necesario para el cumplimiento del control 13
Previene la fuga de información	X	X	X	Necesario para el cumplimiento del control 13
Integración con la protección de navegación	X			Necesario para el cumplimiento del control 7
Integración con la protección de correo	X			Necesario para el cumplimiento del control 7
Costo	Bajo	Medio	Alto	Debe entrar en el presupuesto

Fuente: Elaborado por el autor

Durante el proceso de elaboración del proyecto de titulación la empresa Symantec fue adquirida por la empresa Broadcom y cerró operaciones en Latinoamérica, por lo que se descartó.

3.4.10.4 Selección de plataforma de encriptación

En la figura 3.7 se consideran tres marcas de productos que pueden ser adquiridos y se evalúan los parámetros con base en los subcontroles:

Tabla 3.7 Comparativa para plataforma de encriptación

Funcionalidades	Sophos Encription	McAfee Encription	Kaspersky Encription	Justificación
Administración centralizada cloud	X			Necesario para el cumplimiento del control 13
Cifrado de información sensible	X	X	X	Necesario para el cumplimiento del control 13
Cifrado compatible con bitlocker	X			Necesario para equipos con sistema operativo Windows
Cifrado de disco	X	X	X	Necesario para el cumplimiento del control 13
Costo	Bajo	Medio	Alto	Debe entrar en el presupuesto

Fuente: Elaborado por el autor

Para la selección del producto para encriptación se considera el cumplimiento del equipo de Sophos Endpoint y DLP.

3.4.10.5 Selección de plataforma de gestión de parches

Se puede visualizar en la tabla 3.8 tres marcas de productos que pueden ser adquiridos y se evalúan los parámetros con base en los subcontroles:

Tabla 3.8 Comparativa de plataforma para gestión de parches y vulnerabilidades

Funcionalidades	Kaspersky WSUS	Microsoft WSUS	Justificación
Análisis de vulnerabilidades de aplicaciones de escritorio	X		Necesario para el cumplimiento del control 4
Análisis de vulnerabilidades de sistema operativo	X	X	Necesario para el cumplimiento del control 4
Permite programar tareas de parchado y remediación de vulnerabilidades	X	X	Necesario para el cumplimiento del control 4
Actualización constante de nuevas vulnerabilidades	X	X	Necesario para el cumplimiento del control 4
Costo	Bajo	Medio	Debe entrar en el presupuesto

Fuente: Elaborado por el autor

El producto seleccionado para la gestión de parches y vulnerabilidades es Kaspersky WSUS.

3.4.10.6 Selección de plataforma de gestión de usuarios

En la tabla 3.9 se consideran tres marcas de productos que pueden ser adquiridos y se evalúan los parámetros con base en los subcontroles:

Tabla 3.9 Comparativa para gestión de usuarios

Funcionalidades	Active Directory	LDAP	Radius	Justificación
Permite la administración de usuarios y sus privilegios	X	X	X	Necesario para el cumplimiento del control 5
Permite tener usuarios estándar y administradores	X	X	X	Necesario para el cumplimiento del control 5
Permite almacenar auditorías de las actividades de los usuarios	X	X	X	Necesario para el cumplimiento del control 5
Debe limitar puertos de red	X			Necesario para el cumplimiento del control 9
Administra el firewall del host	X			Necesario para el cumplimiento del control 9
Se puede configurar la longitud de las contraseñas	X	X	X	Necesario para el cumplimiento del control 5
Costo	Bajo	Uso libre	Uso libre	Debe entrar en el presupuesto

Fuente: Elaborado por el autor

Posterior a la evaluación el producto seleccionado para la gestión de usuarios es *Active Directory*.

3.4.10.7 Selección de plataforma de aplicaciones de plataforma web

Como se aprecia en la figura 3.10 se consideran tres marcas de productos que pueden ser adquiridos y se evalúan los parámetros con base en los subcontroles:

Tabla 3.10 Comparativa de plataforma web

Funcionalidades	Sophos WAF	Imperva	F5	Justificación
Bloquea comunicaciones de sitios maliciosos	X	X	X	Necesario para el cumplimiento del control 12
Bloquea comunicaciones de IP con mala reputación	X	X	X	Necesario para el cumplimiento del control 12
Se integra con la solución de protección de navegación	X			Necesario para el cumplimiento del control 12
Costo	Bajo	Alto	Medio	Debe entrar en el presupuesto

Fuente: Elaborado por el autor

Se considera el producto más adecuado Sophos WAF.

3.4.10.8 Selección de plataforma de administración de passwords

Se visualiza en la figura 3.11 tres marcas de productos que pueden ser adquiridos y se evalúan los parámetros con base en los subcontroles:

Tabla 3.11 Comparativa de plataformas administrativas de passwords

Funcionalidades	One password	Lastpass	Kaspersky password manager	Justificación
Genera auditorías del uso de cuentas	X	X	X	Necesario para el cumplimiento del control 16
Permite asignar permisos a las cuentas basadas en la "necesidad del saber"	X	X	X	Necesario para el cumplimiento del control 16
Cuenta con bóvedas que agrupan accesos para los usuarios	X			Solicitado por la empresa auspiciante
Revoca permisos de usuario caduco	X	X	X	Necesario para el cumplimiento del control 5
Ofrece un punto de acceso centralizado	X	X	X	Necesario para el cumplimiento del control 5
Costo	Medio	Bajo	Alto	Debe entrar en el presupuesto

Fuente: Elaborado por el autor

3.4.10.9 Selección de plataforma de doble factor de autenticación

Por requerimiento del negocio la empresa solicita el uso de Google Authenticator, por compatibilidad con los sistemas que operará la gente que usará la red diseñada.

El sistema operativo principal es Debian 3.5, el SDK (*Software Development Kit*) de Google Authenticator es compatible con este sistema.

3.4.10.10 Selección de plataforma para protección del perímetro

Se indica en la figura 3.12 tres marcas de productos que pueden ser adquiridos y se evalúan los parámetros con base en los subcontroles:

Tabla 3.12 Comparativa de plataformas para seguridad perimetral

Funcionalidades	Sophos XG 230	Checkpoint	Palo Alto	Justificación
Permite controlar el acceso a la red de los dispositivos autorizados y no autorizados	X	X	X	Necesario para el cumplimiento del control 1
Permite controlar el uso de aplicaciones de red	X	X	X	Necesario para el cumplimiento del control 2
Cuenta con un motor de antivirus para red	X	X	X	Necesario para el cumplimiento del control 8
Cuenta con protección para correo electrónico	X			Necesario para el cumplimiento del control 7
Cuenta con protección y control para navegación segura	X	X	X	Necesario para el cumplimiento del control 7
Realiza control de puertos y protocolos en capa 4	X	X	X	Necesario para el cumplimiento del control 9
Permite seccionar las redes y brindar accesos por usuarios o equipos específicos	X	X	X	Necesario para el cumplimiento del control 14
Brinda seguridad en el perímetro de las redes	X	X	X	Necesario para el cumplimiento del control 12
Integración con seguridad de punto final	X			Necesidad del manejo de una sola plataforma
Costo	Medio	Alto	Medio	Debe entrar en el presupuesto

Fuente: Elaborado por el autor

Luego de la evaluación se ha seleccionado el equipo de Sophos XG para la protección de perímetro.

3.4.10.11 Selección de plataforma de análisis de código fuente

La empresa auspiciante cuenta actualmente con un equipo de innovación y desarrollo de software, este equipo de trabajo contaba previamente con la solución de Veracode, fue requisito mantener esta solución para el análisis de código. Se ampliará el licenciamiento adquirido.

3.4.11 Análisis de costos:

En la tabla 3.13 se puede observar el análisis por producto, aquí se realizó un análisis con las posibles soluciones para cumplir los controles aceptados por la organización, una vez seleccionadas las opciones se validaron los costos. Al ser una empresa de venta de soluciones de seguridad, accede a cotizaciones directas con los fabricantes o mayoristas de equipos y licencias asociadas, por lo que no fue necesario escoger diferentes empresas oferentes y comparar precios, los mayoristas dan el mayor descuento a esta organización por su giro de negocio.

Los costos se dividen en tres secciones, los costos de equipos o licencias que se deben pagar a un tercero, los costos de hora hombre de las consultorías asociadas a los servicios por implementar y los costos de personal operativo para la puesta de producción de todo lo descrito.

El costo en los productos de

- ALIENVAULT
- SOPHOS XG
- SOPHOS INTEREPT X
- SOPHOS DLP
- SOPHOS ENCRIPTION
- WSUS
- ACTIVE DIRECTORY
- SOPHOS WAF
- ONE PASSWORD
- GOOGLE AUTHENTICATOR
- VERACODE

Se lo manejará en modalidad MSP, es decir administración de proveedor de servicios, esto permite a la empresa no realizar un pago único sino que se realizará un pago mensual, similar a un pago por consumo, que incluye los equipos físicos como el Firewall Sophos XG, esto permite que la empresa no se llene de activos y sea más eficiente a la hora de mantener el flujo de dinero en su administración, así también es un aporte significativo a que el proyecto sea factible de implementar.

Tabla 3.13. Análisis por producto

ITEM	PRODUCTO	TIPO	DESCRIPCIÓN	CANTIDAD PRODUCTOS / HORAS	COSTO LOCAL UNITARIO	COSTO SUB-TOTAL
1	ALIENVAULT	Software as a *service*	AlienVault Anywhere Server 250 GB AlienVault Anywhere Sensor x 2 Suscripción x 12 meses	1	$ 8.197,20	$ 8.197,20
2	SOPHOS XG	Hardware and software	Sophos XG 230 4x1Gbps Full Guard	1	$ 6.112,50	$ 6.112,50
3	SOPHOS INTEREPT X	Software as a *service*	Sophos Intercept X for endpoint and server x 20 licencias Suscripción x 12 meses	20	$ 32,60	$ 652,00
4	SOPHOS ENDPOINT AND DLP	Software as a *service*	Sophos for endpoint and DLP x 20 Licencias Suscripción x 12 meses	20	$ 64,90	$ 1.298,00
5	SOPHOS ENCRIPTION	Software as a *service*	Sophos Encription x 20 licencias Suscripción x 12 meses	20	$ 12,00	$ 240,00
6	WSUS	Software	Licencia de microsoft Windows 2016 x 1	1	$ 1.895,00	$ 1.895,00
7	ACTIVE DIRECTORY	Software	Licencia de microsoft Windows 2016 x 1	1	$ 1.895,00	$ 1.895,00
8	SOPHOS WAF	Hardware and software	Sophos WAF Licencia de WAF + Licencia de Management	1	$ 32.000,00	$ 32.000,00
9	ONE PASSWORD	Software as a service	Licencia One Password x 20 licencias	20	$ 12,00	$ 240,00
10	GOOGLE AUTHENTICATOR	Software	Google Authenticator x 20 usuarios	20	$ -	$ -
11	VERACODE	Software as a service	Veracode Static Scan 80 MB, SCA, Dynamic Scan (3 URL) and Greenlight x 4	1	$ 26.520,00	$ 26.520,00
					TOTAL	**$ 79.049,70**

Fuente: Elaborado por el autor

La tabla 3.14 indica el análisis por servicios, los servicios que implican consultoría se consideran como pago único, si bien los servicios de SOC, ingeniería social y hacking ético no se realizan una única vez, sino que son repetitivos se los toma en pago único puesto que no se puede aplicar el concepto anterior de MSP, sin embargo, al ser horas hombre de servicios profesionales, su pago es contra ejecución de las actividades, por lo que también esto facilita el flujo de caja de la empresa.

El promedio de hora hombre en el mercado, aparentemente, es mucho más elevado, sin embargo, al tratarse de servicios de una empresa que los vende a clientes finales, estos también se consideran al costo que tiene la empresa y no al precio que podrían contratarse, puede ser cliente final de una consultora o prestadora de estos servicios.

Todos los productos y soluciones consideradas dentro de este análisis, en la figura 3.14 se contemplan ser 100% implementadas y mantener operativas, así se vuelve necesario considerar, la instalación, la configuración y la capacitación al personal que posteriormente lo operará, de esta forma se garantiza que el 100% de las soluciones serán aprovechadas por la empresa.

Tabla 3. 14 Análisis por Servicios

ITEM	SERVICIOS	TIPO	DESCRIPCIÓN	CANTIDAD PRODUCTOS / HORAS	COSTO LOCAL UNITARIO	COSTO SUB-TOTAL
1	CONSULTORÍA DE *HARDENING*	Servicios profesionales	Levantamiento de plantillas de endurecimiento de software y hardware, Windows, Linux, AWS, Switch, Server, Sophos WAF, AlienVault, Sophos.	160	$ 25,00	$ 4.000,00
2	CONSULTORÍA DE CLASIFICACIÓN DE INFORMACIÓN	Servicios profesionales	Definición de metodología y consultoría de clasificación de información para un proceso	160	$ 25,00	$ 4.000,00
3	INGENIERÍA SOCIAL	Servicios profesionales	Servicio de Gestión de Ingeniería Social para entrenamiento continuo a usuarios para detectar y no ser víctimas de ataques de phishing	180	$ 25,00	$ 4.500,00
4	CAPACITACIÓN DE HERRAMIENTAS DE SEGURIDAD (adicionales a las implementadas)	Servicios profesionales	Capacitación en respuesta a incidentes y análisis forense	40	$ 25,00	$ 1.000,00
5	CAPACITACIONES ESPECIALIZADAS EN SEGURIDAD	Servicios profesionales	Capacitación en ISO27000 y Sistema de Gestión de Seguridad de la información	80	$ 25,00	$ 2.000,00
6	CONSULTORÍA DE EH	Servicios profesionales	Servicios de *hacking* ético.	240	$ 25,00	$ 6.000,00
7	SERVICIOS CSIRT	Servicios profesionales	Servicios de respuesta a incidentes	96	$ 25,00	$ 2.400,00
8	SERVICIOS DE SOC	Servicios profesionales	Servicios de monitoreo de las plataformas de seguridad, red, servidores y equipos y alertamiento de amenazas y anomalías	360	$ 15,00	$ 5.400,00
9	ALIENVAULT	Servicios profesionales	Instalación (40), configuración (40) y capacitación (40)	120	$ 25,00	$ 3.000,00
10	SOPHOS XG	Servicios profesionales	Instalación (16), configuración (24) y capacitación (20)	60	$ 25,00	$ 1.500,00

11	SOPHOS INTEREPT X	Servicios profesionales	Instalación (32), configuración (8) y capacitación (12)	52	$	25,00	$	1.300,00
12	SOPHOS ENDPOINT AND DLP	Servicios profesionales	Instalación (32), configuración (80) y capacitación (12)	114	$	25,00	$	2.850,00
13	SOPHOS ENCRIPTION	Servicios profesionales	Instalación (40), configuración (8) y capacitación (16)	72	$	25,00	$	1.800,00
14	WSUS	Servicios profesionales	Instalación (16), configuración (16) y capacitación (24)	56	$	25,00	$	1.400,00
15	ACTIVE DIRECTORY	Servicios profesionales	Instalación (40), configuración (20) y capacitación (40)	100	$	25,00	$	2.500,00
16	SOPHOS WAF	Servicios profesionales	Instalación (80), configuración (120) y capacitación (40)	240	$	25,00	$	6.000,00
17	ONE PASSWORD	Servicios profesionales	Instalación (24), configuración (16) y capacitación (8)	48	$	25,00	$	1.200,00
18	GOOGLE AUTHENTICATOR	Servicios profesionales	Instalación (80), configuración (16) y capacitación (20)	116	$	25,00	$	2.900,00
19	VERACODE	Servicios profesionales	Instalación (8), configuración (24) y capacitación (40)	72	$	25,00	$	1.800,00
					Total		$	55.550,00

Fuente: Elaborado por el autor

Los costos de equipos de telecomunicaciones y redes tradicionales como se indica en la tabla 3.15 se consideran los proveedores que la empresa tiene actualmente por lo que no se realiza una gestión de selección de proveedor o mejores precios, ya que este trabajo se había realizado con anterioridad y no se consideró necesario, no se puede adjuntar esta información ya que es considerada confidencial para la empresa.

Tabla 3.15. Análisis de producto para red tradicional

ITEM	PRODUCTO PARA RED TRADICIONAL	TIPO	DESCRIPCIÓN	CANTIDAD PRODUCTOS / HORAS	COSTO LOCAL UNITA-RIO	COSTO SUB-TOTAL
1	Cableado estructurado	Material y servicios profesionales	Puntos de red que incluye cableado, material y mano de obra	36	18,5	$ 666,00
2	Paneles de conexión para cableado	Material y servicios profesionales	Paneles y la instalación	4	160	$ 640,00
3	Conmutadores HP	Material y servicios profesionales	2 para el *core*	2	780	$ 1.560,00
4	Conmutadores DLINK	Material y servicios profesionales	2 para el acceso	2	460	$ 920,00
5	Laptop	Hardware	Equipos de punto final para los usuarios (incluye licencia de sistema operativo y software de ofimática)	14	1260	$ 17.640,00
6	Servidores locales	Hardware	Equipos (incluye montaje y configuración)	2	7200	$ 14.400,00
7	Servidores de nube	Infraestructura como servicio	Servicio de IaaS para servidores en la nube de AWS	12	3000	$ 36.000,00
					Total	$ 71.826,00

Fuente: Elaborado por el autor

En la tabla 3.16 se puede observar el análisis de financiamiento, la empresa mantiene líneas de crédito corporativo con varias entidades financieras por lo que acceden a créditos con menor tasa de interés que un crédito de consumo tradicional, para la inversión se considera la fórmula de financiamiento que contempla, el plazo de pago de 12 meses incluye

capital e interés, también se considera que esto en sí, no constituye un gasto sino una inversión.

La empresa prestará servicios con esta red a otras empresas que son sus clientes, para recuperar la inversión se ha estimado un periodo de 36 meses, con un total de 24 clientes que sean operativos, el análisis de costos, inversión, plazos de recuperación y número de clientes, no se lo incluye ya que la empresa lo entregó como resultado de una consultoría interna que se considera confidencial, estos datos se asumen como válidos sin verificación, para este proceso ya que no se tiene acceso a publicar la información, solo se la ha comprobado con los involucrados en el proceso.

Tabla 3.16. Análisis de financiamiento

ANÁLISIS DE FINANCIAMIENTO		
Presupuesto estimado:	$	250.000,00
Presupuesto ejecutado:	$	214.863,70
Financiamiento anual		9,50%
Plazo		12
Pago mensual		$ (18.840,00)
Institución		Banco de Guayaquil
Total, por pagar		$ (226.080,05)
Tiempo estimado de recuperación:		36 meses
Número de clientes objetivo para el servicio: (es parte de otra consultoría, solo se toma la información)		24 clientes

Fuente: Elaborado por el autor

3.4.12 Cronograma de actividades

Mediante el cronograma que muestra el anexo 2, se planifica ejecutar y poner en producción las acciones de la siguiente forma:

3.4.13 Ventajas del producto

Las ventajas de cada uno de los productos y/o servicios que se emplea en este proyecto están basadas en el cumplimiento de cada control, en la tabla 3.17 se encuentra la lista de las soluciones con nombres genéricos y estándar de la industria, se identifican con un código, que permite asociarlo a las ventajas en términos de cumplimiento de controles, se detalla en la tabla 3.18.

Simbología:

Prod#: Codificación usada en el presente trabajo que indica que es un producto de hardware o software que debe ser adquirido o implementado.

Serv#: Codificación usada en el presente trabajo que indica que es un servicio que se debe ejecutar sobre los productos o elementos que conforman la red.

Net#: Codificación usada en el presente trabajo para indicar que es un elemento del diseño tradicional de redes.

#: Codificación usada en el presente trabajo para indicar que se reemplazará por una secuencia de números.

Tabla 3.17. Soluciones implementadas

ID	Solución
Prod1	Plataforma unificada de gestión de logs y eventos de seguridad
Prod2	Firewall de nueva generación (hasta capa 7)
Prod3	Antimalware
Prod4	Protección de punto final y prevención de fuga de información
Prod5	Respaldos de información
Prod6	Encriptación de datos y discos
Prod7	Servidor de parchado e instalación de actualizaciones
Prod8	Administración de usuarios y equipos
Prod9	Protección de bases de datos y aplicaciones web
Prod10	Gestor de contraseñas y accesos
Prod11	Doble factor de autenticación
Prod12	Analizador de código y desarrollo seguro
Serv1	Servicios para definición de metodología y aplicación de configuraciones seguras y endurecimiento de controles en *harware* y *software*
Serv2	Servicios para definición de metodología de clasificación de información y análisis de riesgo
Serv3	Servicio de evaluación de vulnerabilidades a usuarios finales con ataques simulados de ingeniería social
Serv4	Capacitaciones en seguridad informática
Serv5	Capacitaciones en gobierno de seguridad de la información (SGSI)
Serv6	Servicios de evaluación de seguridad, Hacking Ético, interno y externo.
Serv7	Servicios de diseño de plan de respuesta a incidentes y apoyo ante emergencias de seguridad
Serv8	Servicios de monitoreo y gestión de herramientas de seguridad informática
Net1	Servicios de instalación y equipamiento para cableado estructurado
Net2	paneles de conexión para cableado
Net3	*Switches* para conmutación
Net4	Equipos para usuario final
Net5	Servidores para servicios de red locales
Net6	Infraestructura como servicio contratada en la nube de AWS, *Amazon web services*. (IaaS)

Fuente: Elaborado por el autor

Tabla 3.18. Controles utilizados por equipos y servicios

		Control																		
	ÍTEM	1	2	3	4	5	6	7	8	9	10	11	12	13	14	16	17	18	19	20
ID	**HARDWARE Y SOFTWARE**																			
Prod1	ALIENVAULT	x	X	x	x	X	x									X				
Prod2	SOPHOS XG	x	X					X	X	X			X		X					
Prod3	SOPHOS INTEREPT X							X	X											
Prod4	SOPHOS ENDPOINT AND DLP		X					X	X					X						
Prod5	SOPHOS ENCRIPTION													X						
Prod6	WSUS				x															
Prod7	ACTIVE DIRECTORY					X				X										
Prod8	SOPHOS WAF												X							
Prod9	ONE PASSWORD					X										X				
Prod10	GOOGLE AUTHENTICATOR					X										X				
Prod11	VERACODE																	x		
	SERVICIOS Y MANO DE OBRA																			
Serv1	CONSULTORÍA DE HARDENING			x								X			X					
Serv2	CONSULTORÍA DE CLASIFICACIÓN DE INFORMACIÓN													X	X					
Serv3	INGENIERÍA SOCIAL																X			
Serv4	CAPACITACIÓN DE HERRAMIENTAS DE SEGURIDAD																X			
Serv5	CAPACITACIONES ESPECIALIZADAS EN SEGURIDAD																X			
Serv6	CONSULTORÍA DE EH																			X

Serv7	SERVICIOS CSIRT			X
Serv8	SERVICIOS DE SOC	X		
		DISEÑO TRADICIONAL		
Net 1	Cableado estructurado			
Net 2	paneles de conexión para cableado		N/A	
Net 3	Conmutadores HP y DLINK		N/A	
Net 4	Laptop		N/A	
Net 5	Servidores locales		N/A	
Net 6	Servidores de nube		N/A	

Fuente: Elaborado por el autor

CAPÍTULO 4

IMPLEMENTACIÓN

4.1 Desarrollo

Se realiza un levantamiento de la situación inicial de la red, a pesar de que, por pedido de la empresa no es necesario considerarla, es un diseño e implementación desde cero, es particularmente importante para apreciar el cambio.

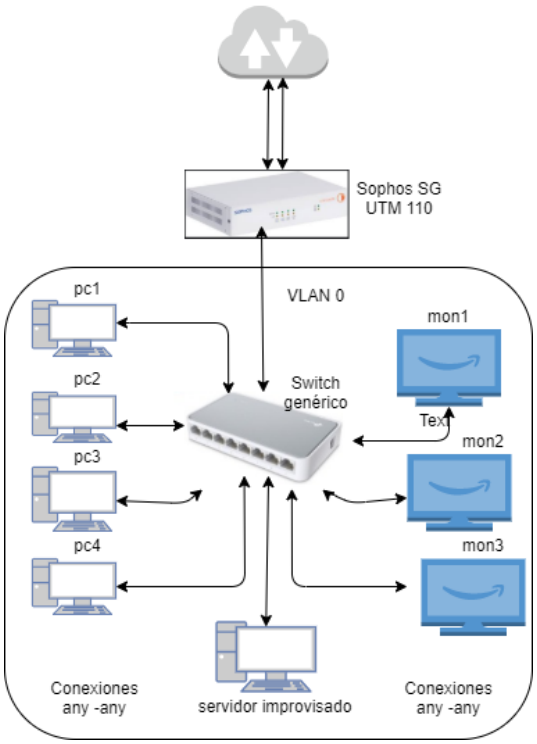


Figura. 4.1. Red antigua

Fuente: Elaborado por el autor

En la figura 4.1, se puede apreciar que la red era completamente plana, el único conmutador no era administrable y no se podía segmentar en VLAN, el equipo de perímetro era muy pequeño, por lo que no se podía aplicar políticas de seguridad y todo el tráfico sin importar el origen, puerto, protocolo o destino se cursaba.

En la figura 4.2 se aprecia la sala de monitoreo antigua la cual era un espacio acomodado de 4 escritorios y equipos de propósito genérico.

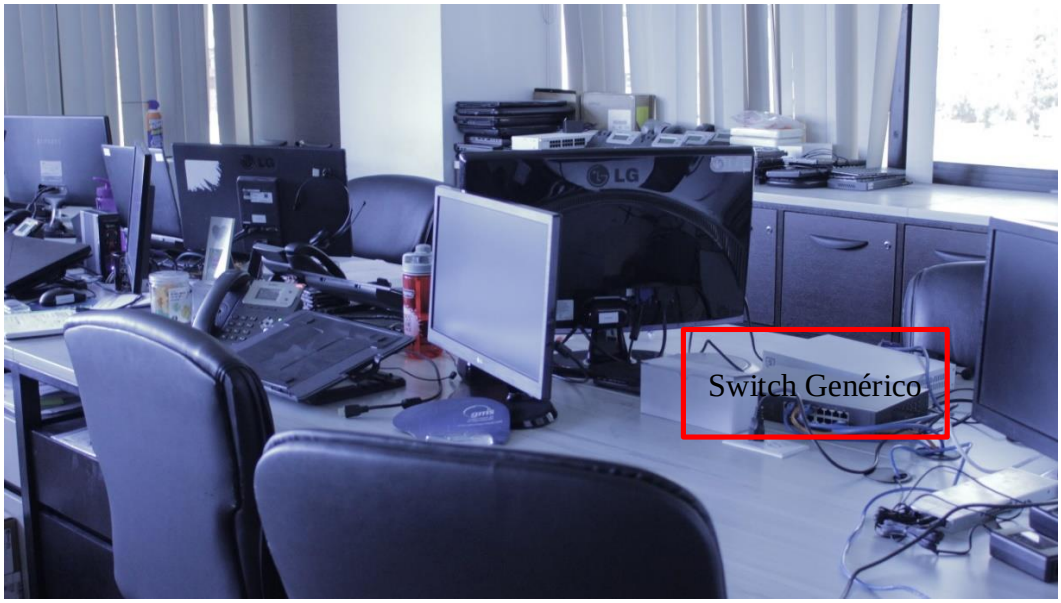


Figura. 4.2. Sala improvisada de monitoreo (antigua)

Fuente: Elaborado por el autor

Se realiza un levantamiento de la situación inicial de la empresa previo al trabajo de titulación, para el efecto se analiza el cumplimiento de los controles y sub-controles sin realizar ningún cambio y se plantea mejorar ese cumplimiento mediante la aceptación de la propuesta descrita anteriormente. La tabla 4.1 indica el cumplimiento inicial de los controles y subcontroles.

Tabla 4.1. Situación inicial de cumplimiento de los controles de seguridad de la información.

Control	**Situación Inicial (Escala de 0 a 5)**
Control 10	1
Control 11	1
Control 12	2
Control 13	0
Control 14	1
Control 16	1
Control 17	0
Control 18	0
Control 19	0
Control 20	1
Control 01	0
Control 02	0
Control 03	0
Control 04	0
Control 05	1
Control 06	0
Control 07	1
Control 08	2
Control 09	1
Promedio	**0.63**

Fuente: Elaborado por el autor

Una vez se termine el desarrollo, se espera alcanzar un promedio de al menos 4 puntos en la escala de 0 a 5 en los 19 controles a intervenir. Se tendrá como resultado la siguiente tabla 4.2 con el objetivo a cumplirse.

Tabla 4.2 Puntuación de cumplimiento

Control	Resultado esperado (Escala de 0 a 5)
Control 10	4
Control 11	4
Control 12	4
Control 13	4
Control 14	4
Control 16	4
Control 17	4
Control 18	4
Control 19	4
Control 20	4
Control 01	4
Control 02	4
Control 03	4
Control 04	4
Control 05	4
Control 06	4
Control 07	4
Control 08	4
Control 09	4
Promedio	4

Fuente: Elaborado por el autor

En esta fase se documenta como se encuentra la red diseñada con los controles de seguridad que ha sido implementada, finalmente, se ha considerado 27 proyectos en total, que conllevan la implementación de soluciones y servicios acorde a las necesidades, mismas que han sido vistas en la propuesta, estos 27 proyectos cubren 19 de los 20 controles existentes y se elimina el control de 15, referente a seguridad de redes *wireless* o comunicaciones inalámbricas, ya que no se provee este servicio en la red.

4.1.2 Diseño

Los siguientes servicios han sido considerados de forma recurrente para cumplir con los controles, subcontroles y tener una red madura respecto a seguridad informática y garantizar disponibilidad, confiabilidad y confidencialidad de los datos.

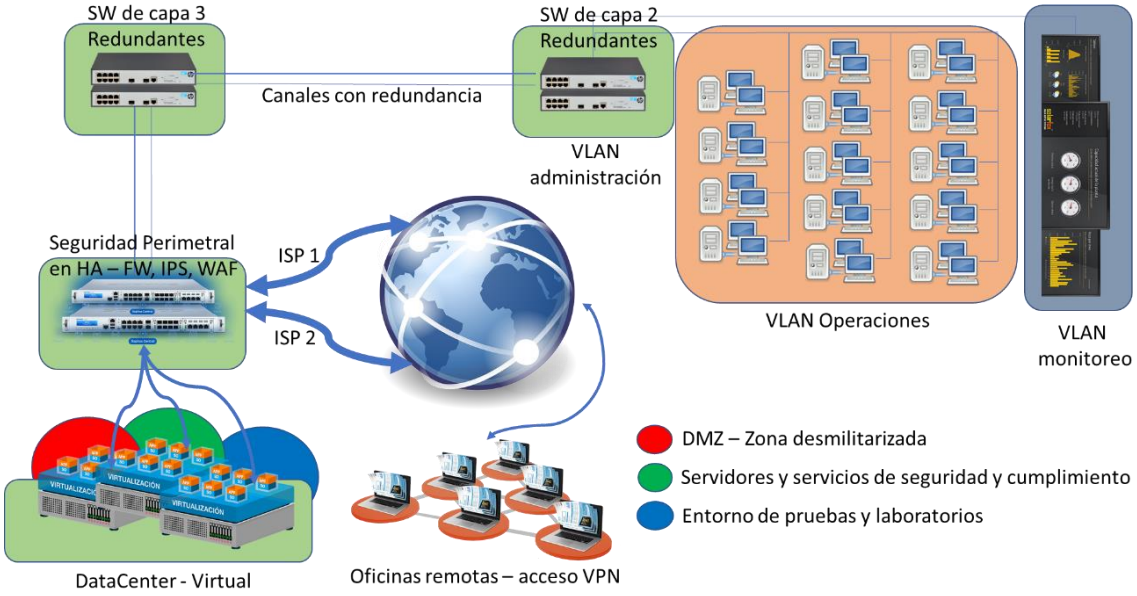


Figura. 4.3. Diseño

Fuente: Elaborado por el autor

En la tabla 4.3 se indica los puntos de conexión para la red de monitoreo, estaciones de trabajo, servidores y redes.

Tabla 4.3 Cableado estructurado

Puntos	Utilización	Característica de cableado	VLAN	Velocidad Mbps
mon1	monitoreo	UTP cat. 6/RJ45, TIA/EIA 568B	VLAN-TV1	1000 Mbps
mon2	monitoreo	UTP cat. 6/RJ45, TIA/EIA 568B	VLAN-TV2	1000 Mbps
mon3	monitoreo	UTP cat. 6/RJ45, TIA/EIA 568B	VLAN-TV3	1000 Mbps
mon4	monitoreo	UTP cat. 6/RJ45, TIA/EIA 568B	VLAN-TV4	1000 Mbps
mon5	monitoreo	UTP cat. 6/RJ45, TIA/EIA 568B	VLAN-TV5	1000 Mbps
mon6	monitoreo	UTP cat. 6/RJ45, TIA/EIA 568B	VLAN-TV6	1000 Mbps
pc1	operadores	UTP cat. 6/RJ45, TIA/EIA 568B	VLAN-PC1	1000 Mbps

pc2	operadores	UTP cat. 6/RJ45, TIA/EIA 568B	VLAN-PC2	1000 Mbps
pc3	operadores	UTP cat. 6/RJ45, TIA/EIA 568B	VLAN-PC3	1000 Mbps
pc4	operadores	UTP cat. 6/RJ45, TIA/EIA 568B	VLAN-PC4	1000 Mbps
pc5	operadores	UTP cat. 6/RJ45, TIA/EIA 568B	VLAN-PC5	1000 Mbps
pc6	operadores	UTP cat. 6/RJ45, TIA/EIA 568B	VLAN-PC6	1000 Mbps
pc7	operadores	UTP cat. 6/RJ45, TIA/EIA 568B	VLAN-PC7	1000 Mbps
pc8	operadores	UTP cat. 6/RJ45, TIA/EIA 568B	VLAN-PC8	1000 Mbps
pc9	operadores	UTP cat. 6/RJ45, TIA/EIA 568B	VLAN-PC9	1000 Mbps
pc10	operadores	UTP cat. 6/RJ45, TIA/EIA 568B	VLAN-PC10	1000 Mbps
pc11	operadores	UTP cat. 6/RJ45, TIA/EIA 568B	VLAN-PC11	1000 Mbps
pc12	operadores	UTP cat. 6/RJ45, TIA/EIA 568B	VLAN-PC12	1000 Mbps
serv1	ESXI 1	UTP cat. 6/RJ45, TIA/EIA 568B	VLAN-ESXI1	1000 Mbps
serv2	ESXI 2	UTP cat. 6/RJ45, TIA/EIA 568B	VLAN-ESXI2	1000 Mbps
serv 3	ESXI-pruebas	UTP cat. 6/RJ45, TIA/EIA 568B	VLAN-pruebas	1000 Mbps
net 1	Sophos XG	UTP cat. 6/RJ45, TIA/EIA 568B	VLAN-XG	1000 Mbps
net 2	sensor1 alienvault	UTP cat. 6/RJ45, TIA/EIA 568B	VLAN-sens1	1000 Mbps
net 3	sensor2 alienvault	UTP cat. 6/RJ45, TIA/EIA 568B	VLAN-sens2	1000 Mbps

Fuente: Elaborado por el autor

4.1.2.1 Diseño de cableado para los puntos de conexión

Se puede apreciar en la figura 4.4 la distribución de los puntos de red que fueron implementados, como se indica en la tabla 4.3, se aprecia el diagrama de conexión físico que actualmente tiene la red.

Se tiene también el detalle de los *patchpanels* que se utilizó y los equipos de conmutación, con su respectiva conexión física y redundancia.

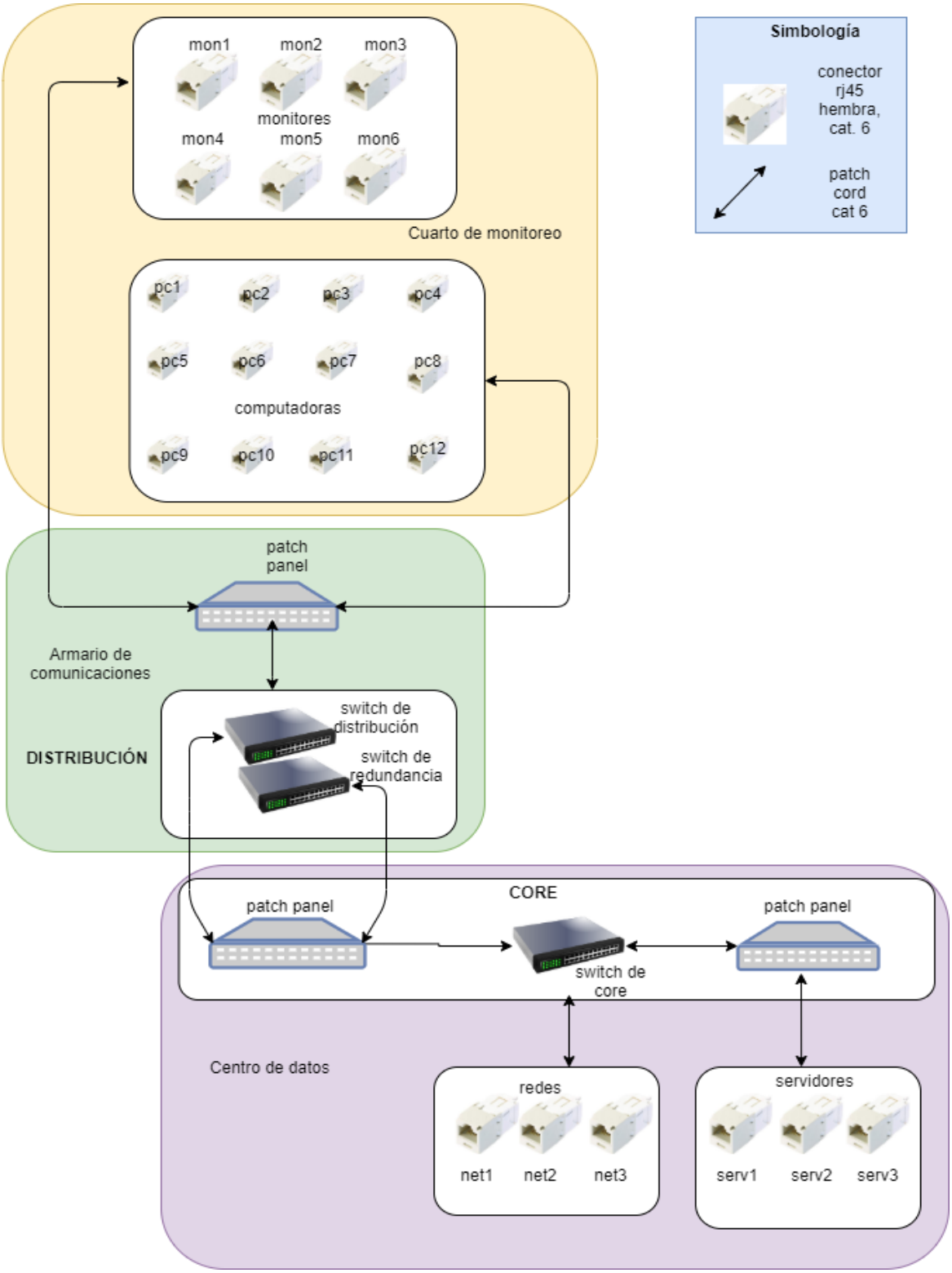


Figura. 4.4. Cableado estructurado

Fuente: Elaborado por el autor

4.1.2.2 Diseño para la red de monitoreo

En la figura 4.5 podemos apreciar el diagrama de conexión lógica del segmento asignado a los monitores, que consisten en pantallas que están empotradas en la pared, con conexión cableada para acceder y mostrar las principales plataformas de gestión que tienen los operadores.

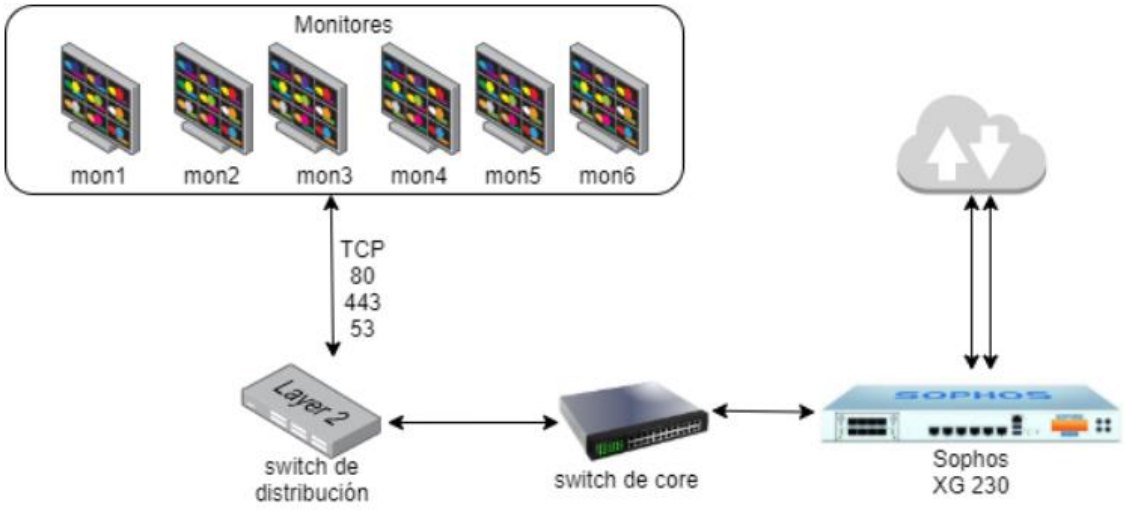


Figura. 4.5. Diseño de la red de monitoreo

Fuente: Elaborado por el autor

4.1.2.3 Diseño para la red de servidores

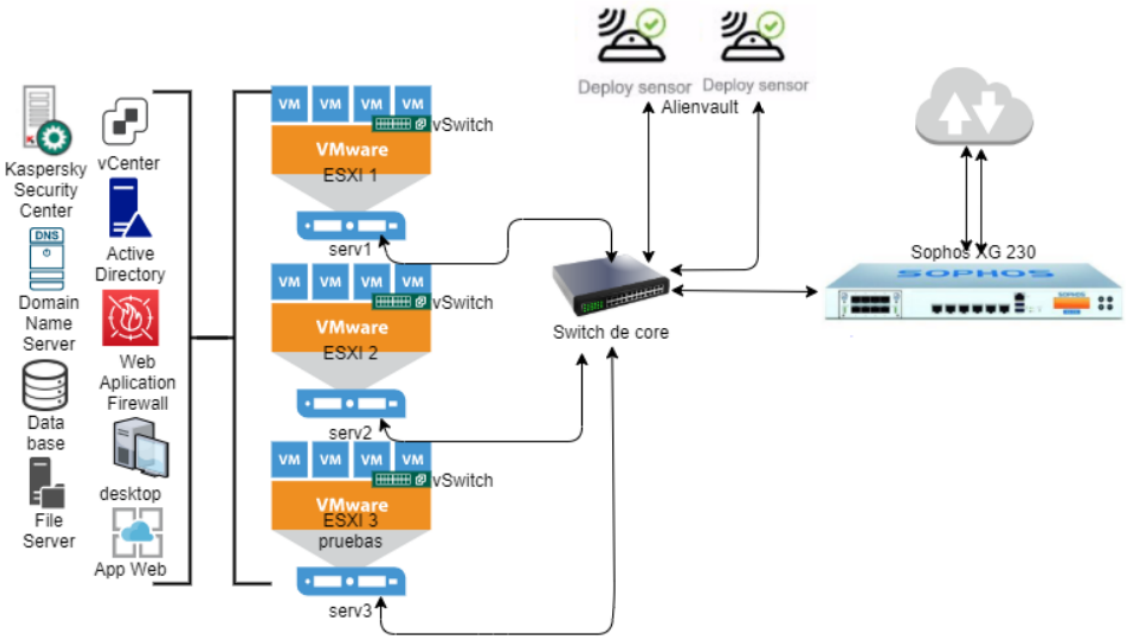


Figura. 4.6. Diseño de la red de servidores

Fuente: Elaborado por el autor

En la figura 4.6 podemos apreciar el diagrama de conexión lógica de los servidores. Están compuestos por 3 equipos físicos con VmWare para manejar virtualización, de estos 2 son para producción y uno para el ambiente pruebas. También en este segmento se considera la conexión del equipo de protección perimetral y los sensores de la plataforma de SIEM. La salida hacia internet cuenta con dos canales de proveedores distintos de 50 y 20 Mbps, respectivamente.

4.1.2.4 Diseño para la red de estaciones de trabajo

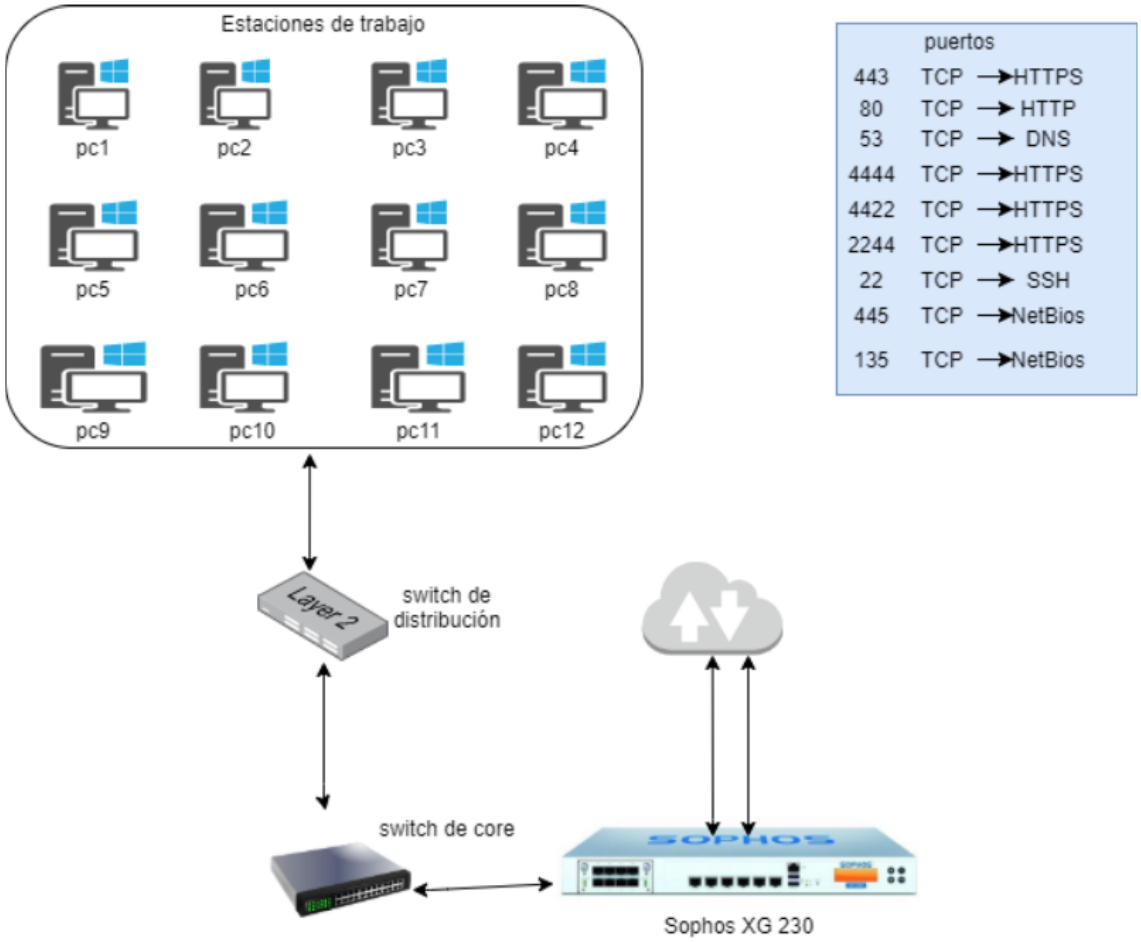


Figura. 4.7. Diseño para estaciones de trabajo

Fuente: Elaborado por el autor

En la figura 4.7 se puede observar el diseño lógico del segmento de estaciones de trabajo, los puertos de conexión y los equipos involucrados.

Durante la fase de instalación se ejecutan los siguientes servicios, son servicios profesionales, desarrollo de procedimientos y procesos:

- Consultoría de *hardening*

- Servicios asociados al endurecimiento de las configuraciones
- Procesos de *backup*
- Consultoría de clasificación de información
- Ingeniería social
- Capacitación de herramientas de seguridad
- Capacitaciones especializadas en seguridad
- Consultoría de EH

Los siguientes productos fueron adquiridos ya que cumplen con los controles y subcontroles que han sido aceptados para el diseño de esta red.

- AlienVault
- Sophos XG
- Sophos Endpoint
- WSUS
- Active Directory
- Sophos WAF
- One password
- Google authenticator
- Sophos Interept X
- Veracode

Los elementos necesarios de red adquiridos fueron:

- Cuatro conmutadores marca HP y DLINK
- Dos paneles de conexión para cableado
- Cableado estructurado para los puntos de red

Los elementos de consumo de red, como computadores, servidores y laptops (equipos de punto final) no se consideran dentro del diseño de red y la implementación. De modo que la operación propia de la red se considera por fuera del alcance de la implementación.

4.1.3 Diseño para los controles y subcontroles a ser implementados

El diseño lo conforma cada uno de los parámetros descritos en la tabla 4.4, la cual muestra a detalle el uso de los controles, el servicio y producto con su característica.

Cabe indicar que no se consideraron para la implementación todos los controles con un proyecto independiente ya que varios controles pueden ser atacados con un proyecto, porque

muchas soluciones comerciales tratan de abarcar varias brechas de seguridad, así como un control puede requerir más de un proyecto por los diversos subcontroles que tiene.

Tabla. 4.4. Diseño con los controles de seguridad

ID CONTROL	ID PROYECTO	Proyectos	Productos o servicios
C01	P01	Implementación de herramienta de inventario de *Hardware* y *Software*	ALIENVAULT
C01	P02	Implementación de control de acceso de infraestructura tecnológica	SOPHOS XG
C01	P03	Implementación de correlación de eventos	ALIENVAULT
C01	P04	Operación de Respuesta a incidentes de seguridad	SERVICIOS CSIRT
C02	P05	Implementación de seguridad de endpoint	SOPHOS ENDPOINT
C02	P17	Gestión de distribución de actualizaciones y parches de seguridad	WSUS
C03	P06	Gestionar protocolos de *hardening* y configuraciones seguras para endpoints y servidores	CONSULTORÍA DE HARDENING
C03	P07	Gestionar respaldos de sistema operativo, software de aplicaciones y los datos, incluidos en el procedimiento de copia de seguridad general de endpoints y servidores	PROCESOS DE BACKUP
C03	P08	Implementación de gestión centralizada de configuraciones y perfiles de usuario	ACTIVE DIRECTORY
C04	P09	Implementar un proceso de evaluación y remediación de vulnerabilidades periódico	ALIENVAULT
C04	P10	Implementación de herramientas de protección de aplicaciones y bases de datos	SOPHOS WAF
C05	P11	Gestión de contraseñas seguras	ONE PASSWORD
C05	P12	Implementar doble factor de autenticación para acceso a sistemas críticos	GOOGLE AUTHENTICATOR
C06	P13	Implementar un servidor NTP para asegurar la sincronía de registros de tiempo para correlación de eventos	ACTIVE DIRECTORY
C07	P14	Implementación de seguridad perimetral	SOPHOS XG
C08	P15	Implementación de protección anti-ataques persistentes avanzados o ataques dirigidos	SOPHOS INTEREPT X
C09	P16	Gestión de seguridad en red interna	SOPHOS ENDPOINT
C13	P18	Gestionar la política de clasificación de información y seguridad de información sensible	CONSULTORÍA DE CLASIFICACIÓN DE INFORMACIÓN
C13	P19	Cifrado de datos	SOPHOS ENDPOINT
C13	P20	Prevención de fugas de información	SOPHOS ENDPOINT
C14	P21	Implementación de control y protección de acceso a servidores de archivos o repositorios compartidos de información sensible	SOPHOS ENDPOINT
C17	P23	Plan de formación y concientización	INGENIERÍA SOCIAL
C17	P24	Plan de formación en seguridad informática	CAPACITACIÓN DE HERRAMIENTAS DE

			SEGURIDAD CAPACITACIONES ESPECIALIZADAS EN SEGURIDAD
C18	P25	Protección de aplicaciones	SOPHOS XG
C18	P26	Evaluación de vulnerabilidades en código fuente	VERACODE
C18	P27	Arquitectura de desarrollo seguro	VERACODE
C20	P28	Servicios de Ethical Hacking	CONSULTORÍA DE EH

Fuente: Elaborado por el autor

Para esto es importante entender cómo se calificará cada control, estos deben ser evaluados y calificados de la siguiente manera:

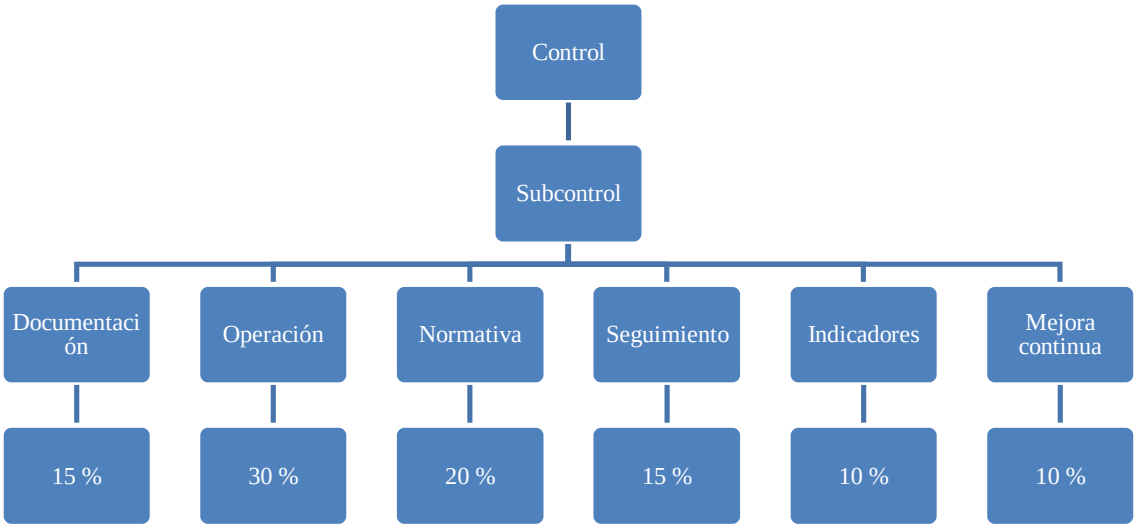


Figura. 4.8. Puntuación de los controles.

Fuente: Elaborado por el autor

Cada control cuenta con un número “n” de subcontroles los cuales pueden tener 6 atributos, mismo que para la calificación tienen un porcentaje de peso, de esta manera, si el control está implementado correctamente y en mejora continua siempre, alcanza un 100 %. Este 100% indicará que el control, en la escala del 0 al 5, alcanza su máximo valor, cada subcontrol aporta de manera igualitaria al control principal, de los 20 descritos.

Para aplicar un subcontrol se debe realizar trabajo operativo y consultivo, el trabajo operativo se refiere a todas las configuraciones o implementaciones de sistemas y soluciones que permitan cumplirlo y medirlo. La parte consultiva se refiere al desarrollo documental y procedimental asociado al subcontrol. Considerando una implementación de un subcontrol que no requiere la adquisición de soluciones sino la aplicación directa se tiene como ejemplo:

Subcontrol: 16.8 Supervise los intentos de acceder a cuentas desactivadas a través del registro de auditoría.

Para cumplir adecuadamente este subcontrol se debe:

- Documentar
- Operar
- Normar
- Dar seguimiento
- Medir con indicadores
- Mantener en mejora continua

El trabajo de documentación toma en tiempo efectivo de 1,5 horas, la parte de operación toma 3 horas, la parte de normar y socializar toma 2 horas, el desarrollo del procedimiento para dar seguimiento al subcontrol puede tomar un promedio de 1,5 horas, la definición de indicadores debe tomar un tiempo de 1 hora, la definición de cómo mantener una mejora continua debe tomar 1 hora.

Con este ejemplo podemos ver que, para un cálculo sencillo de trabajo efectivo de 10 horas, el 15% se invierte en documentar, el 30 % en definir como operar, el 20% en como normar y socializar el subcontrol, la definición de cómo dar seguimiento toma un 15%, el desarrollo de indicadores un 10% y finalmente la estrategia de cómo mantener en mejora continua otro 10%.

Esta tarea se repite con 8 subcontroles de muestra con similar distribución, por lo que se asigna los pesos y parámetros promedio de evaluación como se indica en la tabla 4.5:

Tabla. 4.5. Parámetros de evaluación

Atributo	Descripción	Peso de evaluación
Documentación	Registro actualizado de la información del control que al menos incluye: Responsables, Configuración/Procedimiento de gestión del control, Método de auditoría de cumplimiento e Indicadores.	15%
Operación	Facilidades del control implementadas y en operación (Activo/Herramienta/Proceso)	30%
Normativa	Política documentada y aprobada por la organización que rige al control y responde a las necesidades de seguridad de información de la organización	20%
Seguimiento	Facilidades de monitoreo del control implementadas y en operación, así como el mecanismo de identificación de una alarma de seguridad y un proceso de respuesta frente a la acción de una amenaza	15%
Indicadores	Medición periódica de la efectividad del control para cumplir su propósito de seguridad de información	10%
Mejora Continua	Plan en ejecución de mejoras a los controles, enfocada en una optimización de indicadores o de cumplimiento de las necesidades de seguridad de información de la organización	10%

Fuente: Elaborado por el autor

La tabla 4.6 muestra la descripción de cada atributo, este debe ser calificado del 0 al 5, 6 en caso de no ser aplicable a la organización o no haber sido aceptado por esta, en cuyo caso, ese subcontrol pasará a tener el valor de 5, el más alto para no afectar a la evaluación final.

Tabla. 4.6. Descripción por atributos

0. No existente	Control inexistente
1. Inicial	"No Confiable- Ambiente impredecible donde las organizaciones no tienen actividades de control y no están diseñadas". (Cuna, 2018).
2. Repetible	Informal- "Las actividades de control existen, pero no se ponen en práctica. Los controles dependen básicamente de las personas. No hay un entrenamiento formal ni comunicación de las actividades de control". (Cuna, 2018).
3. Definido	Estandarizado- "Las actividades de control existen y están diseñadas, han sido documentadas y comunicadas a los empleados, las desviaciones de las actividades de control probablemente no se detecten". (Cuna, 2018).
4. Gestionado	Monitoreado- "Se utilizan herramientas en una forma limitada para soportar las actividades de control". (Cuna, 2018).
5. Optimizado	"Es una estructura integrada de control interno con un monitoreo en tiempo real por la gerencia, así como mejoras continuas-auto control, se encuentran cambios más rápidos al momento de detectar errores en los manejos de las actividades o en las personas". (Cuna, 2018).
6. No aplicable	Justificación aceptable inherente al negocio o a la estrategia de gestión

Fuente: Elaborado por el autor

4.2 Implementación

La implementación de la red se realizó acorde al planteamiento, para esto la empresa auspiciante realizó obra civil reemplazando un espacio de 2 oficinas por la sala de monitoreo, la figura 4.9 nos permite observar la oficina antigua.

Oficinas antiguas

Figura. 4.9. Oficina uno, que se reemplazó por la sala de monitoreo

Fuente: Elaborado por el autor

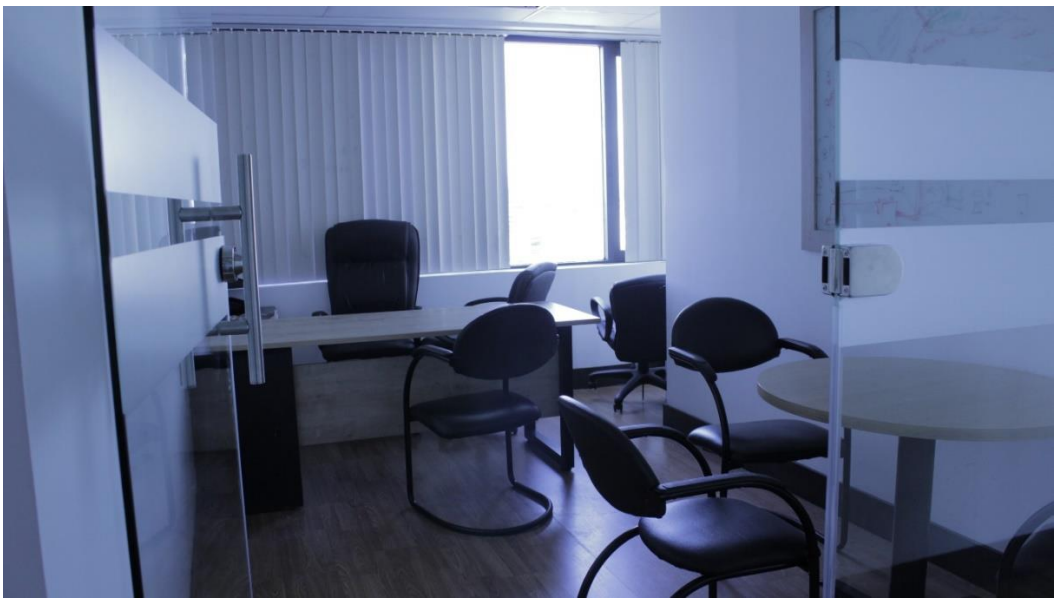


Figura. 4.10. Oficina dos, que se reemplazó por la sala de monitoreo

Fuente: Elaborado por el autor

Sala de monitoreo nueva

La sala de monitoreo reemplazó ambas oficinas y para esta sala se realizó la red con los controles de seguridad por el propósito que tiene.

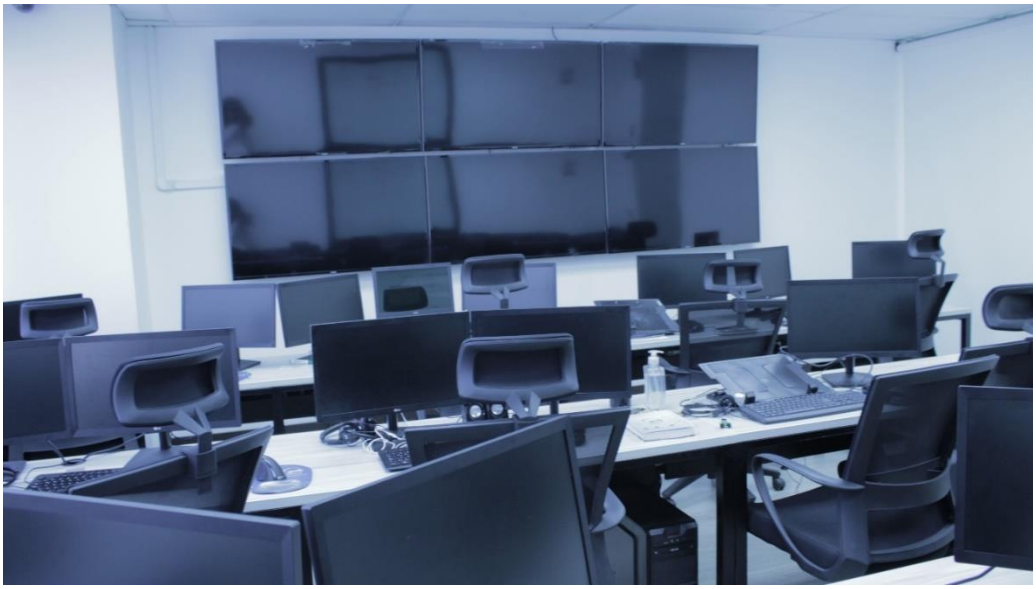


Figura. 4.11. Sala de monitoreo actual

Fuente: Elaborado por el autor

Los puntos de red para las estaciones de trabajo, con sus respectivas etiquetas, se ubican en la parte inferior de las mesas, especialmente diseñadas para este propósito como se indica en la figura 4.12.

Figura. 4.12. Puntos de red de las estaciones de trabajo

Fuente: Elaborado por el autor

La figura 4.13 indica cada estación de trabajo, cada una cuenta con un punto de red y es habilitada para trabajar con una laptop o PC y dos monitores.

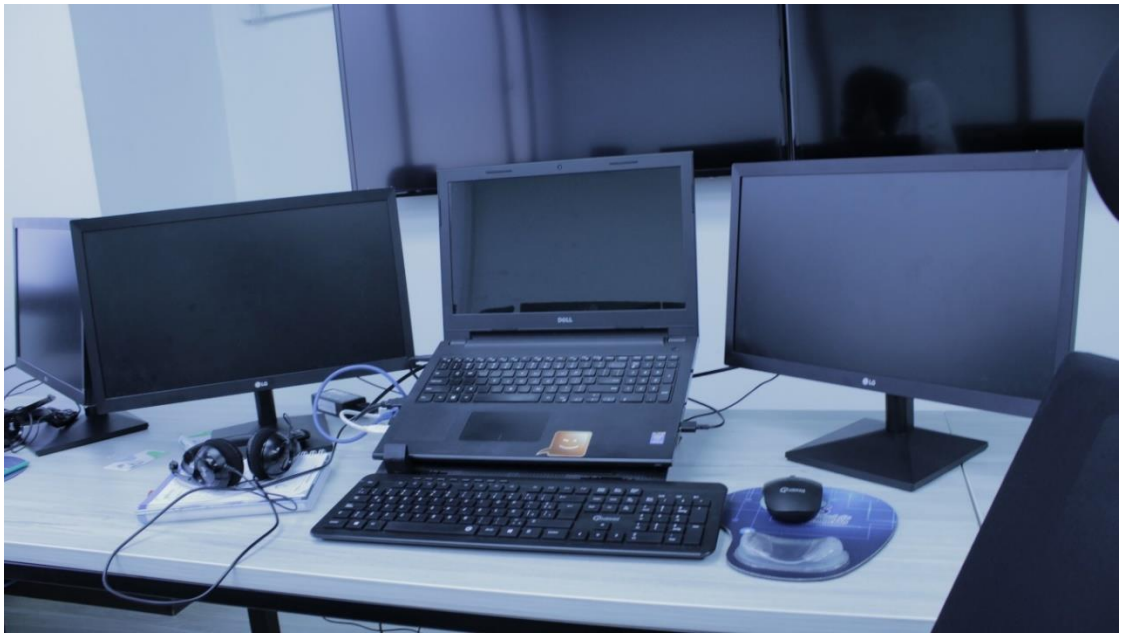


Figura. 4.13. Estación de trabajo real actual

Fuente: Elaborado por el autor

El segmento de monitores se encuentra en pared, los puntos de red están atrás de los monitores, como indica la figura 4.14.

Figura. 4.14. Puntos de red para monitores

Fuente: Elaborado por el autor

Estos equipos, monitores y de usuarios van al armario de comunicaciones que se muestra en la figura 4.15.

Figura. 4.15. Armario de comunicaciones

Fuente: Elaborado por el autor

Finalmente, las comunicaciones se dirigen al centro de datos como se puede observar en la figura 4.16.

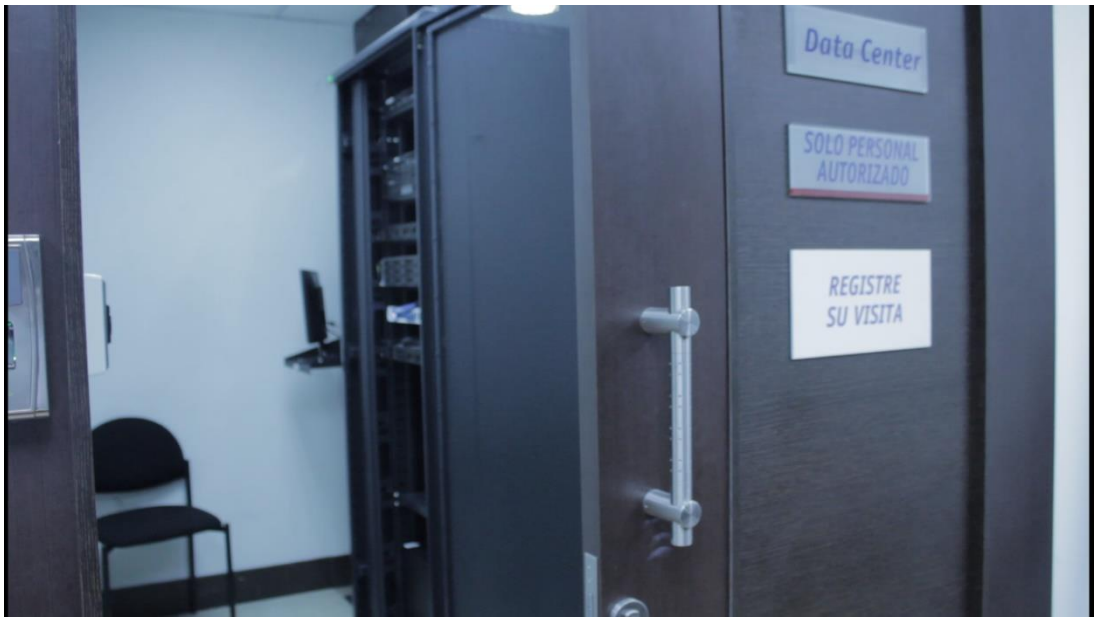


Figura. 4.16. Centro de datos

Fuente: Elaborado por el autor

En el centro de datos podemos observar los equipos implementados, en la figura 4.17 se puede apreciar el patch panel del centro de datos, el switch de core y el equipo de protección perimetral Sophos XG.

Figura. 4.17. *Patch panel, switch de core* y Sophos XG

Fuente: Elaborado por el autor

4.2.1 Implementación de AlienVault

Se realiza la implementación de los sensores de AlienVault, que reportan a una consola central, AlienVault AnyWhere, el licenciamiento es un 250GB estándar 30.

En la figura 4.18 se indica el sensor 1

Figura. 4.18. Sensor 1 de AlienVault

Fuente: Elaborado por el autor

La figura 4.19 indica el sensor 2

Figura. 4.19. Sensor 2 de AlienVault

Fuente: Elaborado por el autor

Posterior a la implementación física se realiza la conexión lógica hacia la consola de administración, la figura 4.20 indica la conexión lógica.

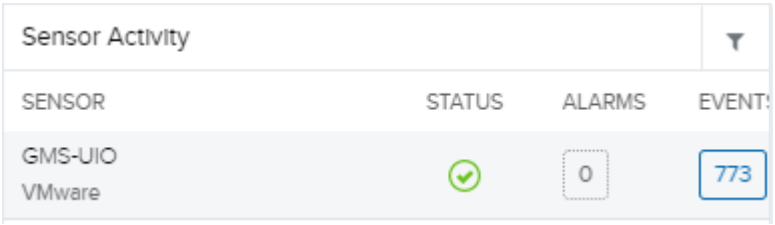


Figura. 4.20. Verificación de actividad del sensor

Fuente: Elaborado por el autor

La consola de administración permite la gestión de los controles como se lo había propuesto y esta se visualiza en la figura 4.21.

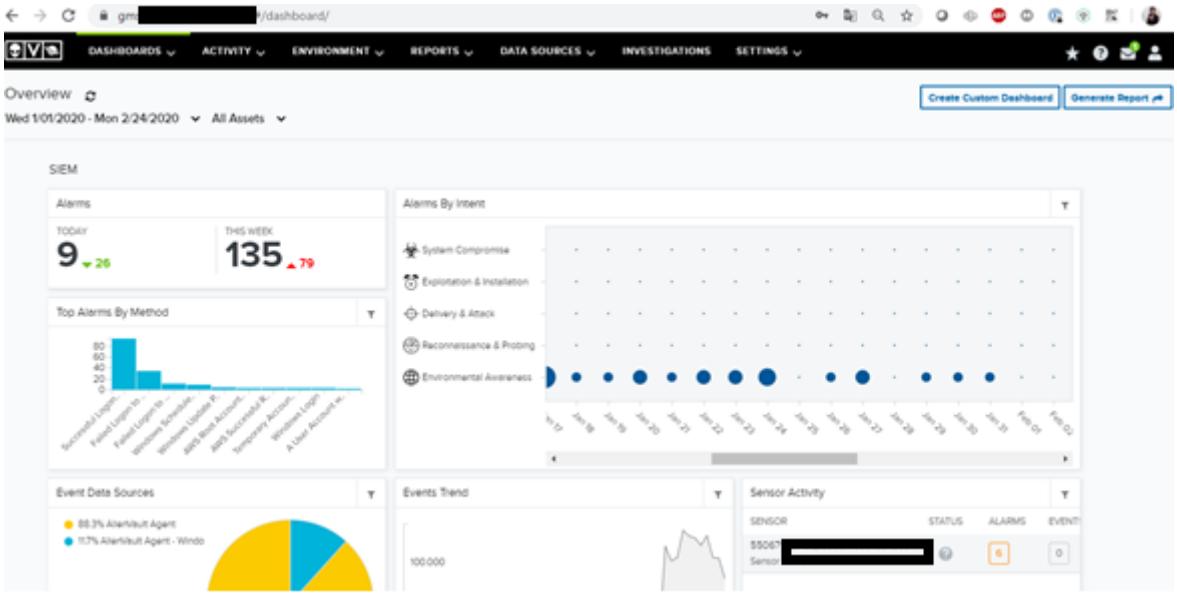


Figura. 4.21. Gestión de controles

Fuente: Elaborado por el autor

4.2.2 Implementación de Sophos Intercept X

En los equipos de usuario se implementa la solución en las estaciones de trabajo y servidores con un agente como se puede apreciar en la figura 4.22a

Figura. 4.22a. Sophos Intercept X instalada

Fuente: Elaborado por el autor

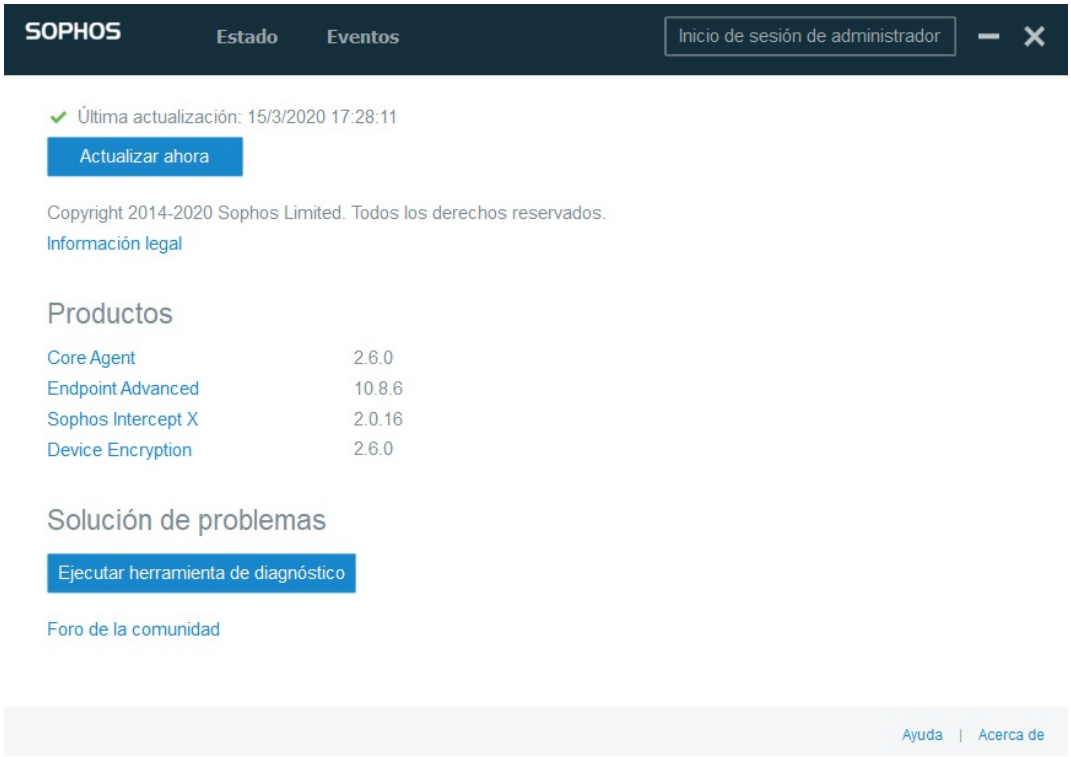


Figura. 4. 23b. Módulos instalados para su administración centralizada

Fuente: Elaborado por el autor

4.2.3 Implementación de Sophos DLP

En los equipos de usuario se implementa la solución en las estaciones de trabajo y servidores con un agente como se puede apreciar en la figura 4.22b

4.2.4 Implementación de Sophos Encription

En los equipos de usuario se implementa la solución en las estaciones de trabajo y servidores con un agente como se puede apreciar en la figura 4.23

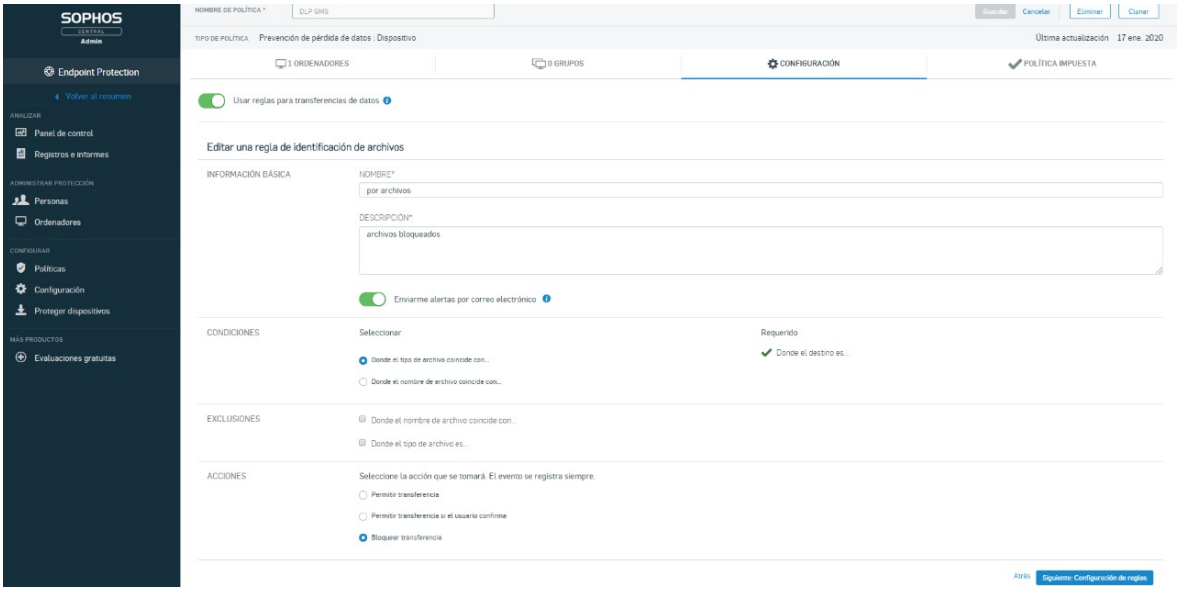


Figura. 4.24. Consola de gestión de la plataforma de DLP Sophos

Fuente: Elaborado por el autor

4.2.5 Implementación de WSUS

Para el uso de WSUS se realiza la implementación de un servidor de *Kaspersky Security Center* (KSC), el cuál es centralizado y el software permite la administración de todos los nodos desde la plataforma, también permite realizar tareas remotas de búsqueda de vulnerabilidades y el envío de todos los parches faltantes en los equipos.

Equipo servidor Windows 2012 con 8 GB en Ram y 100 GB de espacio en disco.

Se indica en la figura 4.24 el resultado de vulnerabilidades y parches.

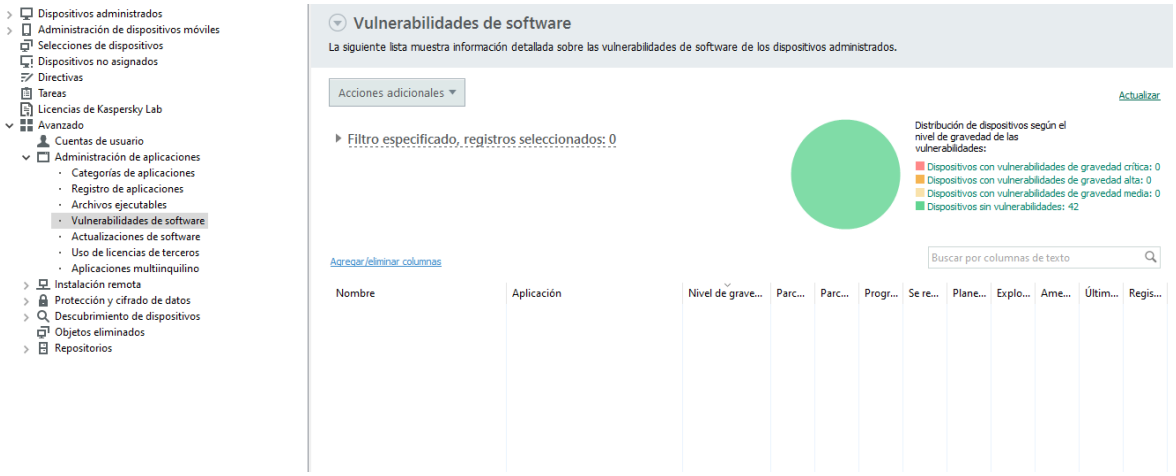


Figura. 4.25. Consola de gestión de vulnerabilidades, parches y actualización de sistemas

Fuente: Elaborado por el autor

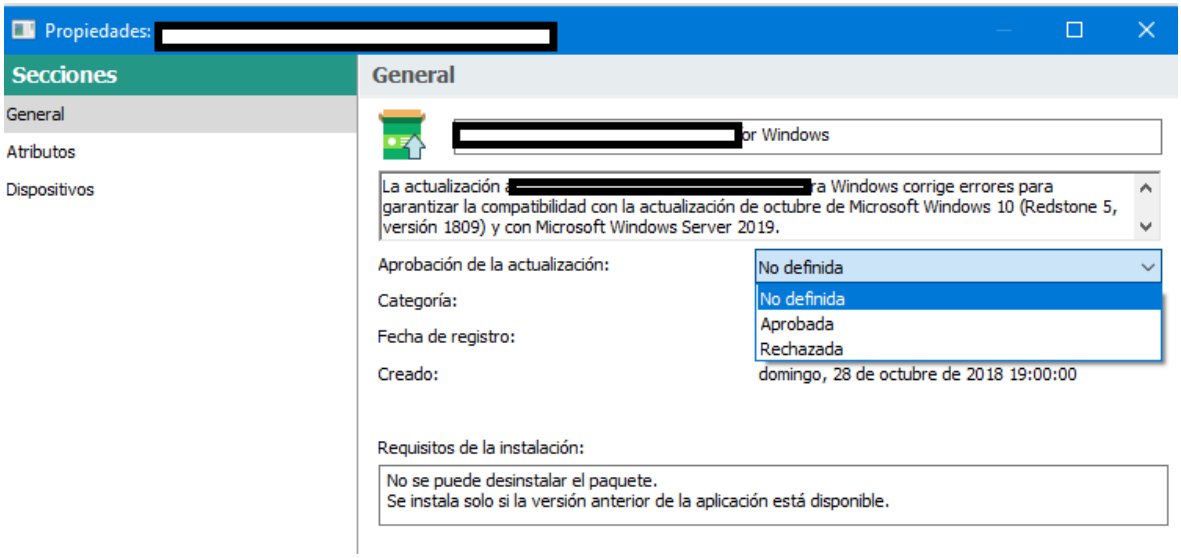


Figura. 4.26. configuración de la remediación de vulnerabilidades, parches y actualización de sistemas y aplicaciones

Fuente: Elaborado por el autor

4.2.6 Implementación de Active Directory

Se procede con la instalación de un Windows server 2016 como indica la figura 4.26, la configuración del dominio gxxxxxxxxxad.com y el registro de los activos que pertenecen a esta red. Y la consola en operación que indica la figura 4.27.

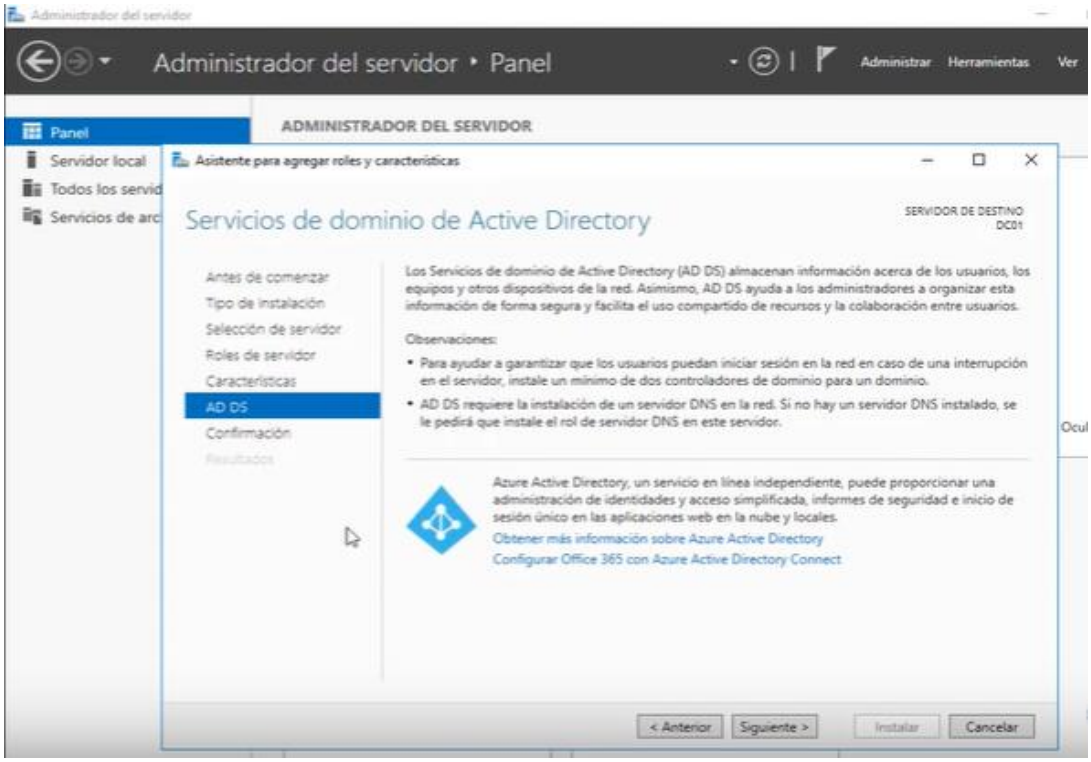


Figura. 4.27. Instalación y activación de los servicios de directorio activo

Fuente: Elaborado por el autor

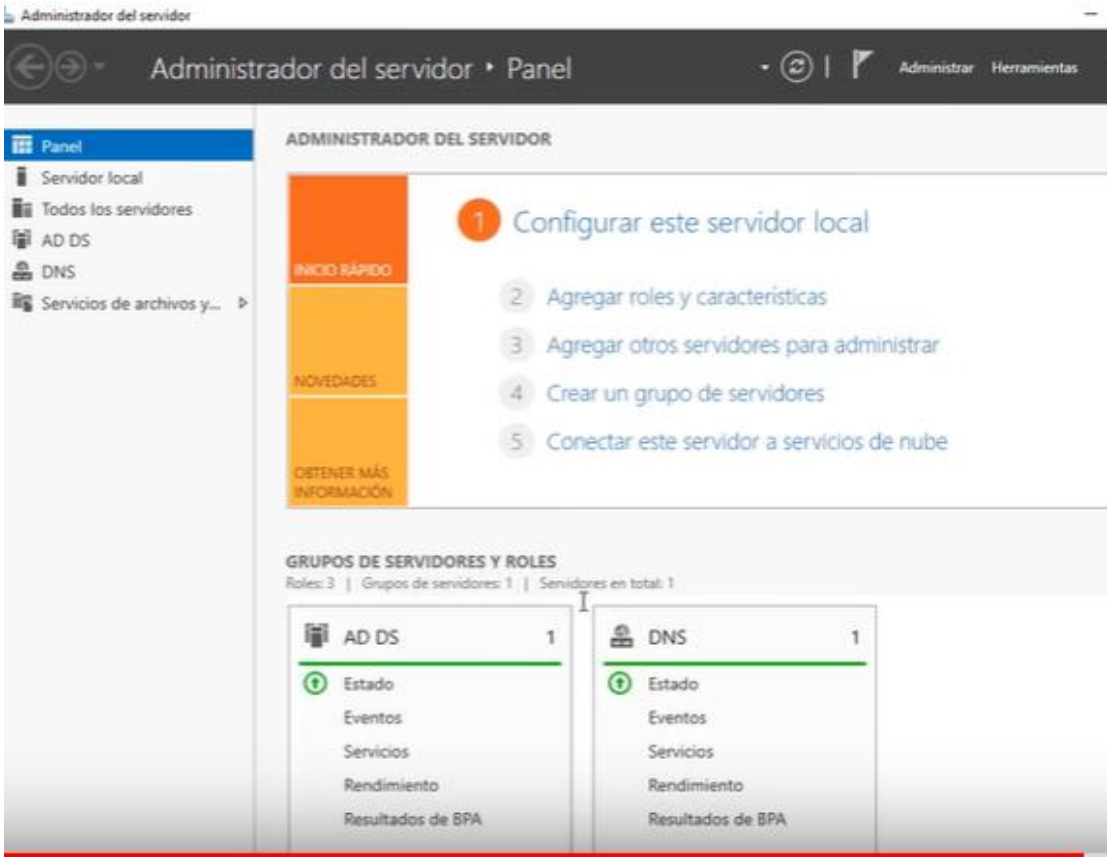


Figura. 4.28. Consola operativa del servidor de dominio

Fuente: Elaborado por el autor

4.2.7 Implementación de Sophos WAF

En la figura 4.28 se aprecia la implementación de la consola de gestión de la funcionalidad de WAF de Sophos, se activan 3 reglas de seguridad para la aplicación web, como se muestra en la figura:

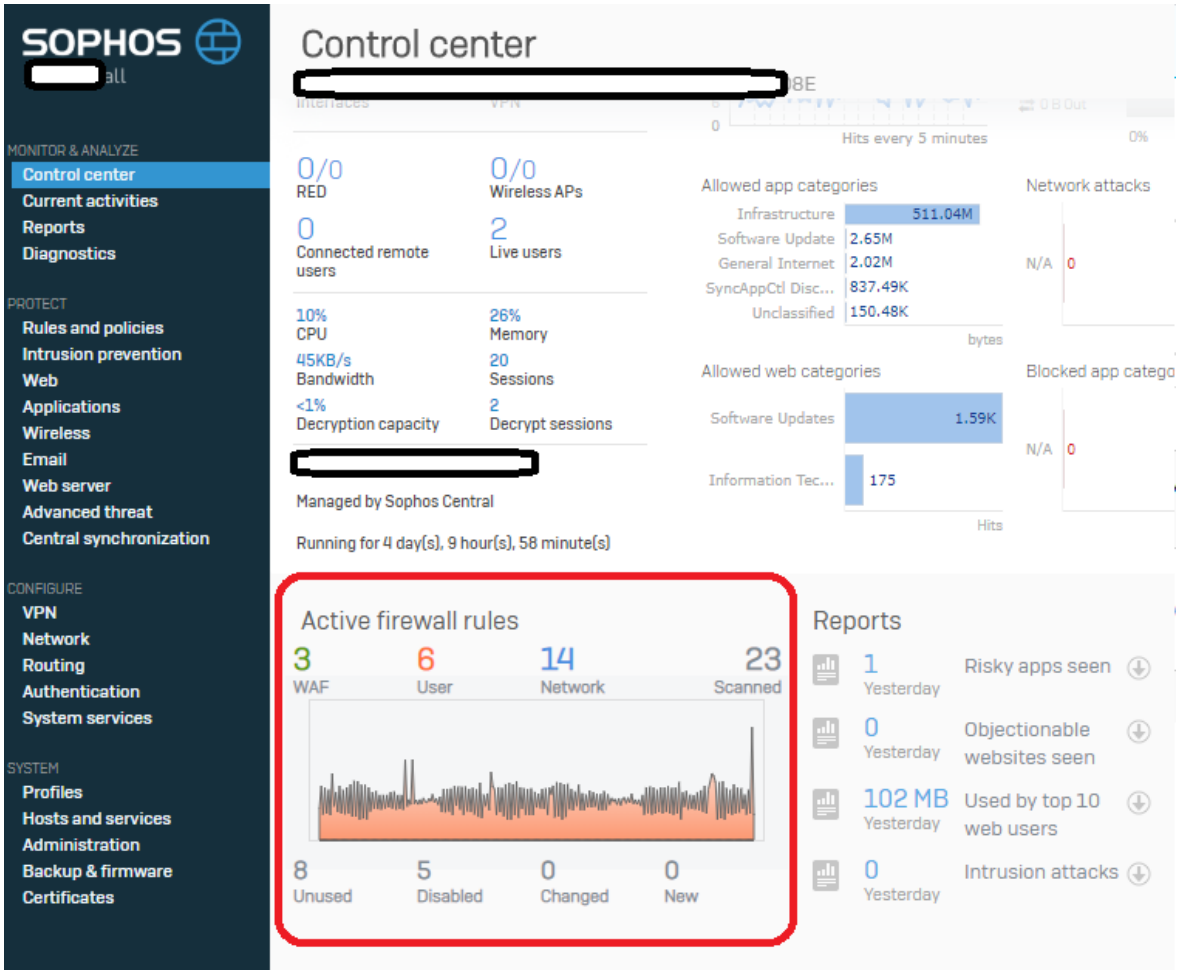


Figura. 4.29. consola de gestión de Sophos, políticas de WAF activas

Fuente: Elaborado por el autor

4.2.8 Implementación de One Password

Se implementa la solución en los equipos y navegadores de los usuarios para gestionar las contraseñas y accesos de usuarios privilegiados de forma centralizada y poder auditar el uso, también para asignar o revocar permisos, la figura 4.29 indica la implementación.

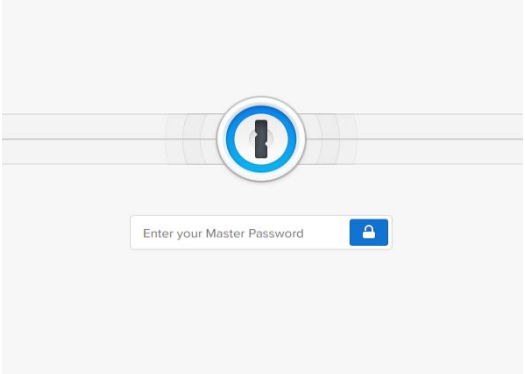


Figura. 4.30. *Login* principal de la consola de onepassword

Fuente: Elaborado por el autor

La figura 4.30 indica el *dashboard* con las configuraciones para la gestión de usuarios y credenciales implementado

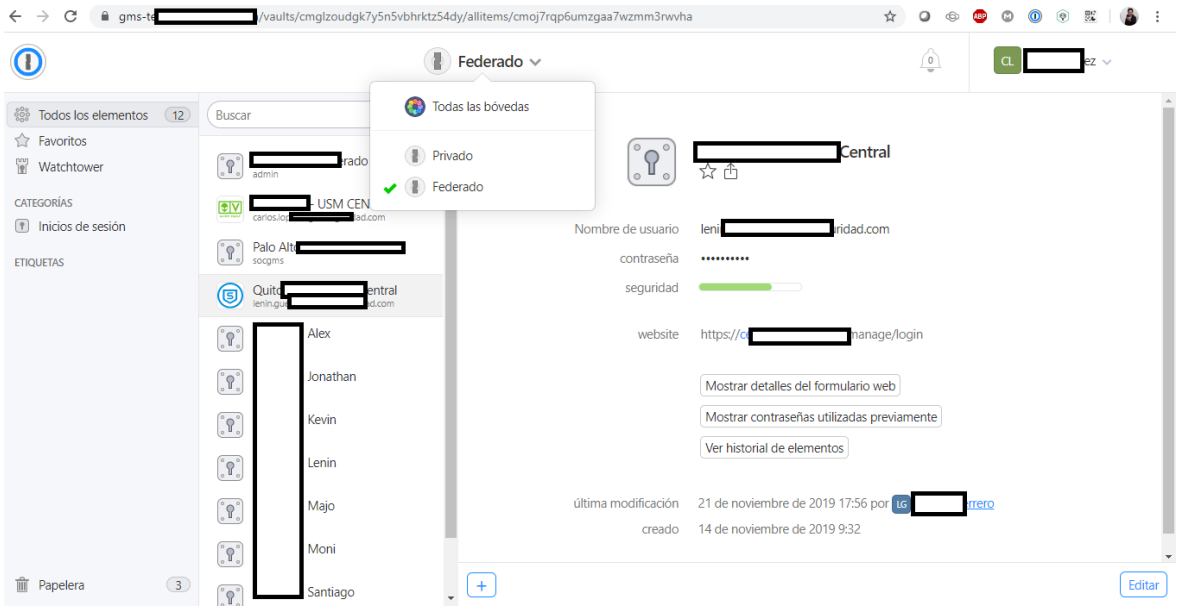


Figura. 4.31. Consola de gestión de one password

Fuente: Elaborado por el autor

4.2.9 Implementación de Google Authenticator

Como indica la figura 4.31 se implementa en los servidores solicitados (debian)

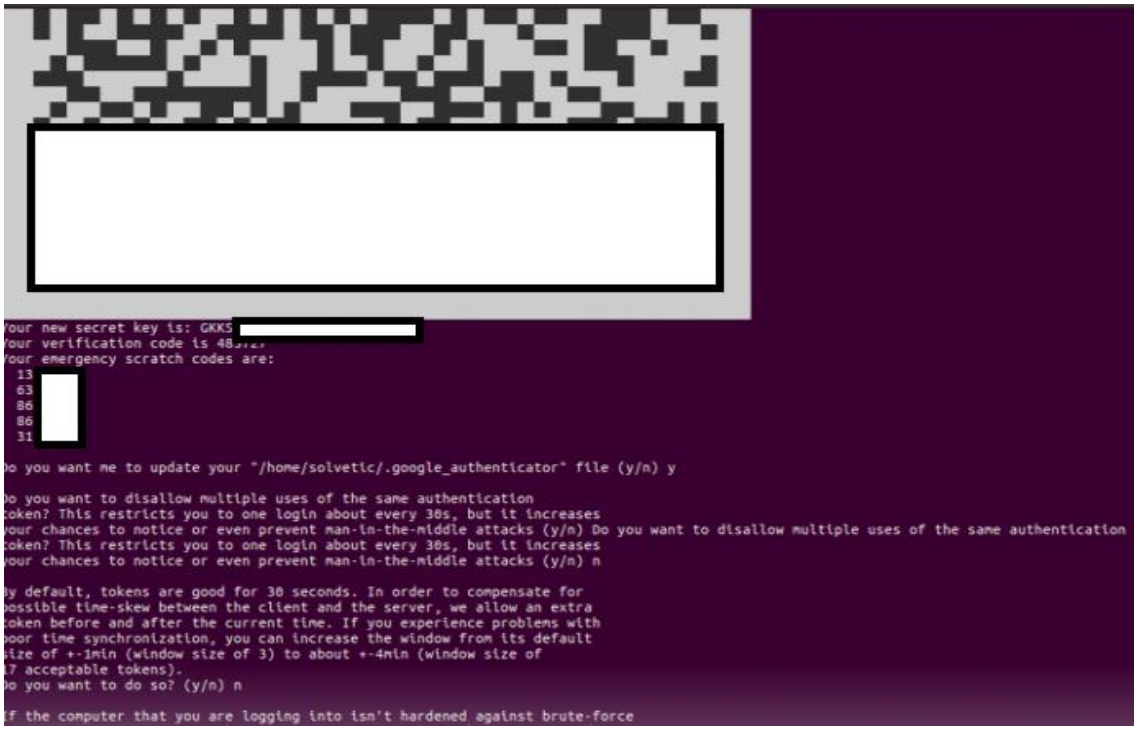


Figura. 4.32. Instalación de la plataforma de doble factor de autenticación

Fuente: Elaborado por el autor

La figura 4.32 indica cómo opera desde el celular una vez que se registra el doble factor de autenticación.

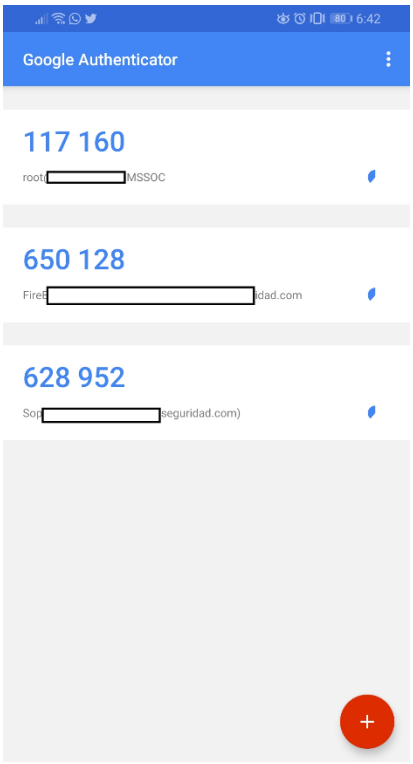


Figura. 4.33. Operación del doble factor de autenticación

Fuente: Elaborado por el autor

4.2.10 Implementación de Veracode

Al ser una plataforma SaaS, esta solución únicamente se activa en línea y se tiene acceso, a continuación, en la figura 4.33 encontramos los accesos y la configuración actual. También el resultado de los escaneos realizados.

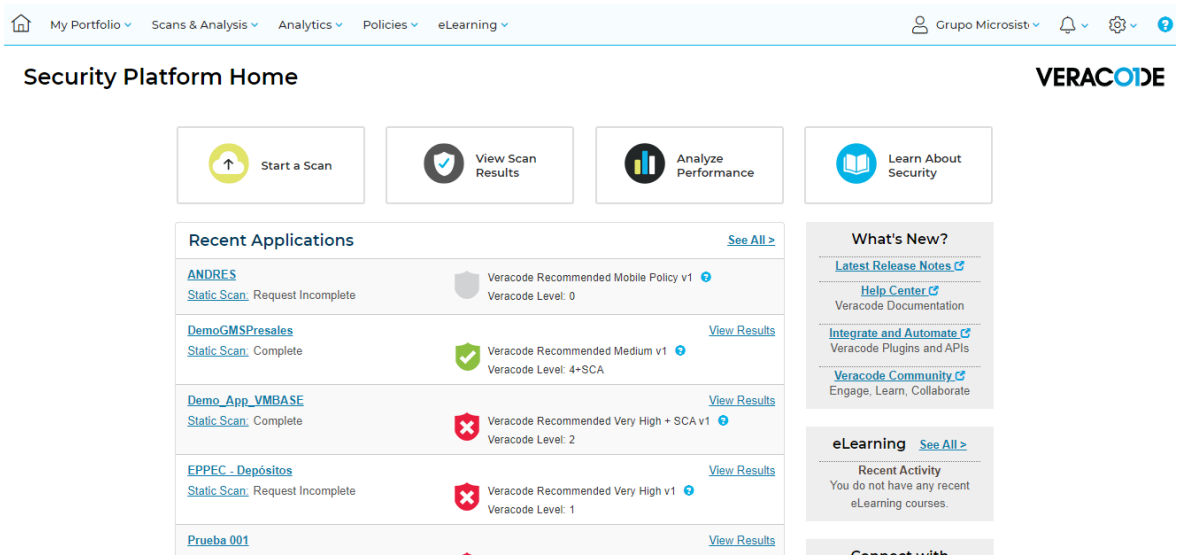


Figura. 4.34. Consola de administración de Veracode

Fuente: Elaborado por el autor

4.2.11 Implementación de Sophos XG

Figura. 4.35. Implementación de Sophos XG en el rack del centro de datos

Fuente: Elaborado por el autor

La figura 4.34 muestra la implementación del equipo 4.34, a continuación, se detalla las configuraciones principales de cada uno de los módulos configurados en el equipo Sophos para la implementación.

Por motivos de seguridad y confidencialidad de la empresa no se puede dar visibilidad a las direcciones de red y direccionamientos ya que son equipos puestos en producción.

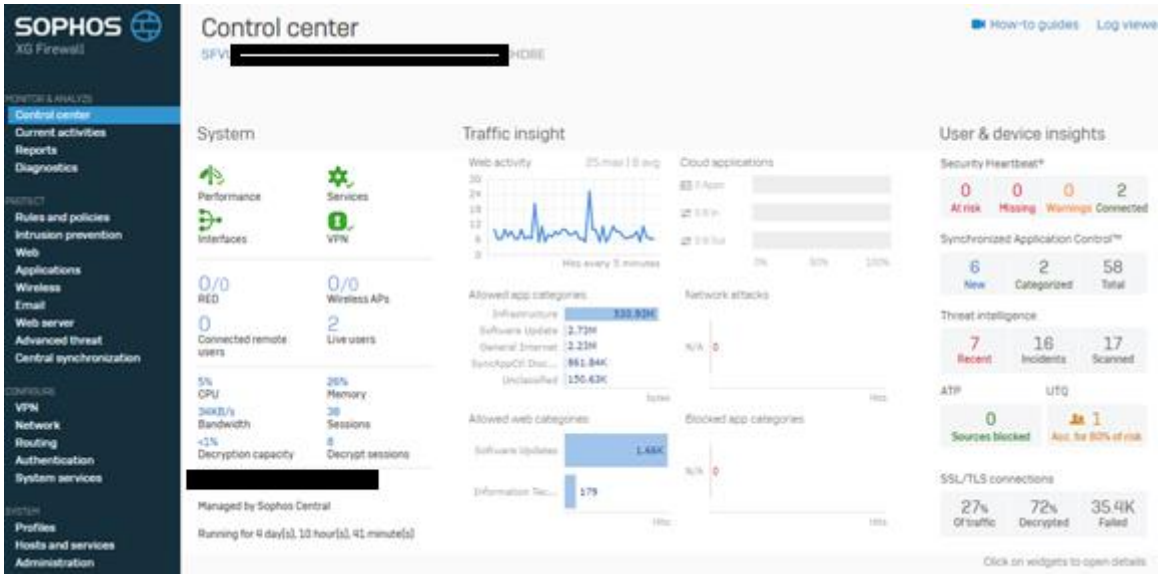


Figura. 4.36. Consola de gestión de firewall Sophos XG

Fuente: Elaborado por el autor

4.2.11.1 Firewall

Se crean reglas que van a permitir la navegación de las redes LAN y DMZ hacia internet y visualización de las redes entre sí.

4.2.11.2 Reglas de Firewall

Se crean reglas de Firewall para permitir el tráfico entre zonas LAN y DMZ y WAN.

En la figura 4.36 se coloca la regla LAN-DMZ para tener la salida al exterior con seguridad y conectividad para cualquier servicio, esta queda habilitada.

Figura. 4.37. Regla para visualizar la Red DMZ con la red LAN

En la figura 4.37 se puede observar la creación de una regla en el Sophos de firewall que permite salida a internet de la DMZ, se considera que la regla tiene la configuración de seguridad y conectividad desde la WAN.

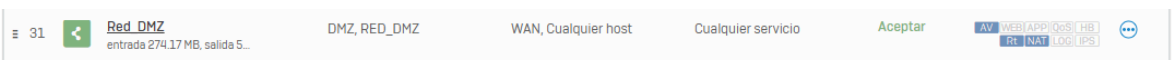


Figura. 4.38. Regla para permitir salida a internet de la red DMZ

En la figura 4.38 se permite la salida a internet a la red LAN con el fin de tener navegación y evaluar los controles de seguridad, como parámetros principales para la

creación de esta regla. De no cumplir las alertas serán llevadas desde el Sophos XG al Alienvault mediante la sincronización respectiva como correlacionador de eventos.

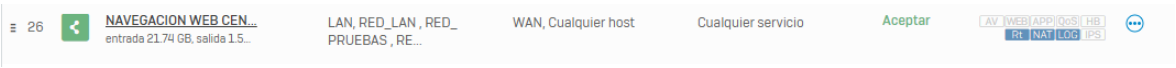


Figura. 4.39. Regla para permitir salida a internet a las redes LAN

4.2.11.3 Distribución VLAN

Se crean las siguientes VLAN como proceso de segmentación para la red del SOC.

En la figura 4.39 se realiza la segmentación de la red, de esta manera se hace uso de las VLAN, como primer paso para la red de servidores y se considera la asignación de IP estáticas.

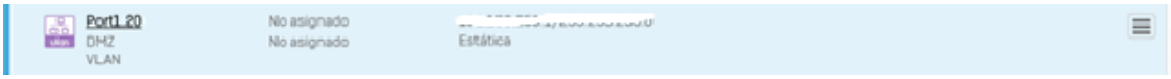


Figura. 4.40. VLAN destinada para red de Servidores

En la figura 4.40 se indica una VLAN de pruebas con dirección estática para evaluar las conexiones salientes.

Figura. 4.41. VLAN destinada para red de pruebas

En la figura 4.41 se crea la segmentación para la red de acceso a los biométricos y televisores que utiliza el SOC en funcionamiento 24/7 para la visibilidad de alertas por cualquier motivo de ataque o cambios sin autorización, este direccionamiento es estático y debe considerarse como uno de los principales ya que tiene sincronización con cada uno de los correlacionadores y la visibilidad de la información que estos entregan.

Figura. 4.42. VLAN destinada para red de televisores y acceso biométrico

En la figura 4.42 se muestra la segmentación de la VLAN para los operadores esto con el fin de un acceso seguro y confiable a cada aplicación o servicio recibido o entregado.

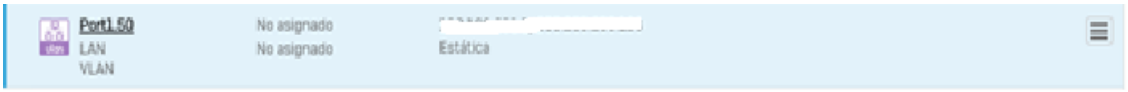


Figura. 4.43. VLAN destinada para la red de los operadores

4.2.11.4 Creación de DHCP y reversa de direcciones IP

Se crean los siguientes servidores DHCP para reserva de direcciones IP por MAC en las

diferentes redes.

Figura. 4.44. Creación de servidores DHCP para las diferentes VLAN y reserva de direcciones IP

En la figura 4.44 se puede observar la reserva de direcciones para los televisores con el fin de evitar sobrelapar direcciones esto de acuerdo con el uso de controles de seguridad.

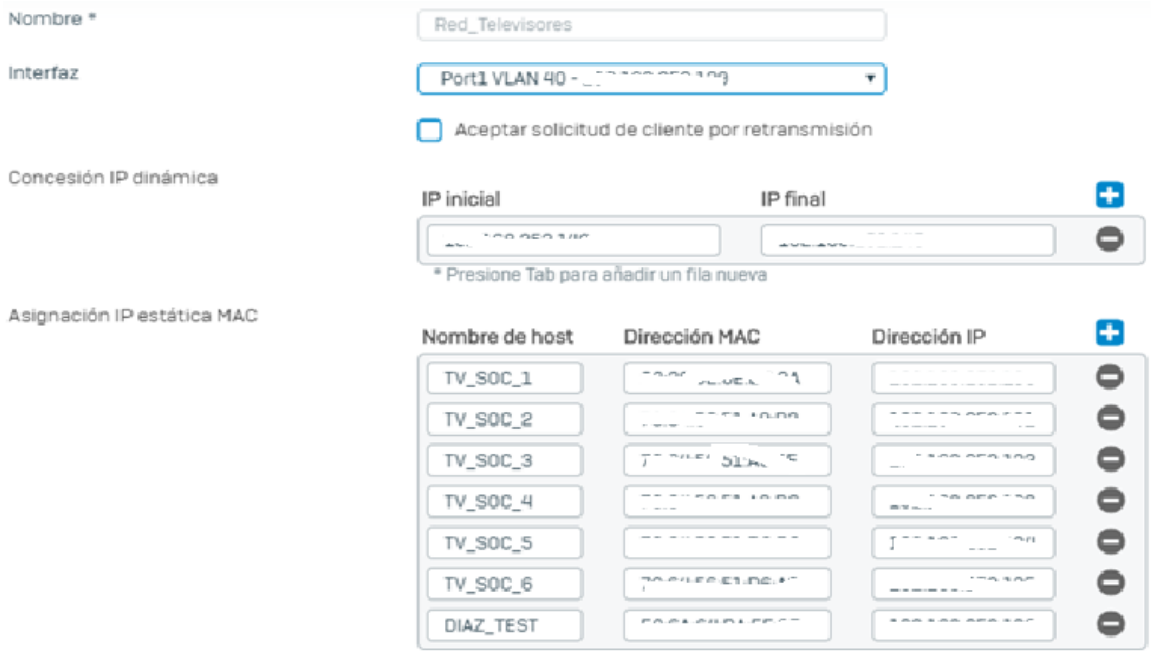


Figura. 4.45. Reserva direcciones IP en red de Televisores

En la figura 4.45 se muestra las configuraciones de la red de servidores los campos permiten configurar una concesión dinámica de IP en un segmento determinado y la asignación IP estática MAC.

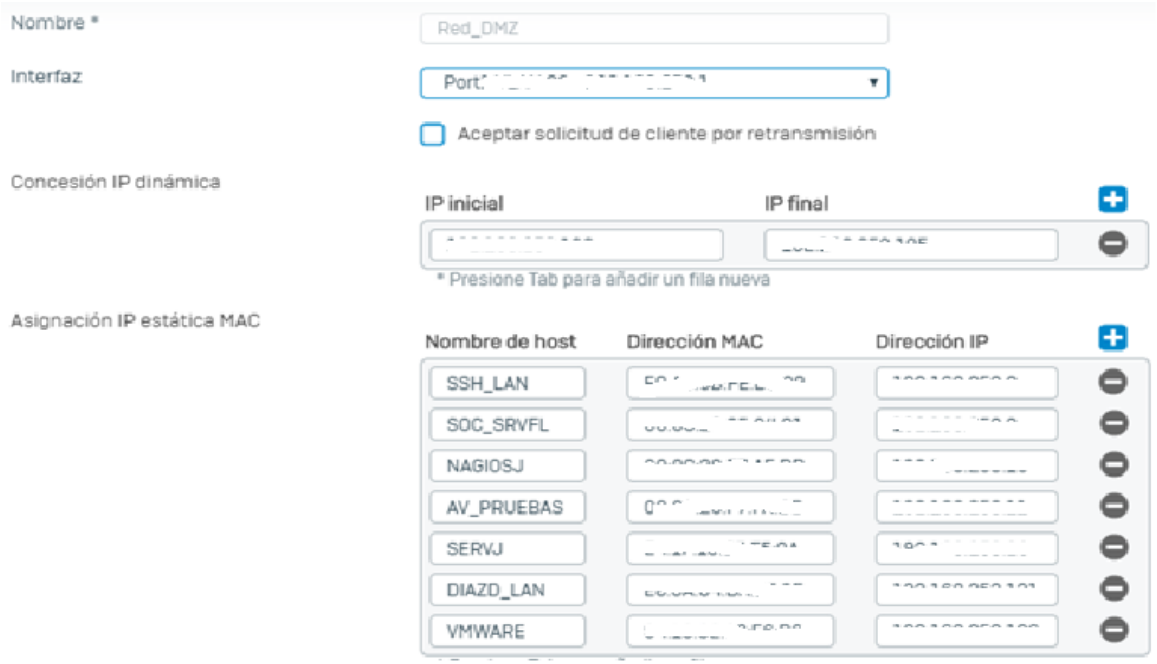


Figura. 4.46. Reserva de direcciones IP para red de servidores

En la figura 4.46 se indica la configuración de una red de pruebas que permite evaluar luego de la segmentación y la asignación de redes la conectividad y la entrega de datos en la red externa e interna.

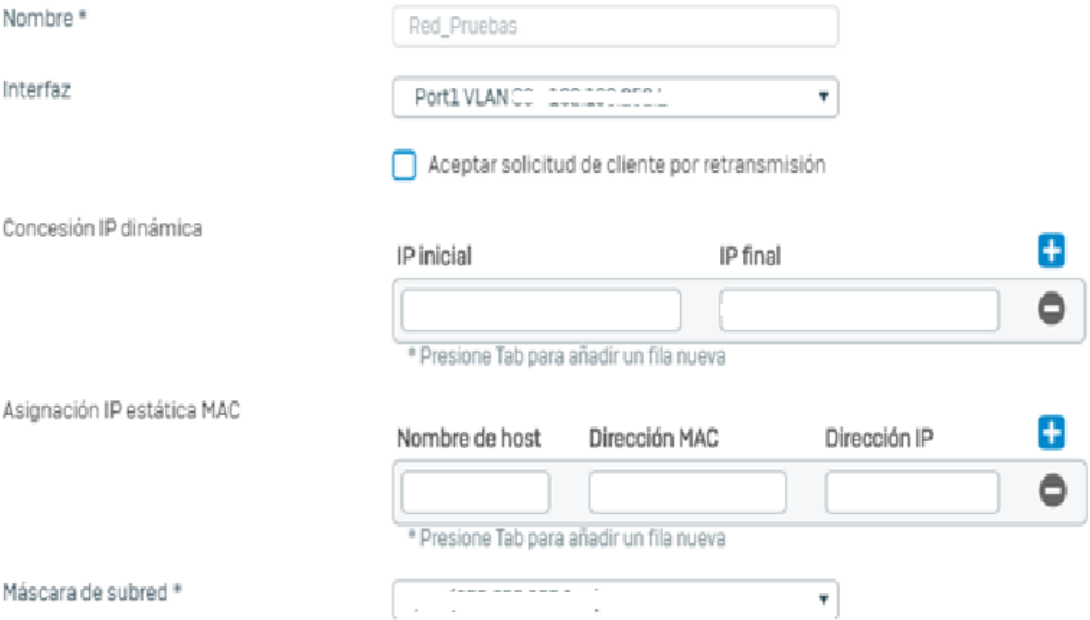


Figura. 4.47. Creación DHCP y reserva para red de pruebas

En la figura 4.47 se indica la configuración en los equipos de Sophos mediante reglas que permite a los operadores registrar en un segmento definido para el acceso, navegación, entrega de servicios, evaluación de seguridad, etc.

Figura. 4.48. Reserva de direcciones IP dentro de la red LAN para operadores

Fuente: Elaborado por el autor

4.2.12 Resumen direccionamiento red SOC

A continuación, se detalla en la tabla 4.7 el direccionamiento de todas las VLAN que se encuentran en operación dentro de la red interna del SOC.

Tabla. 4.7. Descripción por atributos

N°	ID, VLAN	NOMBRE	RED	MASCARA	GATEWAY
1	20	Red_DMZ	192.x.x.x	/25	192.x.x.x
2	30	Red_Pruebas	192.x.x.x	/25	192.x.x.x
3	40	Red_Monitoreo	192.x.x.x	/25	192.x.x.x
4	50	Red_LAN	192.x.x.x	/25	192.x.x.x

Fuente: Elaborado por el autor

4.3. Pruebas de funcionamiento

Se debe calificar cada uno de los controles con base en los subcontroles que tiene, de forma que cada subcontrol aporta al cumplimiento del control y todos los controles a la seguridad de la compañía.

Se debe realizar la evaluación de los controles de forma ordenada, de izquierda a derecha

y de arriba hacia abajo como muestra en la figura 4.48.

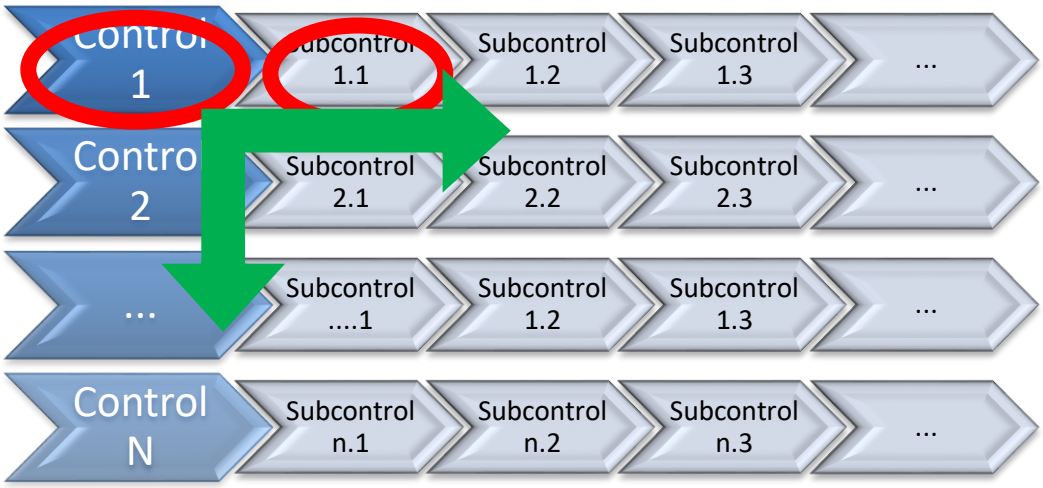
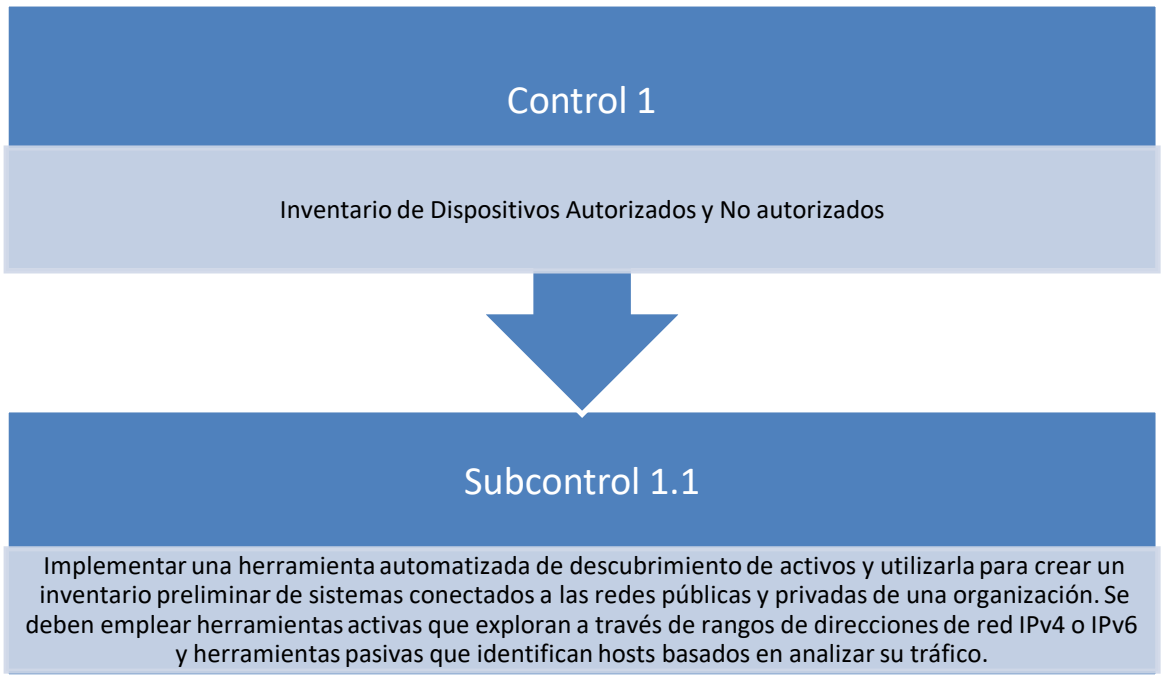


Figura. 4.49. Calificación por control y subcontrol

Fuente: Elaborado por el autor



Fuente: Elaborado por el autor

Debe ser calificado sobre los 6 atributos:

Tabla. 4.8. Calificación total

	Documentación	Operación	Normativa	Seguimiento	Indicadores	Mejora continua	Total
Atributo calificado	**5. Optimizado**	**5. Optimizado**	**5. Optimizado**	**5. Optimizado**	**5. Optimizado**	**5. Optimizado**	**5**
Valor del atributo	**5**	**5**	**5**	**5**	**5**	**5**	**30**
Peso de evaluación	**15%**	**30%**	**20%**	**15%**	**10%**	**10%**	**100 %**
Calificación obtenida	**0,75**	**1,5**	**1**	**0,75**	**0,5**	**0,5**	**5**

Fuente: Elaborado por el autor

De esta manera, un control perfectamente implementado, debe tener un valor final de 5, como calificación completa. Esto indicará:

El control está documentado, operativo, cumple con la política o normativa de la organización, se dispone una persona que realiza seguimiento continuo de la ejecución, existen indicadores para medirlo, está en mejora continua, ya que se evalúan de forma constante sus resultados.

Para una mejor aplicabilidad de esta metodología se ha diseñado una hoja de Excel capaz de realizar los cálculos de forma automática y así, las entrevistas sean más eficientes y alcancen también el efecto deseado en las personas que participan en el diseño de la red.
Este documento, hace parte de los anexos del presente proyecto de titulación.

Control Name	Family	Control	Control Description	Doc NM	Op NM	Norm NM	Seg NM	Indic NM	Mej NM	Total
Critical Security Control #1: Inventory of Authorized and Unauthorized Devices	System	1.1	Implementar una herramienta automatizada de descubrimiento de inventario de activos y utilizarla para crear un inventario preliminar de sistemas conectados a las redes públicas y privadas de una organización. Se deben emplear herramientas activas que exploran a través de rangos de direcciones de red IPv4 o IPv6 y herramientas pasivas que identifican hosts basados en analizar su tráfico.	3. Definido	5. Optimizado	5. Optimizado	5. Optimizado	5. Optimizado	5. Optimizado	5
	System	1.2	Si la organización asigna dinámicamente direcciones que utilizan DHCP, active el registro de logs del servidor de DHCP y utilice esta información para mejorar el inventario de activos y ayudar a detectar sistemas desconocidos.	1. Inicial	2. Repetible	0. No existente	1. Inicial	0. No existente	0. No existente	1
	System	1.3	Asegúrese de que todas las adquisiciones de equipos actualizan automáticamente el sistema de inventario a medida que se conectan nuevos dispositivos aprobados a la red.	0. No existente	0. No existente	0. No existente	0. No existente	0. No existente	0. No existente	0
	System	1.4	Mantener un inventario de activos de todos los sistemas conectados a la red y los propios dispositivos de red, registrado al menos las direcciones de red, nombre de máquina, propósito de cada sistema, propietario responsable de cada dispositivo y departamento asociado a cada dispositivo. El inventario debe incluir todos los sistemas que tengan una dirección IP en la red, pero no limitado a computadoras de escritorio, computadoras portátiles, servidores, equipos de red (enrutadores, *switches*, firewalls, etc.), impresoras, redes de área de almacenamiento, Teléfonos *over*-IP, direcciones *multi-homed*, direcciones virtuales, etc. El inventario de activos creado también debe incluir datos sobre si el dispositivo es un dispositivo portátil y / o personal. Los dispositivos tales como teléfonos móviles, tabletas, ordenadores portátiles y otros dispositivos electrónicos portátiles que almacenan o procesan datos deben identificarse, independientemente de si están conectados a la red de la organización.	2. Repetible	3. Definido	0. No existente	1. Inicial	0. No existente	0. No existente	1
	System	1.5	Implementar la autenticación a nivel de red a través de 802.1x para limitar y controlar qué dispositivos se pueden conectar a la red. El 802.1x se deben atar en los datos del inventario para determinar sistemas autorizados contra los no autorizados.	0. No existente	0. No existente	0. No existente	0. No existente	0. No existente	0. No existente	0
	System	1.6	Utilice certificados de cliente para validar y autenticar sistemas antes de conectarse a la red privada.	0. No existente	0. No existente	0. No existente	0. No existente	0. No existente	0. No existente	0

Figura. 4.50. Captura de hoja de Excel preparada para evaluar el cumplimiento de los controles y subcontroles.

Fuente: Elaborado por el autor

Con este recurso se puede establecer un nivel de madurez en seguridad de la red diseñada, también se puede controlar que ese nivel se mejore o mantenga durante la vida útil de la red.

4.4 Análisis de resultados

Para el análisis de resultados se evalúa el cumplimiento de los parámetros técnicos de las soluciones que se implementaron en la red. Esto cumple con lo propuesto de manera exitosa y la debida justificación a detalle en la tabla 4.9 y las figuras precedentes.

Tabla. 4.9. Cumplimiento

Funcionalidades/Producto		
Alienvault	**CUMPLE**	**NO CUMPLE**
SIEM	X	
Análisis de vulnerabilidades	X	
Inventario de activos	X	
Descubrimiento activo de activos	X	
Descubrimiento pasivo de activos	X	
Monitoreo de cuentas de usuario	X	
Monitoreo de integridad de archivos	X	
Monitoreo de integridad de sistema		
Cumplimiento normativo	X	
Clasificación dinámica de activos por el software de red	X	
Inventario de software de red	X	
Monitoreo de logs de actividades realizados por usuarios administradores	X	
Monitoreo de errores en configuración de sistemas	X	
Monitoreo y detección de malas prácticas en la administración de sistemas	X	
Sophos Central		
Protección centralizada *cloud*	X	
IPS basado en host	X	
Control de periféricos	X	
Protección en tiempo real	X	
Protección de navegación	X	
Protección de *malware* de correo electrónico	X	
Control de archivos por extensión	X	
Sophos Enpoint DLP		
Identificación de aplicaciones por categoría	X	
Permiso o denegación de ejecución de aplicaciones	X	
Comprueba la integridad de los archivos	X	
Identificación de información sensible	X	
Previene la fuga de información	X	
Integración con la protección de navegación	X	
Integración con la protección de correo	X	

Kaspersky WSUS	
Análisis de vulnerabilidades de aplicaciones de escritorio	X
Análisis de vulnerabilidades de sistema operativo	X
Permite programar tareas de parchado y remediación de vulnerabilidades	X
Actualización constante de nuevas vulnerabilidades	X
Active Directory	
Permite la administración de usuarios y sus privilegios	X
Permite tener usuarios estándar y administradores	X
Permite almacenar auditorías de las actividades de los usuarios	X
Debe limitar puertos de red	X
Administra el firewall del host	X
Se puede configurar la longitud de las contraseñas	X
Sophos WAF	
Bloquea comunicaciones de sitios maliciosos	X
Bloquea comunicaciones de IP con mala reputación	X
Se integra con la solución de protección de navegación	X
One password	
Genera auditorías del uso de cuentas	X
Permite asignar permisos a las cuentas basadas en la "necesidad del saber"	X
Cuenta con bóvedas que agrupan accesos para los usuarios	X
Revoca permisos de usuario caduco	X
Ofrece un punto de acceso centralizado	X
Sophos XG 230	
Permite controlar el acceso a la red de los dispositivos autorizados y no autorizados	X
Permite controlar el uso de aplicaciones de red	X
Cuenta con un motor de antivirus para red	X
Cuenta con protección para correo electrónico	X
Cuenta con protección y control para navegación segura	X
Realiza control de puertos y protocolos en capa 4	X
Permite seccionar las redes y brindar accesos por usuarios o equipos específicos	X
Brinda seguridad en el perímetro de las redes	X
Integración con seguridad de punto final	X

Fuente: Elaborado por el autor

Evidencias de cumplimiento:

- AlienVault

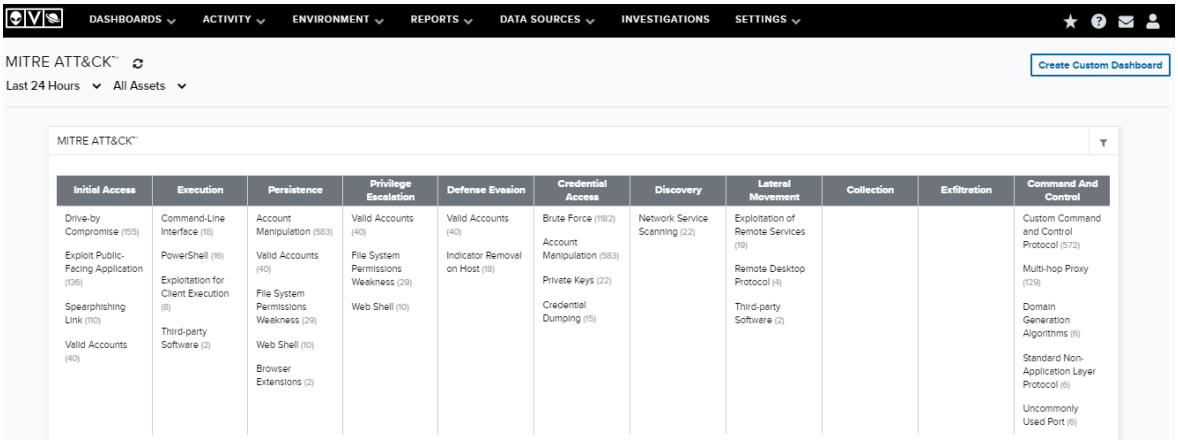


Figura. 4.51. Evidencia de cumplimiento AlienVault

Fuente: Elaborado por el autor

- Sophos XG

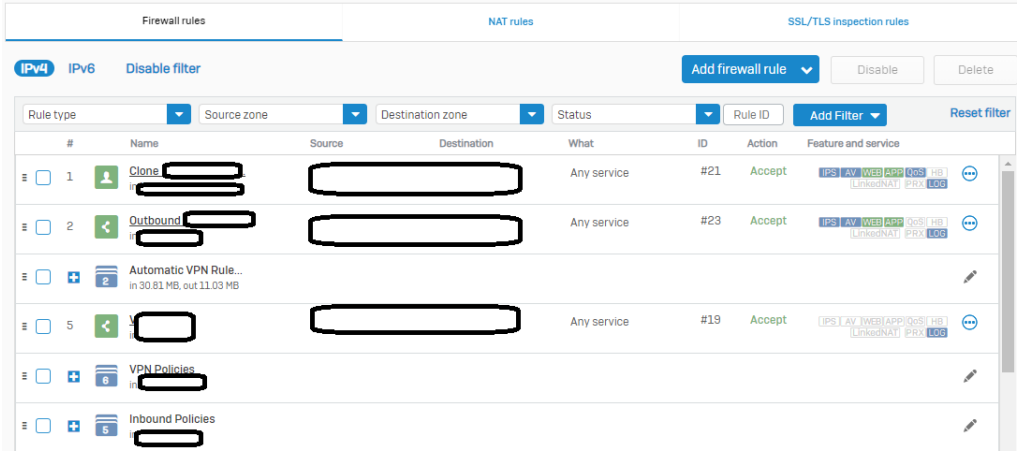


Figura. 4.52. Evidencia de operación de Sophos XG

Fuente: Elaborado por el autor

- Sophos Intercept X

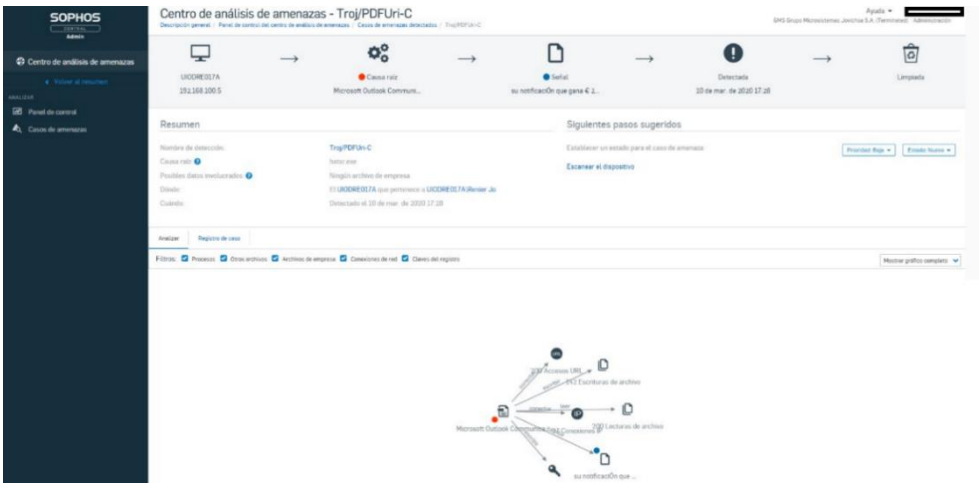


Figura. 4.53. Evidencia de cumplimiento de Sophos Intercept X

Fuente: Elaborado por el autor

- Sophos Encription

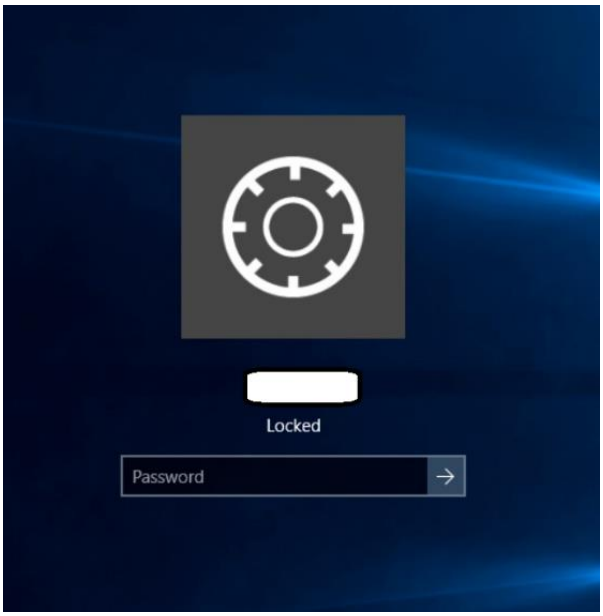


Figura. 4.54. Evidencia de aplicación del cifrado con Sophos Encription

Fuente: Elaborado por el autor

- Sophos WAF

Figura. 4.55. Evidencia de la aplicación de reglas de WAF

Fuente: Elaborado por el autor

- Sophos DLP

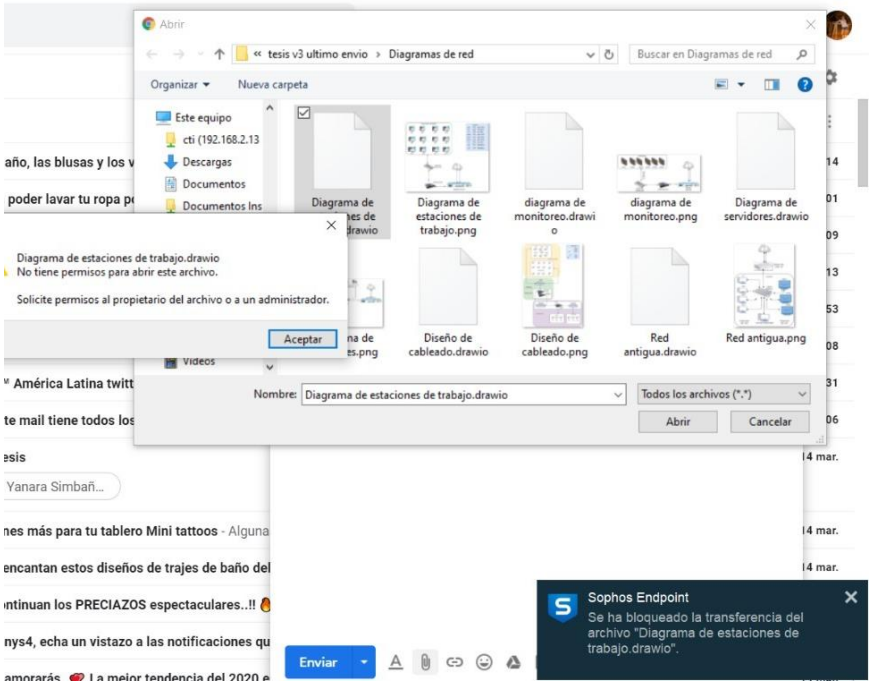


Figura. 4.56. Evidencia de cumplimiento del control de DLP

Fuente: Elaborado por el autor

- Kaspersky WSUS

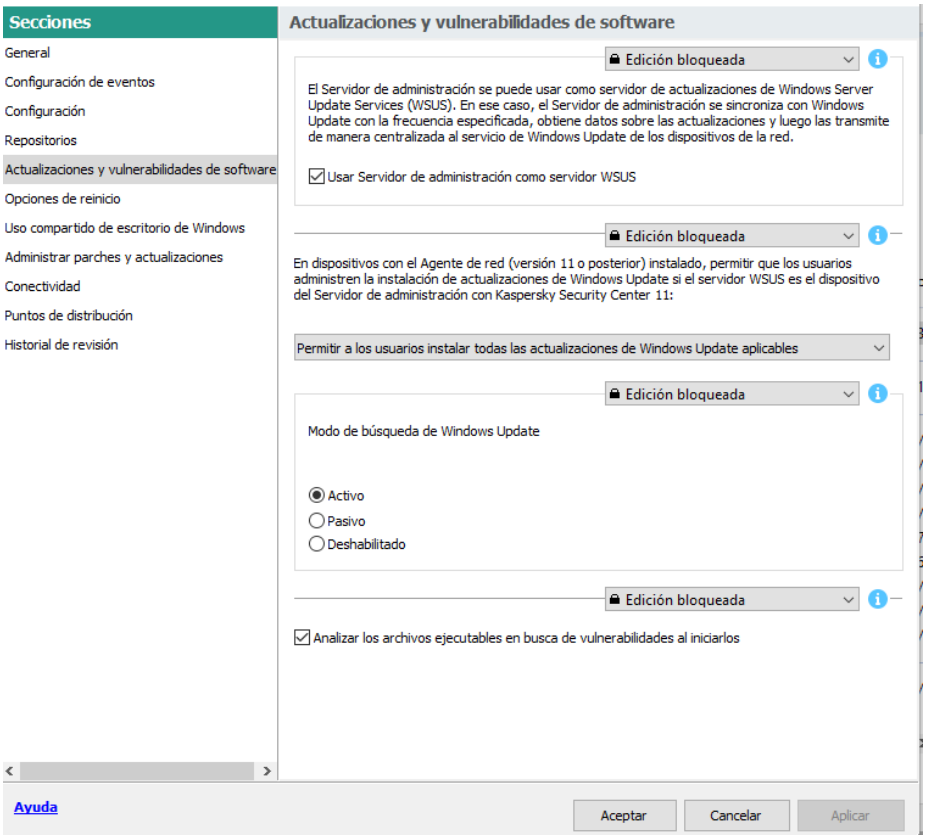


Figura. 4.57. Evidencia de cumplimiento de WSUS

Fuente: Elaborado por el autor

- Active Directory

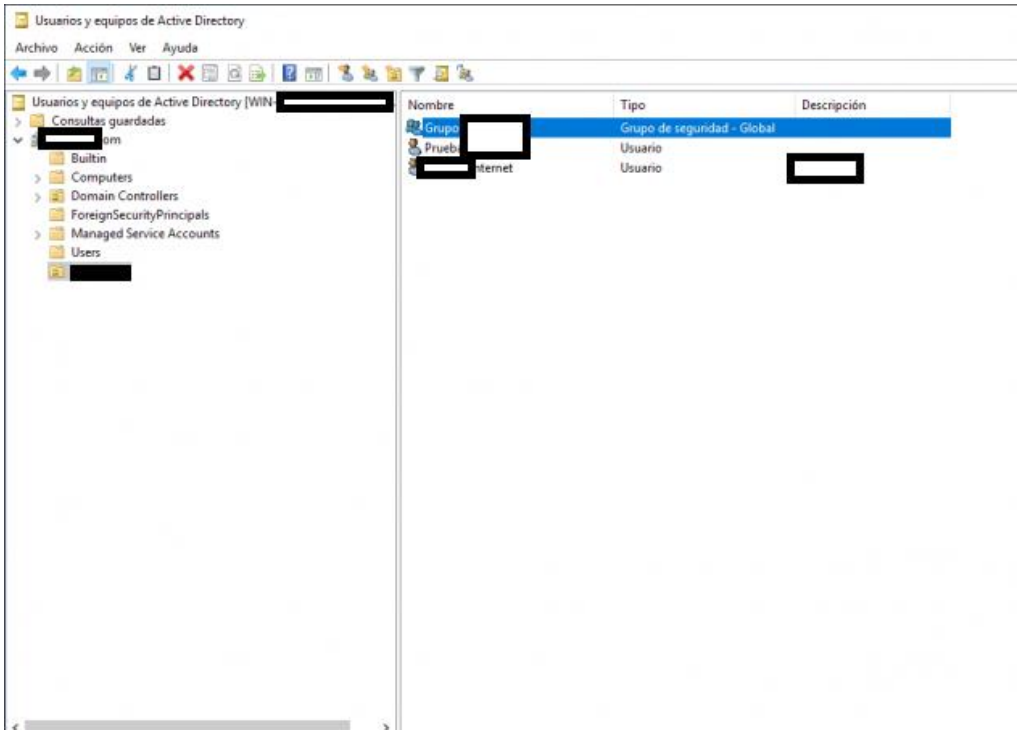


Figura. 4.58. Evidencia de configuración de usuarios y grupos

Fuente: Elaborado por el autor

- One Password

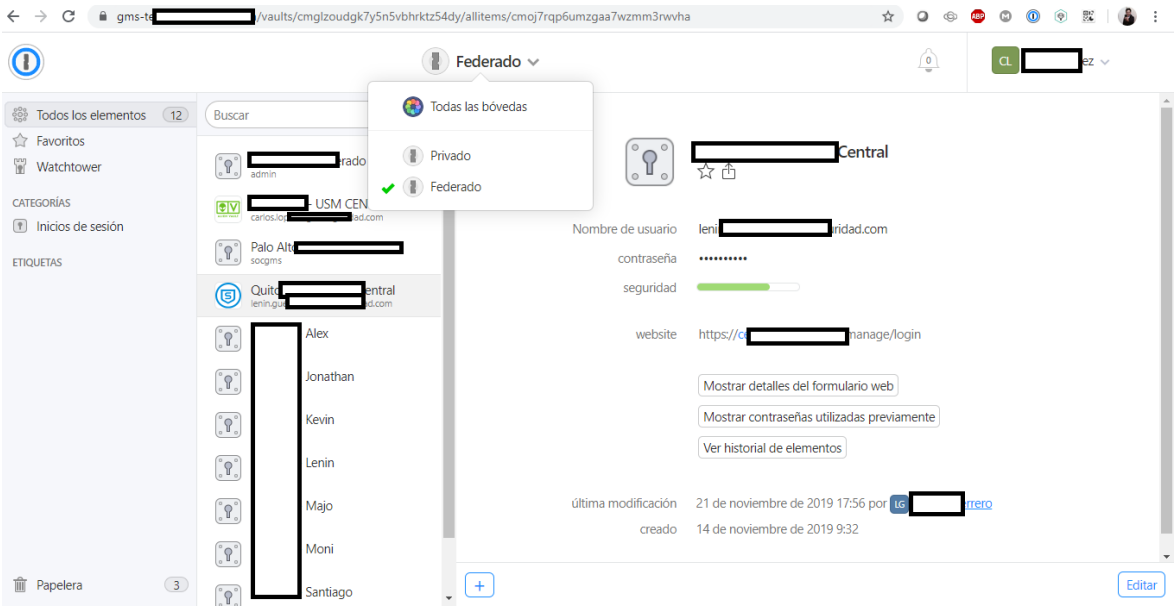


Figura. 4.59. Evidencia de configuración de one password

Fuente: Elaborado por el autor

- Google Authenticator

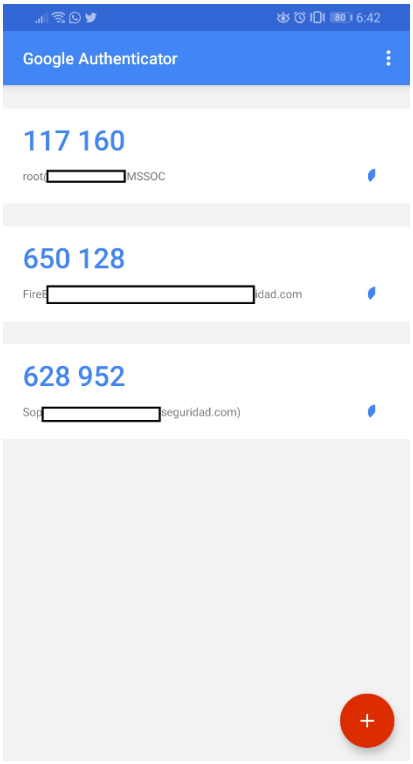


Figura. 4.60. Operación del doble factor de autenticación

Fuente: Elaborado por el autor

- Veracode

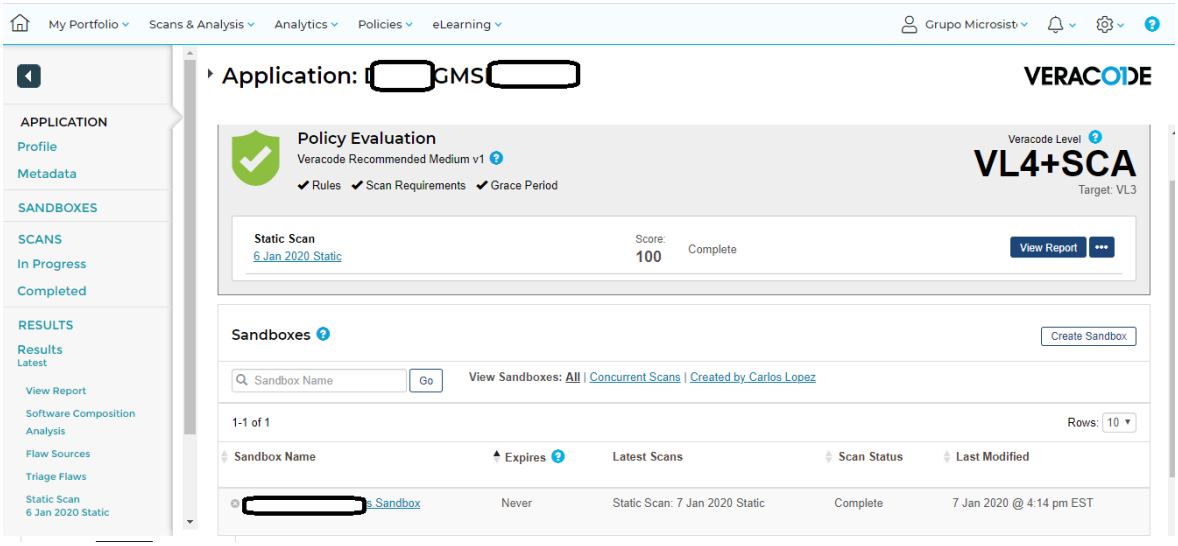


Figura. 4.61. Evidencia de operación de la plataforma de análisis de código Veracode

Fuente: Elaborado por el autor

Como parte del proceso de implementación se han considerado seguimientos, consultas a los encargados y futuros administradores, así se evalúa el impacto que puede darse al ser implementado, da como resultado positivo lo siguiente:

Se ha podido establecer un diseño que considera puntos importantes, antes del análisis de costos, la validación de alternativas de las diversas tecnologías de software y de hardware, los requerimientos y términos de referencia que permiten escoger los elementos a implementar en la red con todas las seguridades recomendadas.

Se aplican soluciones donde el impacto puede depender de decisiones tomadas al momento de implementar, por ejemplo, al momento de emplear un *switch* de *core* y un *router* deben ser evaluados con los requerimientos de seguridad y controles de protección de la red que permiten combinar en un firewall de nueva generación, el cual puede manejar enrutamiento y observar la seguridad hasta capa 7 del modelo OSI, es decir hasta las aplicaciones, solución que es capaz de entender a los usuarios y los perfila de acuerdo a sus roles, permite así permisos o deniega de forma más explicitas y contundentes que las tradicionales reglas de acceso o ACL.

El resultado en temas de nueva metodología de diseño es aplicable y poco complejo, sin embargo, se debe apoyar de hojas de datos, tablas de controles y subcontroles que hacen parte de este trabajo, esto permite tener la documentación de los cambios, variaciones o nuevos servicios brindados o adquiridos para los usuarios y clientes.

Se realiza un análisis puntual, calificativo y en general de la solución a implementar, se estiman pérdidas en años pasados de un 15% , por la base de clientes que maneja la empresa y el crecimiento año tras año sin cumplir en su totalidad con controles de seguridad en su infraestructura, se tenía acceso a servicios nuevos e inmersos a las nuevas tecnologías, sin controles y subcontroles para la pérdida de datos o bases de clientes, al ser una empresa de seguridad actualmente con este proyecto se cumple con los objetivos de brindar calidad de servicio, permite a los usuarios ser eficientes y eficaces en el manejo de todos los servicios que recibe y brinda la empresa, así las perdidas tienen una reducción de un 12%, su evaluación final considera la calificación total por control y su margen faltante debido a las reglas que el usuario a pesar de experimentar estas fases de implementación las ignora.

El resultado económico es viable de esta manera considera factores y estadísticas para estimar cuanto la empresa puede perder, si no tuviera una red segura, que por el giro de negocio esto es inaceptable. El apoyo para la inversión tras este análisis también es fácilmente accesible.

Tabla 4.10. Implementación de servicios y productos vs inversión actual

ITEM/CONTROL	Producto o servicio Implementado	Inversión actual
1	CONSULTORÍA DE HARDENING	$4.000,00
2	CONSULTORÍA DE CLASIFICACIÓN DE INFORMACIÓN	$4.000,00
3	INGENIERÍA SOCIAL	$4.500,00
4	CAPACITACIÓN DE HERRAMIENTAS DE SEGURIDAD (adicionales a las implementadas)	$1.000,00
5	CAPACITACIONES ESPECIALIZADAS EN SEGURIDAD	$2.000,00
6	CONSULTORÍA DE EH	$6.000,00
7	SERVICIOS CSIRT	$2.400,00
8	SERVICIOS DE SOC	$5.400,00
9	ALIENVAULT	$3.000,00
10	SOPHOS XG	$1.500,00
11	SOPHOS INTEREPT X	$1.300,00
12	SOPHOS ENDPOINT AND DLP	$2.850,00
13	SOPHOS ENCRIPTION	$1.800,00
14	WSUS	$1.400,00
15	ACTIVE DIRECTORY	$2.500,00
16	SOPHOS WAF	$6.000,00
17	ONE PASSWORD	$1.200,00
18	GOOGLE AUTHENTICATOR	$2.900,00
19	VERACODE	$1.800,00
		$55.550,00

Fuente: Elaborado por el autor

La ejecución del presupuesto alcanzó el 86% y deja un 15% para gastos indirectos que

pudieran presentarse, esto permite concluir que el resultado es satisfactorio y viable.

Los productos fueron adquiridos con la finalidad de proveer apoyo a la operación propia de la compañía, es decir como apoyo al negocio y prevención de riesgos asociados a las nuevas tecnologías que cada día se vuelven vulnerables a ataques de día cero, así como también para cumplir los controles de seguridad.

Se observa la calificación obtenida de la red plana sin controles de seguridad, esto según un estudio minucioso como levantamiento de información inicial.

En la tabla 4.8 vs la tabla 4.9 se puede evidenciar un antes y un después de este proyecto, se muestran los puntajes que se obtuvo en un levantamiento de información inicial y un puntaje con la implementación de una red segura y operativa, cada puntaje está basado en la tabla 4.5.

Tabla 4.11. Levantamiento inicial en una red plana

Control	Controles	Nivel de Madurez
Control 01	Inventario de dispositivos autorizados y no autorizados	**1**
Control 02	Inventario de software autorizado y no autorizado	**1**
Control 03	Configuraciones de seguridad de *hardware* y *software*	**0**
Control 04	Evaluación continua de vulnerabilidades y remediación	**0**
Control 05	Uso controlado de privilegios administrativos	**0**
Control 06	Mantenimiento, monitoreo y análisis de auditoria de logs	**0**
Control 07	Protección de email y web browser	**0**
Control 08	Defensa de *malware*	**0**
Control 09	Limitación y control de puertos de red	**0**
Control 10	Capacidad de recuperación de datos	**0**
Control 11	Configuración de seguridad para dispositivos de red	**0**
Control 12	Defensa perimetral	**0**
Control 13	Protección de datos	**0**
Control 14	Control de acceso basado en la “necesidad de saber”	**0**
Control 15	Control de acceso *Wireless*	-
Control 16	Monitoreo y control de cuentas	**0**
Control 17	Evaluación de habilidades de seguridad y capacitación apropiada para llenar vacíos	**0**
Control 18	Seguridad de *software* de Aplicaciones	**0**
Control 19	Gestión y respuesta a incidentes	**0**
Control 20	*Penetration tests* y ejercicios de red *team*	**0**

Fuente: Elaborado por el autor

La figura muestra el puntaje inicial que se tenía implementado en una red plana sin controles de seguridad y con plataformas básicas como un servidor que almacenaba varias aplicaciones.

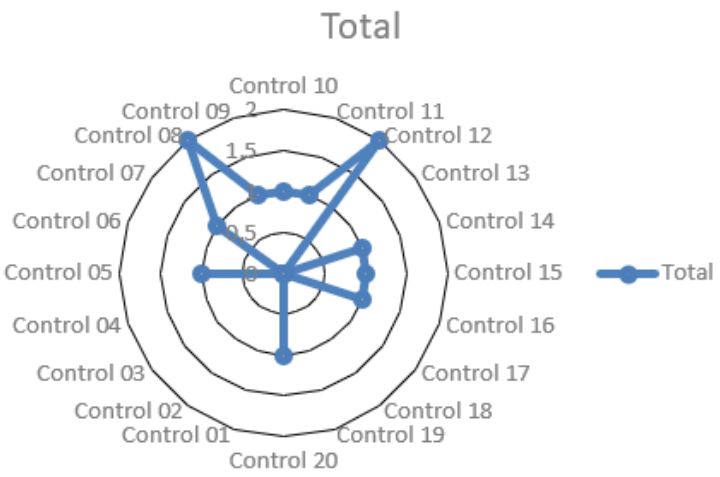


Figura. 4.61. Situación inicial mapa de calor

Fuente: Elaborado por el autor

El cumplimiento del trabajo que se planteó permite tener los resultados que se describe en la tabla 4.9 a continuación:

Tabla 4.12. Puntaje de evaluación de los controles de seguridad que se implementó

Control	Controles	Resultado final
Control 01	Inventario de dispositivos autorizados y no autorizados	**4**
Control 02	Inventario de *software* autorizado y no autorizado	**4**
Control 03	Configuraciones de seguridad de *hardware* y *software*	**4**
Control 04	Evaluación continua de vulnerabilidades y remediación	**4**
Control 05	Uso Controlado de privilegios administrativos	**4**
Control 06	Mantenimiento, monitoreo y análisis de auditoria de logs	**4**
Control 07	Protección de *email* y *web browser*	**4**
Control 08	Defensa de *malware*	**4**
Control 09	Limitación y control de puertos de red	**4**
Control 10	Capacidad de recuperación de datos	**4**
Control 11	Configuración de seguridad para dispositivos de red	**4**
Control 12	Defensa perimetral	**4**
Control 13	Protección de datos	**4**
Control 14	Control de acceso basado en la “necesidad de saber”	**4**
Control 15	Control de acceso *Wireless*	-
Control 16	Monitoreo y control de Cuentas	**4**
Control 17	Evaluación de habilidades de seguridad y capacitación apropiada para llenar vacíos	**4**
Control 18	Seguridad de *software* de aplicaciones	**4**
Control 19	Gestión y respuesta a incidentes	**4**
Control 20	*Penetration tests* y ejercicios de *red team*	**4**

Fuente: Elaborado por el autor

En la siguiente figura se puede observar en un mapa de calor el puntaje final después de implementar la red con los controles establecidos por seguridad en plataformas de hardware y software dedicadas para cada una.

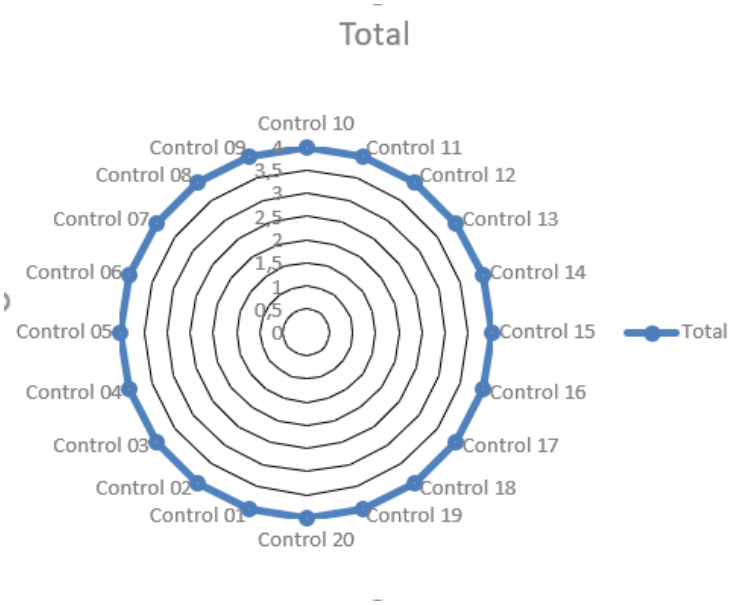


Figura. 4.62. Puntaje final con los controles de la SANS

Fuente: Elaborado por el autor

CONCLUSIONES

- Se implementó una red LAN con acceso WAN, en la empresa GMS, administrada de acuerdo con los 20 controles establecidos por el Instituto SANS – *SysAdmin, Networking and Security Institute*, la solución que se aplica en la red dentro del proyecto cumple con un diseño basado en el estándar de controles propuestos por el Instituto SANS, estos controles hacen cumplir con los principios de confidencialidad, integridad y disponibilidad, así también considera una implementación escalable, modular y de fácil administración.

- Se definen las diferentes metodologías de diseño de redes y los controles críticos de seguridad establecidos por el Instituto SANS para la administración, gestión de una red considerada como segura, así se concluye cada evaluación con base a las necesidades del empleado y la entrega de servicios disponibles dentro y fuera de la empresa, de esta forma se cuenta con la eficiencia, control y administración adecuada.

- Se implementa la red diseñada con cada uno de los controles y subcontroles los cuales han sido evaluados y puntuados según el análisis, compromisos, faltantes, reuniones establecidas y normativas de la empresa para poder implementar, así como el manejo de *hardware* y *software* a ser adquirido y empleado dado que la ponderación de calificación es de 5 puntos que considera operabilidad completa de acuerdo con la calificación final.

- Se realiza un análisis de resultados y se establece un resumen crítico de resultados y factibilidad de estandarización de la metodología particular empleada así la empresa cumple con los parámetros de seguridad y control adecuados que se realizó mediante una evaluación final interna, calificada y puntuada según los controles establecidos e implementados, así alcanza una eficiencia del 99% de disponibilidad y seguridad en la red, el margen de error depende de cada usuario de acuerdo a las órdenes y conocimiento que tenga para su operación.

RECOMENDACIONES

- Se recomienda tener un estudio general o información auditada de la empresa para un mapeo adecuado de los faltantes y selección de los controles adecuados para su correcto funcionamiento y puesta en producción.

- Para mantener el funcionamiento adecuado a futuro, como se encuentra ahora, se necesita realizar un análisis de resultados con un resumen crítico de los puntos establecidos cada seis meses, esto considera los cambios en la red de acuerdo con el crecimiento o manejo de nuevos sistemas, con la adición de nuevos servicios o aplicativos, la incorporación y desvinculación de personal, también pueden afectar a los indicadores de gestión, con esta base los análisis de resultados se recomiendan ejecutar mínimo dos veces por año.

- De acuerdo con la vertical del negocio se deberían analizar controles de seguridad adicionales a los expuestos en este proyecto de titulación, en industrias como la banca, aplican estándares como PCI (*Payment Card Industry Data Security Standard*) e ISO 27000 ("*International Organization for Standardization*"), otro ejemplo son las instituciones de la salud en la cual aplican estándares como las recomendaciones norteamericanas HIPAA *(Health Insurance Portability and Accountability Act)*

- Se recomienda el manejo de un *datacenter* con equipos activos-pasivos con la finalidad de evitar pérdidas en el supuesto caso de daños a los equipos, configuraciones variables, desconexión de la red, afectaciones climáticas, daños de fábrica, cambio de personal, entre otros factores que pueden ocasionar el reverso de este proyecto, para lo cual el administrador o responsable debe considerar un plan de gestión como *backup*.

REFERENCIAS BIBLIOGRÁFICAS

AlienVault. (14 de Abril de 2019). *https://www.corporatearmor.com/documents/AlienVault_USM_Anywhere_Datasheet.pdf*. Obtenido de https://www.corporatearmor.com/documents/AlienVault_USM_Anywhere_Datasheet.pdf

CERT-PY. (14 de Enero de 2014). *Guía de Controles Críticos de Ciberseguridad*. Obtenido de https://www.cert.gov.py/index.php/download_file/view_inline/1375?cv=1

Cisco. (15 de Abril de 2014). *www.cisco.com.* Obtenido de https://www.cisco.com/c/dam/r/es/la/internet-of-everything-ioe/assets/pdfs/en-05_campus-wireless_wp_cte_es-xl_42333.pdf

Crespo, A. (19 de Enero de 2017). *www.redeszone.net.* Obtenido de https://www.redeszone.net/2017/01/17/dmz-routers-descubre-mejor-forma-utilizacion/

Cuna, J. (27 de Junio de 2018). *¿CMMI 5 qué es y quienes cuentan con este modelo?* Obtenido de https://revistacio.com/cmmi-5-que-es-y-quienes-cuentan-con-este-modelo/?cv=1

Diseño de la LAN. (14 de Enero de 2020). *www.itesa.edu.* Obtenido de https://www.itesa.edu.mx/netacad/switching/course/module1/1.1.1.5/1.1.1.5.html

Gallardo, C. (14 de Diciembre de 2017). Obtenido de https://bibdigital.epn.edu.e: https://bibdigital.epn.edu.ec/bitstream/15000/19021/1/CD-8418.pdf

GOT A PLAN. (2017). Obtenido de www.incidentresponse.com: https://www.incidentresponse.com/playbooks/

IS IT SKULL. (14 de Febrero de 2019). *www.it-skull.com.* Obtenido de https://www.it-skull.com/2-seguridad-de-la-informacion-que-es/6-triangulo-de-la-seguridad-de-la-informacion.html

Modelo OSI. (14 de Febrero de 2019). *La historia que cambio las redes.* Obtenido de https://seaccna.com/modelo-osi-guia-definitiva/

Modelo OSI. (11 de Febrero de 2020). Obtenido de https://www.bonaval.com/kb/sistemas/redes/modelo-osi

Rodríguez, K. (22 de Junio de 2017). *Información por redes.* Obtenido de blogger1-1karimerodriguez.blogspot.com

SANS. (14 de Enero de 2017). Obtenido de https://www.sans.org/vendor/analyst-program

Simbaña, Y. (2020). *Implementación de una red LAN con acceso WAN, en la empresa GMS, administrada de acuerdo con la norma establecida por el Instituto SANS - SysAdmin Audit, Networking and Security Institute.* Quito.

ANEXOS

ANEXO 1 Establecimiento de subcontroles de seguridad

Los 150 subcontroles de los 20 controles de la SANS

SubControl	Descripción
1.1	Implementar una herramienta automatizada de descubrimiento de inventario de activos y utilizarla para crear un inventario preliminar de sistemas conectados a las redes públicas y privadas de una organización. Se deben emplear herramientas activas que exploran a través de rangos de direcciones de red IPv4 o IPv6 y herramientas pasivas que identifican hosts basados en analizar su tráfico.
1.2	Si la organización asigna dinámicamente direcciones que usen DHCP, active el registro de logs del servidor de DHCP y utilice esta información para mejorar el inventario de activos y ayudar a detectar sistemas desconocidos.
1.3	Asegúrese de que todas las adquisiciones de equipos actualizan automáticamente el sistema de inventario a medida que se conectan nuevos dispositivos aprobados a la red.
1.4	Mantener un inventario de activos de todos los sistemas conectados a la red y los propios dispositivos de red, al menos las direcciones de red, nombre de máquina, propósito de cada sistema, propietario responsable de cada dispositivo y departamento asociado a cada dispositivo. El inventario debe incluir todos los sistemas que tengan una dirección IP en la red, pero no limitado a computadoras de escritorio, computadoras portátiles, servidores, equipos de red (enrutadores, *switches*, *firewalls*, etc.), impresoras, redes de área de almacenamiento, Teléfonos *over*-IP, direcciones *multi-homed*, direcciones virtuales, etc. El inventario de activos creado también debe incluir datos sobre si el dispositivo es un dispositivo portátil y / o personal. Los dispositivos tales como teléfonos móviles, tabletas, ordenadores portátiles y otros dispositivos electrónicos portátiles que almacenan o procesan datos deben identificarse, independientemente de si están conectados a la red de la organización.
1.5	Implementar la autenticación a nivel de red a través de 802.1x para limitar y controlar qué dispositivos se pueden conectar a la red. El 802.1x se deben atar en los datos del inventario para determinar sistemas autorizados contra los no autorizados.
1.6	Utilice certificados de cliente para validar y autenticar sistemas antes de conectarse a la red privada.
2.1	Elabore una lista de software autorizado y versión que se requieren en la empresa para cada tipo de sistema, incluidos servidores, estaciones de trabajo y portátiles de diversos tipos y usos. Esta lista debe ser monitoreada por herramientas de comprobación de integridad de archivos para validar que el software autorizado no ha sido modificado.
2.2	Implementar un software de control de aplicaciones que permite a los sistemas ejecutar software sólo si se incluye en la *white list* e impide la ejecución de los demás programas del sistema. La lista blanca puede ser muy extensa, para que los usuarios puedan usar software común. O, para algunos sistemas especiales (que requieren sólo un número reducido de programas para lograr la funcionalidad empresarial necesaria), la lista blanca puede ser muy estrecha.
2.3	Implementar herramientas de inventario de software en toda la organización que cubran cada uno de los tipos de sistemas operativos en uso, incluidos servidores, estaciones de trabajo y computadoras portátiles. El sistema de inventario de software debe realizar un seguimiento de la versión del sistema operativo subyacente, así como de las aplicaciones instaladas en él. Los sistemas de inventario de software deben estar vinculados al inventario de activos de hardware para que todos los dispositivos y el software asociado se rastree desde una única ubicación.
2.4	Las máquinas virtuales y / o los sistemas air-*gapped* deben usarse para aislar y ejecutar aplicaciones que son requeridas para las operaciones de negocios, pero basadas en un riesgo mayor no deben ser instaladas dentro de un entorno de red.

3.1	Establecer configuraciones estándar seguras de sus sistemas operativos y aplicaciones de software. Las imágenes normalizadas deben representar versiones endurecidas del sistema operativo subyacente y las aplicaciones instaladas en el sistema. Estas imágenes deben ser validadas y actualizadas periódicamente para actualizar su configuración de seguridad a la luz de las vulnerabilidades y vectores de ataque recientes.
3.2	Siga la administración de configuración estricta, construya una imagen segura que se utiliza para construir todos los nuevos sistemas que se despliegan en la empresa. Cualquier sistema existente que se vea comprometido debe ser *re-imaged* con la construcción segura. Actualizaciones regulares o excepciones a esta imagen deben integrarse en los procesos de gestión de cambios de la organización. Las imágenes deben crearse para estaciones de trabajo, servidores y otros tipos de sistemas utilizados por la organización.
3.3	Almacenar las imágenes maestras en servidores configurados de forma segura, validados con herramientas de comprobación de integridad capaces de inspección continua y gestión de cambios para garantizar que sólo son posibles cambios autorizados en las imágenes. Alternativamente, estas imágenes maestras se pueden almacenar en máquinas sin conexión, filtradas desde la red de producción, con imágenes copiadas a través de medios seguros para moverlas entre los servidores de almacenamiento de imágenes y la red de producción.
3.4	Realiza toda la administración remota de servidores, estaciones de trabajo, dispositivos de red y equipos similares a través de canales seguros. Protocolos tales como Telnet, VNC, RDP u otros que no soportan activamente cifrado fuerte sólo deben ser utilizados si se realizan a través de un canal de cifrado secundario, como SSL, TLS o IPSEC.
3.5	Utilice herramientas de comprobación de integridad de archivos para asegurarse de que los archivos críticos del sistema (incluidos los archivos ejecutables, las bibliotecas y las configuraciones sensibles del sistema y de la aplicación) no se han alterado. El sistema de información debería: tener la capacidad de dar cuenta de los cambios de rutina y esperados; Resaltar y alertar sobre alteraciones inusuales o inesperadas; Muestran el historial de cambios de configuración a lo largo del tiempo e identifican quién realizó el cambio (incluida la cuenta registrada original en el caso de un cambio de ID de usuario, como con el comando su o sudo). Estas comprobaciones de integridad deben identificar alteraciones sospechosas del sistema, tales como: cambios de propietario y permisos en archivos o directorios; El uso de flujos de datos alternativos que podrían utilizarse para ocultar actividades maliciosas; Y la introducción de archivos adicionales en las áreas clave del sistema (lo que podría indicar cargas malintencionadas dejadas por atacantes o archivos adicionales inapropiadamente añadidos durante los procesos de distribución por lotes).
3.6	Implementar y probar un sistema automatizado de monitoreo de configuración que verifica todos los elementos de configuración seguros que se pueden probar remotamente y alerta cuando ocurren cambios no autorizados. Esto incluye detectar nuevos puertos de escucha, nuevos usuarios administrativos, cambios en los objetos de directiva de grupo y locales (cuando sea aplicable) y nuevos servicios que se ejecutan en un sistema. Siempre que sea posible utilice herramientas compatibles con el Protocolo de Automatización de Contenido de Seguridad (SCAP) para agilizar la generación de informes y la integración.
3.7	Implementar las herramientas de administración de configuración del sistema, como los objetos de directiva de grupo de Active Directory para sistemas Microsoft Windows o los sistemas LDAP para UNIX que automáticamente aplicarán y reasignarán los valores de configuración a los sistemas a intervalos regulares. Deberían ser capaces de desencadenar la redistribución de los ajustes de configuración de forma programada, manual o basada en eventos.
4.1	Ejecute herramientas automatizadas de análisis de vulnerabilidades contra todos los sistemas de la red de forma semanal o más frecuente y entregue listas priorizadas de las vulnerabilidades más críticas a cada administrador del sistema responsable, junto con las puntuaciones de riesgo que comparan la eficacia de los administradores y departamentos del sistema para reducir el riesgo. Utilice un escáner de vulnerabilidades validado por SCAP que busque vulnerabilidades basadas en código (como las descritas en las entradas de *Common Vulnerabilities* and *Exposures*) y

	vulnerabilidades basadas en la configuración (enumeradas por el *Common Configuration Enumeration* Project).
4.2	Correlacione los registros de eventos con información de exploraciones de vulnerabilidades para cumplir dos objetivos. En primer lugar, el personal debe verificar que la actividad de las herramientas regulares de análisis de vulnerabilidades está registrada. En segundo lugar, el personal debe ser capaz de correlacionar los eventos de detección de ataques con resultados previos de escaneo de vulnerabilidades para determinar si el *exploit* dado se utilizó contra un objetivo conocido como vulnerable.
4.3	Realice el escaneado de vulnerabilidades en modo autenticado, ya sea con agentes que se ejecutan localmente en cada sistema final para analizar la configuración de seguridad o con escáneres remotos a los que se administran derechos administrativos en el sistema que está a prueba. Utilice una cuenta dedicada para exploraciones de vulnerabilidades autenticadas, que no deben utilizarse para otras actividades administrativas y deben estar vinculadas a máquinas específicas en direcciones IP específicas. Asegúrese de que sólo los empleados autorizados tengan acceso a la interfaz de usuario de gestión de vulnerabilidades y que las funciones se apliquen a cada usuario
4.4	Suscríbase a los servicios de inteligencia de vulnerabilidad para mantenerse al tanto de las exposiciones emergentes y utilice la información obtenida de esta suscripción para actualizar las actividades de análisis de vulnerabilidades de la organización al menos una vez al mes. Como alternativa, asegúrese de que las herramientas de análisis de vulnerabilidades que utiliza se actualizan periódicamente con todas las vulnerabilidades de seguridad importantes relevantes.
4.5	Implementar herramientas automatizadas de administración de parches y herramientas de actualización de software para sistemas operativos y software / aplicaciones en todos los sistemas para los cuales dichas herramientas estén disponibles y sean seguras. Los parches deben aplicarse a todos los sistemas, incluso a los sistemas que estén adecuadamente protegidos contra el aire. *properly* air *gapped.*
4.6	Supervise los registros asociados a cualquier actividad de análisis y cuentas de administrador asociadas para garantizar que esta actividad se limite a los plazos de las exploraciones legítimas.
4.7	Compare los resultados de los análisis de vulnerabilidades consecutivos para verificar que las vulnerabilidades se solucionaron mediante parches, implementación de un control compensatorio o documentación y aceptación de un riesgo comercial razonable. Esta aceptación de los riesgos empresariales para las vulnerabilidades existentes debe ser revisada periódicamente para determinar si nuevos controles compensatorios o parches subsiguientes pueden abordar vulnerabilidades que se aceptaron previamente o si las condiciones han cambiado, lo que aumenta el riesgo.
4.8	Establecer un proceso para clasificar las vulnerabilidades basadas en la vulnerabilidad y el potencial impacto de la vulnerabilidad, segmentadas por grupos apropiados de activos (por ejemplo, servidores DMZ, servidores de red internos, equipos de escritorio, portátiles). Aplique primero los parches para las vulnerabilidades más arriesgadas. Se puede usar un despliegue gradual para minimizar el impacto para la organización. Establecer los plazos de parche esperados basados en el nivel de clasificación de riesgo.
5.1	Minimice los privilegios administrativos y sólo utilice las cuentas administrativas cuando se requieran. Implementar auditorías focalizadas en el uso de funciones privilegiadas administrativas y monitorear el comportamiento anómalo
5.2	Utilice herramientas automatizadas para inventariar todas las cuentas administrativas y validar que cada persona con privilegios administrativos en escritorios, computadoras portátiles y servidores esté autorizada por un ejecutivo senior.
5.3	Antes de implementar nuevos dispositivos en un entorno de red, cambie todas las contraseñas predeterminadas para aplicaciones, sistemas operativos, enrutadores,

	firewalls, puntos de acceso inalámbricos y otros sistemas para que los valores sean consistentes con las cuentas de administración.
5.4	Configure los sistemas para que emitan una entrada de registro y una alerta cuando una cuenta se agrega o se quita de un grupo de administradores de dominio o cuando se agrega una nueva cuenta de administrador local en un sistema.
5.5	Configure los sistemas para emitir una entrada de registro y una alerta en cualquier inicio de sesión fallido en una cuenta administrativa.
5.6	Utilice la autenticación multifactor para todos los accesos administrativos, incluido el acceso administrativo de dominio. La autenticación de múltiples factores puede incluir una variedad de técnicas, para incluir el uso de tarjetas inteligentes, certificados, fichas de contraseña de One Time (OTP), biometría u otros métodos de autenticación similares.
5.7	Si no se admite la autenticación de varios factores, se requerirá que las cuentas de usuario utilicen contraseñas largas en el sistema (más de 14 caracteres).
5.8	Los administradores deben tener acceso a un sistema que utiliza una cuenta completamente registrada y no administrativa. Luego, una vez conectado a la máquina sin privilegios administrativos, el administrador debe pasar a privilegios administrativos herramientas como Sudo en Linux / UNIX, *RunAs* en Windows y otras instalaciones similares para otros tipos de sistemas.
5.9	Los administradores utilizarán una máquina dedicada para todas las tareas administrativas o tareas que requieran un acceso elevado. Esta máquina estará aislada de la red primaria de la organización y no se permitirá el acceso a Internet. Esta máquina no debe usarse para leer correos electrónicos, componer documentos o navegar por Internet.
6.1	Incluya al menos dos fuentes de tiempo sincronizadas desde las que todos los servidores y equipos de red recuperen la información de tiempo de forma regular para que las marcas de tiempo en los registros sean consistentes.
6.2	Valide la configuración del registro de auditoría para cada dispositivo de hardware y el software instalado en él, asegurándose de que los registros incluyan una fecha, hora, direcciones de origen, direcciones de destino y varios otros elementos útiles de cada paquete y / o transacción. Los sistemas deben registrar los registros en un formato estandarizado, como las entradas de *syslog* o las descritas por la iniciativa *Common Event Expression*. Si los sistemas no pueden generar registros en un formato estandarizado, las herramientas de normalización de registros se pueden desplegar para convertir los registros en tal formato
6.3	Asegúrese de que todos los sistemas que almacenan registros tengan espacio de almacenamiento adecuado para los registros generados de forma regular, de modo que los archivos de registro no se llenen entre intervalos de rotación de registros. Los registros deben ser archivados y firmados digitalmente periódicamente.
6.4	Haga que el personal de seguridad y / o los administradores del sistema ejecuten informes quincenales que identifiquen anomalías en los registros. Luego deben revisar activamente las anomalías, documentar sus hallazgos.
6.5	Configure los dispositivos perimetrales, incluidos firewalls, IPS basados en red y *proxies* entrantes y salientes, para registrar de forma detallada todo el tráfico (permitido y bloqueado) que llega al dispositivo.
6.6	Implementar una herramienta SIEM (Administración de eventos e información de seguridad) o logarítmicas analíticas para la agregación y consolidación de registros desde varias máquinas y para correlación y análisis de registros. Utiliza la herramienta SIEM, los administradores de sistemas y el personal de seguridad deben diseñar perfiles de eventos comunes de sistemas dados para que puedan sintonizar la detección para centrarse en actividades inusuales, evitar falsos positivos, identificar más rápidamente anomalías y evitar alarmantes alertas.
7.1	Asegúrese de que sólo los navegadores web y los clientes de correo electrónico totalmente compatibles se pueden ejecutar en la organización, idealmente sólo se utiliza la última versión de los navegadores proporcionados por el proveedor para aprovechar las funciones de seguridad más recientes y las correcciones.
7.2	Desinstale o deshabilite cualquier navegador innecesario o no autorizado o complementos de correo electrónico de cliente o aplicaciones complementarias. Cada

	complemento utilizará la lista blanca de aplicaciones / URL y sólo permitirá el uso de la aplicación para dominios pre-aprobados.
7.3	Limitar el uso de lenguajes de scripting innecesarios en todos los navegadores web y clientes de correo electrónico. Esto incluye el uso de lenguajes como ActiveX y JavaScript en sistemas en los que es innecesario soportar dichas capacidades.
7.4	Registre todas las solicitudes de URL de cada uno de los sistemas de la organización, ya sea en el sitio o en un dispositivo móvil, con el fin de identificar la actividad potencialmente malintencionada y ayudar a los gestores de incidentes con la identificación de sistemas potencialmente comprometidos.
7.5	Implementar dos configuraciones de navegador distintas en cada sistema. Una configuración debe desactivar el uso de todos los complementos, lenguajes de scripting innecesarios y, en general, configurarse con una funcionalidad limitada y utilizarse para la navegación web general. La otra configuración permitirá una mayor funcionalidad del navegador, pero sólo debe utilizarse para acceder a sitios web específicos que requieren el uso de dicha funcionalidad.
7.6	La organización debe mantener y hacer cumplir filtros de URL basados en la red que limiten la capacidad de un sistema para conectarse a sitios web no aprobados por la organización. La organización debe suscribirse a los servicios de categorización de URL para asegurarse de que estén actualizados con las definiciones de categorías de sitios web más recientes disponibles. Los sitios sin clasificar se bloquearán de forma predeterminada. Este filtrado se aplicará para cada uno de los sistemas de la organización, ya sea que estén físicamente en las instalaciones de una organización o no.
7.7	Para reducir la probabilidad de mensajes de correo electrónico falsificados, implemente el Sender *Policy* Framework (SPF) implemente registros SPF en DNS y habilite la verificación del lado del receptor en los servidores de correo.
7.8	Escanee y bloquee todos los archivos adjuntos de correo electrónico que ingresen a la puerta de enlace de correo electrónico de la organización si contienen códigos maliciosos o tipos de archivos innecesarios para el negocio de la organización. Esta exploración debe realizarse antes de que el correo electrónico se coloque en la bandeja de entrada del usuario. Esto incluye filtrado de contenido de correo electrónico y filtrado de contenido web.
8.1	Utilice herramientas automatizadas para monitorear continuamente estaciones de trabajo, servidores y dispositivos móviles con antivirus, antispyware, firewalls personales y funcionalidad IPS basada en host. Todos los eventos de detección de malware deben enviarse a las herramientas de administración antimalware de la empresa y los servidores de registro de eventos
8.2	Emplear software antimalware que ofrece una infraestructura centralizada que compila información sobre reputación de archivos o que los administradores manualmente empujan las actualizaciones a todas las máquinas. Después de aplicar una actualización, los sistemas automatizados deben verificar que cada sistema ha recibido su actualización de firma.
8.3	Limitar el uso de dispositivos externos a aquellos con una necesidad empresarial aprobada y documentada. Monitor para el uso y el intento de uso de dispositivos externos. Configure ordenadores portátiles, estaciones de trabajo y servidores para que no ejecuten automáticamente contenido de medios extraíbles, como tokens USB, unidades de disco duro USB, CD / DVD, dispositivos *FireWire*, Y los recursos compartidos de red montados. Configure los sistemas para que lleven a cabo automáticamente una exploración antimalware de los medios extraíbles cuando se insertan.
8.4	Habilite las funciones antiexplotación, como la Prevención de Ejecución de Datos (DEP), la Asignación de Direcciones de Espacio de Direcciones (ASLR), la virtualización / contenedorización, etc. Para mayor protección, despliegue capacidades como el *Enhanced Mitigation Experience Toolkit* (EMET) que se puede configurar para aplicarlas Protege a un conjunto más amplio de aplicaciones y ejecutables.
8.5	Utilice herramientas antimalware basadas en la red para identificar ejecutables en todo el tráfico de red y utilice técnicas distintas a la detección basada en firmas para identificar y filtrar el contenido malintencionado antes de que llegue al punto final

8.6	Habilitar el registro de consultas del sistema de nombres de dominio (DNS) para detectar la búsqueda de nombres de host para dominios C2 maliciosos conocidos.
9.1	Asegúrese de que sólo se ejecuten en cada sistema puertos, protocolos y servicios con necesidades empresariales validadas.
9.2	Aplicar firewalls basados en host o herramientas de filtrado de puertos en sistemas finales, con una regla de denegación predeterminada que descarta todo el tráfico excepto los servicios y puertos que están explícitamente permitidos.
9.3	Realizar escaneos de puertos automatizados de forma regular contra todos los servidores clave y comparados con una línea base efectiva conocida. Si se descubre un cambio que no aparece en la línea base aprobada de la organización, se debe generar y revisar una alerta.
9.4	Compruebe cualquier servidor que sea visible desde Internet o una red no confiable y, si no es necesario para fines comerciales, muévalo a una VLAN interna y de una dirección privada.
9.5	Operar servicios críticos en máquinas host físicas o lógicas separadas, como servidores de DNS, archivos, correo, web y bases de datos.
9.6	Coloque los firewalls de aplicaciones frente a cualquier servidor crítico para verificar y validar el tráfico que va al servidor. Se debe bloquear cualquier servicio o tráfico no autorizado y generar una alerta.
10.1	Asegúrese de que cada sistema se respalda automáticamente al menos una vez por semana, y más a menudo para sistemas que almacenan información confidencial. Para ayudar a garantizar la capacidad de restaurar rápidamente un sistema desde una copia de seguridad, el sistema operativo, el software de aplicación y los datos de una máquina deben incluirse en el procedimiento de copia de seguridad general. Estos tres componentes de un sistema no tienen que ser incluidos en el mismo archivo de copia de seguridad o utilizar el mismo software de copia de seguridad. Debe haber varias copias de seguridad con el tiempo, de modo que, en caso de infección de malware, la restauración puede ser de una versión que se cree que es anterior a la infección original. Todas las políticas de respaldo deben cumplir con los requisitos reglamentarios u oficiales.
10.2	Pruebe los datos de los medios de copia de seguridad de forma periódica realiza un proceso de restauración de datos para asegurarse de que la copia de seguridad funciona correctamente.
10.3	Asegúrese de que las copias de seguridad están protegidas adecuadamente mediante la seguridad física o el cifrado cuando se almacenan, así como cuando se trasladan a través de la red. Esto incluye copias de seguridad remotas y servicios en la nube.
10.4	Asegúrese de que los sistemas clave tengan al menos un destino de copia de seguridad que no pueda direccionarse continuamente a través de llamadas al sistema operativo. Esto mitigará el riesgo de ataques como *CryptoLocker* que buscan cifrar o dañar datos en todos los datos compartidos de direcciones, incluidos los destinos de copia de seguridad.
11.1	Compare la configuración de cortafuegos, enrutador y conmutador con las configuraciones seguras estándar definidas para cada tipo de dispositivo de red que se utiliza en la organización. La configuración de seguridad de dichos dispositivos debe ser documentada, revisada y aprobada por un comité de control de cambios de la organización. Cualquier desviación de la configuración estándar o actualizaciones de la configuración estándar debe documentarse y aprobarse en un sistema de control de cambios.
11.2	Todas las nuevas reglas de configuración más allá de una configuración endurecida por la línea de base que permiten que el tráfico fluya a través de dispositivos de seguridad de red, como firewalls y IPS basados en red, deben documentarse y registrarse en un sistema de gestión de configuración. Nombre del individuo específico responsable de esa necesidad del negocio, y una duración esperada de la necesidad.
11.3	Utilice herramientas automatizadas para verificar configuraciones de dispositivos estándar y detectar cambios. Todas las alteraciones a tales archivos deben ser registradas y reportadas automáticamente al personal de seguridad.
11.4	Administrar dispositivos de red mediante autenticación de dos factores y sesiones cifradas.
11.5	Instale la última versión estable de las actualizaciones relacionadas con la seguridad en todos los dispositivos de red.

11.6	Los ingenieros de red utilizarán una máquina dedicada para todas las tareas administrativas o tareas que requieran un acceso elevado. Esta máquina estará aislada de la red primaria de la organización y no se permitirá el acceso a Internet. Esta máquina no debe usarse para leer correos electrónicos, componer documentos o navegar por Internet.
11.7	Administre la infraestructura de red a través de las conexiones de red que están separadas del uso empresarial de esa red, depende de VLAN separadas o, preferiblemente, de conectividad física totalmente diferente para sesiones de administración para dispositivos de red.
12.1	Denegar las comunicaciones con (o limitar el flujo de datos a) direcciones IP malintencionadas conocidas (listas negras) o limitar el acceso sólo a sitios de confianza (listas blancas). Las pruebas pueden realizarse periódicamente se envía paquetes desde direcciones IP de origen de *bogon* (direcciones IP no enrutables o no utilizadas) a la red para verificar que no se transmiten a través de los perímetros de la red. Las listas de direcciones de *bogon* están públicamente disponibles en Internet desde varias fuentes e indican una serie de direcciones IP que no deben usarse para el tráfico legítimo que atraviesa Internet.
12.2	En redes DMZ, configure sistemas de monitoreo (que pueden ser incorporados a los sensores IDS o desplegados como una tecnología separada) para registrar al menos información de encabezado de paquetes, y preferiblemente cabecera de paquete completo y cargas útiles del tráfico destinado o que pasa a través del borde de red. Este tráfico debe enviarse a un SIEM o al sistema de análisis de log para que los eventos puedan correlacionarse con todos los dispositivos de la red.
12.3	Implementar sensores IDS basados en redes en sistemas DMZ de Internet y extranet que busquen mecanismos de ataque inusuales y detecten el compromiso de estos sistemas. Estos sensores IDS basados en la red pueden detectar ataques mediante el uso de firmas, análisis de comportamiento de la red u otros mecanismos para analizar el tráfico.
12.4	Los dispositivos IPS basados en la red deben ser desplegados para complementar IDS al bloquear firmas mal conocidas o el comportamiento de ataques potenciales. A medida que los ataques se vuelven automatizados, los métodos como IDS suelen demorar la cantidad de tiempo que tarda alguien en reaccionar ante un ataque. Un IPS basado en red correctamente configurado puede proporcionar automatización para bloquear tráfico defectuoso. Cuando se evalúan los productos IPS basados en la red, incluya aquellos que utilicen técnicas distintas de la detección basada en firmas (como máquinas virtuales o enfoques basados en *sandbox*) para su consideración.
12.5	Diseñar e implementar perímetros de red para que todo el tráfico de red saliente a Internet pase por al menos una capa de aplicación que filtre el servidor proxy. El proxy debe admitir el descifrado del tráfico de red, el registro de sesiones TCP individuales, el bloqueo de direcciones URL específicas, nombres de dominio y direcciones IP para implementar una lista negra y la aplicación de listas blancas de sitios permitidos a los que se puede acceder a través del proxy. Las organizaciones deben forzar el tráfico saliente a Internet a través de un servidor proxy autenticado en el perímetro de la empresa.
12.6	Requiere todo el acceso de inicio de sesión remoto (incluye VPN, acceso telefónico y otras formas de acceso que permiten iniciar sesión en sistemas internos) para usar la autenticación de dos factores.
12.7	Todos los dispositivos empresariales que se registren de forma remota en la red interna deben ser administrados por la empresa, con control remoto de su configuración, software instalado y niveles de parche. Para dispositivos de terceros (por ejemplo, subcontratistas / vendedores), publique estándares mínimos de seguridad para el acceso a la red empresarial y realice una exploración de seguridad antes de permitir el acceso.
12.8	Analizar periódicamente las conexiones de canal posterior a Internet que pasan por alto la DMZ, incluidas las conexiones VPN no autorizadas y los hosts de doble sede conectados a la red empresarial ya otras redes a través de módems inalámbricos, de acceso telefónico u otros mecanismos.
12.9	Implemente la recopilación y el análisis de NetFlow a los flujos de red DMZ para detectar actividad anómala.

12.10	Para ayudar a identificar canales encubiertos que exfiltran datos a través de un servidor de seguridad, configure los mecanismos de seguimiento de sesión de firewall integrados incluidos en muchos firewalls comerciales para identificar sesiones TCP que duran un tiempo inusualmente largo para la organización y el dispositivo de firewall, alerta al personal sobre la fuente y el destino Direcciones asociadas con estas sesiones largas.
13.1	Realizar una evaluación de datos para identificar información sensible que requiera la aplicación de cifrado y controles de integridad
13.2	Implementar software de cifrado de disco duro aprobado en dispositivos móviles y sistemas que contienen datos confidenciales.
13.3	Despliegue una herramienta automatizada en los perímetros de la red que monitorea información sensible (por ejemplo, información personal identificable), palabras clave y otras características del documento para descubrir intentos no autorizados de exfiltrar datos a través de los límites de la red y bloquear tales transferencias mientras alerta al personal de seguridad de la información.
13.4	Realizar análisis periódicos de máquinas servidoras que utilizan herramientas automatizadas para determinar si los datos confidenciales (por ejemplo, información personal identificable, salud, tarjeta de crédito o información clasificada) están presentes en el sistema en texto claro. Estas herramientas, que buscan patrones que indican la presencia de información confidencial, pueden ayudar a identificar si un negocio o proceso técnico con un filtro de información confidencial.
13.5	Si no hay ninguna necesidad comercial de soportar dichos dispositivos, configure los sistemas para que no escriban datos en tokens USB o unidades de disco duro USB. Si se requieren estos dispositivos, se debe utilizar software empresarial que pueda configurar sistemas para permitir el acceso a dispositivos USB específicos (basados en el número de serie u otra propiedad única) y que puedan cifrar automáticamente todos los datos colocados en dichos dispositivos. Se debe mantener un inventario de todos los dispositivos autorizados.
13.6	Utilice soluciones DLP basadas en red para supervisar y controlar el flujo de datos dentro de la red. Se deben anotar las anomalías que excedan los patrones de tráfico normales y tomar las medidas apropiadas para abordarlos.
13.7	Supervisar todo el tráfico que sale de la organización y detectar cualquier uso no autorizado del cifrado. Los atacantes suelen usar un canal encriptado para evitar los dispositivos de seguridad de red. Por lo tanto, es esencial que las organizaciones sean capaces de detectar conexiones deshonestas, terminar la conexión y remediar el sistema infectado.
13.8	Bloquear el acceso a sitios web conocidos de transferencia de archivos y correo electrónico de exfiltración.
13.9	Utilice la prevención de pérdida de datos (DLP) basada en host para aplicar las ACL incluso cuando se copian datos de un servidor. En la mayoría de las organizaciones, el acceso a los datos es controlado por ACL que se implementan en el servidor. Una vez que los datos se han copiado en un sistema de escritorio, las ACL ya no se aplican y los usuarios pueden enviar los datos a quien quieran.
14.1	Segmente la red en base a la etiqueta o nivel de clasificación de la información almacenada en los servidores. Localice toda la información confidencial en VLANS separados con filtrado de cortafuegos para garantizar que sólo las personas autorizadas sólo puedan comunicarse con los sistemas necesarios para cumplir con sus responsabilidades específicas.
14.2	Toda la comunicación de información confidencial sobre redes menos confiables debe ser cifrada. Siempre que la información fluya a través de una red con un nivel de confianza más bajo, la información debe ser cifrada.
14.3	Todos los conmutadores de red permitirán que las redes de área local privada (VLAN) para redes de estaciones de trabajo segmentadas limiten la capacidad de los dispositivos de una red de comunicarse directamente con otros dispositivos de la subred y limitar la capacidad de los atacantes de moverse lateralmente para comprometer sistemas vecinos.

14.4	Toda la información almacenada en los sistemas se protegerá con listas de control de acceso específicas de sistema de archivos, de recurso compartido de red, de reclamaciones, de aplicaciones o de bases de datos. Estos controles harán cumplir el principio de que sólo las personas autorizadas deben tener acceso a la información basada en su necesidad de acceder a la información como parte de sus responsabilidades.
14.5	La información sensible almacenada en los sistemas se cifrará en reposo y requerirá un mecanismo de autenticación secundario, no integrado en el sistema operativo, para acceder a la información.
14.6	Imponga registro de auditoría detallado para el acceso a datos no públicos y autenticación especial para datos confidenciales.
14.7	Los conjuntos de datos archivados o los sistemas a los que no se accede regularmente por la organización se eliminarán de la red de la organización. Estos sistemas sólo se utilizarán como sistemas autónomos (desconectados de la red) por la unidad de negocio que necesite ocasionalmente utilizar el sistema o completamente virtualizado y apagado hasta que sea necesario.
15.1	Asegúrese de que cada dispositivo inalámbrico conectado a la red coincida con un perfil de configuración y seguridad autorizado, con un propietario documentado de la conexión y una necesidad de negocio definida. Las organizaciones deben denegar el acceso a los dispositivos inalámbricos que no tienen tal configuración y perfil.
15.2	Configurar las herramientas de análisis de vulnerabilidades de red para detectar puntos de acceso inalámbricos conectados a la red cableada. Los dispositivos identificados deben reconciliarse con una lista de puntos de acceso inalámbricos autorizados. Los puntos de acceso no autorizados (es decir, deshonestos) deben desactivarse.
15.3	Utilice sistemas inalámbricos de detección de intrusiones (WIDS) para identificar dispositivos inalámbricos deshonestos y detectar intentos de ataque y compromisos exitosos. Además de WIDS, todo el tráfico inalámbrico debe ser supervisado por WIDS a medida que el tráfico pasa a la red cableada.
15.4	Si se ha identificado una necesidad de negocio específica para el acceso inalámbrico, configure el acceso inalámbrico en las máquinas cliente para permitir el acceso sólo a las redes inalámbricas autorizadas. Para los dispositivos que no tienen un propósito esencial de negocio inalámbrico, desactive el acceso inalámbrico en la configuración de hardware (sistema básico de entrada / salida o interfaz de firmware extensible).
15.5	Asegúrese de que todo el tráfico inalámbrico aproveche al menos el cifrado AES (*Advanced Encryption* Standard) utilizado con al menos la protección *Wi*-Fi *Protected* Access 2 (WPA2).
15.6	Asegúrese de que las redes inalámbricas usen protocolos de autenticación como Protocolo de autenticación extensible (EAP / TLS), que proporcionan protección de credenciales y autenticación mutua.
15.7	Deshabilite las capacidades de red inalámbrica punto a punto en clientes inalámbricos.
15.8	Deshabilite el acceso periférico inalámbrico de dispositivos (como Bluetooth), a menos que este acceso sea pertinente para una necesidad de negocio documentada.
15.9	Crear redes de área local virtual (VLAN) separadas para sistemas BYOD u otros dispositivos no confiables. El acceso a Internet desde esta VLAN debe pasar por lo menos la misma frontera que el tráfico corporativo. El acceso empresarial desde esta VLAN debe ser tratado como no fiable y filtrado y auditado en consecuencia.
16.1	Revise todas las cuentas del sistema y deshabilite cualquier cuenta que no pueda asociarse con un proceso de empresa y propietario.
16.2	Asegúrese de que todas las cuentas tienen una fecha de caducidad que se supervisa y se aplica.
16.3	Establecer y seguir un proceso para revocar el acceso al sistema de cuentas inmediatamente después de la terminación de un empleado o contratista. La desactivación en lugar de eliminar cuentas permite la conservación de pistas de auditoría.
16.4	Supervisar regularmente el uso de todas las cuentas, el usuario automáticamente se elimina después de un período estándar de inactividad.
16.5	Configure bloqueos de pantalla en sistemas para limitar el acceso a estaciones de trabajo desatendidas.

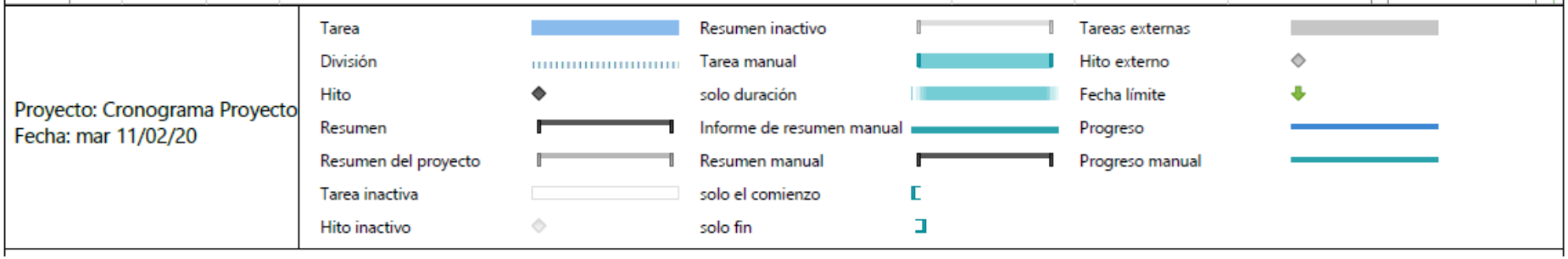
16.6	Supervisar el uso de la cuenta para determinar las cuentas inactivas, este notifica al usuario o al administrador del usuario. Deshabilite dichas cuentas si no es necesario, o documenta y supervisa las excepciones (por ejemplo, las cuentas de mantenimiento del proveedor necesarias para la recuperación del sistema o las operaciones de continuidad). Exigir que los gerentes coincidan con empleados activos y contratistas con cada cuenta perteneciente a su personal administrado. Los administradores de sistemas o de seguridad deben desactivar las cuentas que no están asignadas a miembros válidos de la fuerza de trabajo.
16.7	Utilice y configure los bloqueos de cuenta de tal manera que después de un número definido de intentos de inicio de sesión fallidos, la cuenta se bloquee durante un período de tiempo estándar.
16.8	Supervise los intentos de acceder a cuentas desactivadas a través del registro de auditoría.
16.9	Configurar el acceso para todas las cuentas a través de un punto centralizado de autenticación, por ejemplo, Active Directory o LDAP. Configure los dispositivos de red y de seguridad para la autenticación centralizada también.
16.10	Haga un perfil del uso típico de la cuenta de cada usuario que tiene el acceso normal a la hora del día y la duración del acceso. Deben generarse informes que indiquen a los usuarios que se hayan conectado durante horas inusuales o hayan excedido su duración normal de inicio de sesión. Esto incluye marcar el uso de las credenciales del usuario desde un equipo distinto de los equipos en los que el usuario generalmente trabaja.
16.11	Requiere autenticación multifactorial para todas las cuentas de usuario que tengan acceso a datos o sistemas sensibles. La autenticación de múltiples factores se puede lograr mediante tarjetas inteligentes, certificados, tokens de contraseña de tiempo único (OTP) o datos biométricos.
16.12	Si no se admite la autenticación de varios factores, se requerirá que las cuentas de usuario utilicen contraseñas largas en el sistema (más de 14 caracteres).
16.13	Asegúrese de que todos los nombres de usuario de la cuenta y las credenciales de autenticación se transmiten a través de las redes que usan canales cifrados.
16.14	Compruebe que todos los archivos de autenticación están encriptados o hash y que no se puede acceder a estos archivos sin privilegios de administrador o *root*. Auditar todo el acceso a archivos de contraseñas en el sistema.
17.1	Realizar análisis de brechas para ver qué habilidades necesitan los empleados y qué comportamientos los empleados no están en cumplimiento según normas de la empresa, esta información para construir una línea de base de formación y sensibilización para todos los empleados.
17.2	Ofrecer capacitación para llenar el vacío de habilidades. Si es posible, use un personal más alto para impartir la capacitación. Una segunda opción es que los profesores externos proporcionen capacitación en el lugar de manera que los ejemplos utilizados sean directamente pertinentes. Si usted tiene un pequeño número de personas para entrenar, use conferencias de capacitación o capacitación en línea para llenar las lagunas.
17.3	Implementar un programa de concienciación de seguridad que (1) se centre sólo en los métodos comúnmente utilizados en las intrusiones que pueden ser bloqueados a través de la acción individual, (2) se entrega en corto módulos en línea conveniente para los empleados (3) se actualiza con frecuencia (al menos anualmente) Representan las técnicas de ataque más recientes, (4) están obligadas a ser completadas por todos los empleados por lo menos una vez al año, y (5) son supervisadas de manera fiable para que los empleados se completen.
17.4	Validar y mejorar los niveles de conciencia a través de pruebas periódicas para ver si los empleados hacen clic en un enlace de correo electrónico sospechoso o proporcionar información confidencial en el teléfono sin seguir los procedimientos adecuados para la autenticación de una persona que llama; Se debe proporcionar capacitación específica a aquellos que son víctimas del ejercicio.
17.5	Utilice las evaluaciones de habilidades de seguridad para cada una de las funciones de misión crítica para identificar brechas de habilidades. Utilice ejemplos prácticos del mundo real para medir el dominio. Si no tiene tales evaluaciones, use una de las competiciones en línea disponibles que simulan escenarios del mundo real para cada uno de los trabajos identificados con el fin de medir el dominio de las habilidades

18.1	Para todo el software de aplicación adquirido, compruebe que la versión que está todavía es compatible con el proveedor. Si no es así, actualice la versión más reciente e instale todos los parches y recomendaciones de seguridad del fabricante.
18.2	Proteja las aplicaciones web mediante la implementación de firewalls de aplicaciones web (WAF) que inspeccionan todo el tráfico que fluye hacia la aplicación web para ataques comunes de aplicaciones web, entre otros, ataques de scripts entre sitios, inyección de SQL, inyección de comandos y ataques de directorio. Para las aplicaciones que no están basadas en web, firewalls de aplicación específicos deben desplegarse si dichas herramientas están disponibles para el tipo de aplicación dado. Si el tráfico está encriptado, el dispositivo debe sentarse detrás del cifrado o ser capaz de descifrar el tráfico antes del análisis. Si ninguna de las opciones es apropiada, se debe implementar un firewall de aplicaciones web basado en host.
18.3	Para software desarrollado internamente, asegúrese de que la comprobación explícita de errores se realiza y documenta para todas las entradas, incluye el tamaño, el tipo de datos y los rangos o formatos aceptables.
18.4	Pruebe aplicaciones web desarrolladas internamente y de terceros para detectar fallas de seguridad comunes, escáneres automatizados de aplicaciones web remotas antes de la implementación, siempre que se realicen actualizaciones en la aplicación y periódicamente. En particular, la validación de entrada y las rutinas de codificación de salida del software de aplicación deben ser revisadas y probadas.
18.5	No muestre mensajes de error del sistema a los usuarios finales (desinfección de salida).
18.6	Mantener ambientes separados para sistemas de producción y no producción. Normalmente, los desarrolladores no deben tener acceso sin supervisión a los entornos de producción.
18.7	Para aplicaciones que dependen de una base de datos, utilice plantillas de configuración de endurecimiento estándar. Todos los sistemas que forman parte de procesos críticos de negocio también deben ser probados.
18.8	Asegúrese de que todo el personal de desarrollo de software recibe capacitación en la escritura de código seguro para su entorno de desarrollo específico.
18.9	Para las aplicaciones desarrolladas internamente, asegúrese de que los artefactos de desarrollo (datos de ejemplo y secuencias de comandos, bibliotecas no utilizadas, componentes, código de depuración o herramientas) no estén incluidos en el software desplegado ni accesibles en el entorno de producción.
19.1	Asegúrese de que hay procedimientos escritos de respuesta a incidentes que incluyen una definición de roles de personal para manejar incidentes. Los procedimientos deben definir las fases de manejo de incidentes.
19.2	Asignar títulos de trabajo y deberes para manejar incidentes de computadora y red a individuos específicos.
19.3	Definir al personal directivo que apoyará el proceso de manejo de incidentes que realizan en roles clave de toma de decisiones.
19.4	Elaborar estándares en toda la organización para el tiempo requerido para que los administradores del sistema y otro personal reporten eventos anómalos al equipo de manejo de incidentes, los mecanismos para dicha notificación y el tipo de información que debe incluirse en la notificación del incidente. Esta notificación debe incluir también la notificación al Equipo de Respuesta a Emergencias de la Comunidad de conformidad con todos los requisitos legales o reglamentarios para la participación de esa organización en incidentes informáticos.
19.5	Reúna y mantenga información sobre los datos de contacto de terceros que se utilizará para informar un incidente de seguridad (por ejemplo, mantener una dirección de correo electrónico de security@organization.com o una página web http://organization.com/security).
19.6	Publicar información para todo el personal, incluye empleados y contratistas, con respecto a reportar anomalías informáticas y alarmas al equipo de manejo de incidentes. Dicha información debe incluirse en las actividades habituales de concienciación de los empleados.
19.7	Realizar sesiones de escenarios de incidentes periódicos para el personal asociado con el equipo de manejo de incidentes para asegurarse de que entienden las amenazas y riesgos actuales, así como sus responsabilidades en apoyar al equipo de manejo de incidentes.

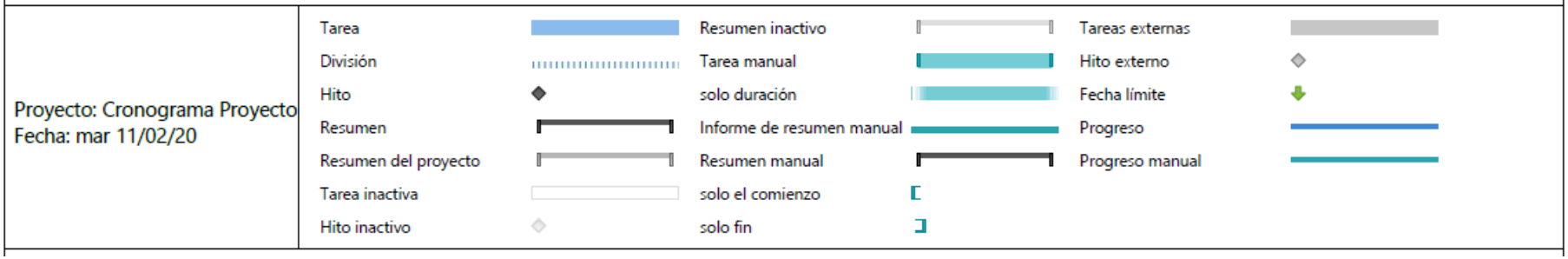
20.1	Realizar pruebas de penetración externas e internas regulares para identificar vulnerabilidades y vectores de ataque que pueden utilizarse para explotar con éxito los sistemas empresariales. Las pruebas de penetración deben realizarse fuera del perímetro de la red (es decir, la Internet o las frecuencias inalámbricas alrededor de una organización), así como desde dentro de sus límites (es decir, en la red interna) para simular ataques externos e internos.
20.2	Las cuentas de usuario o de sistema utilizadas para realizar pruebas de penetración deben ser controladas y monitoreadas para asegurarse de que sólo se utilizan con fines legítimos y se eliminan o se restauran a funciones normales una vez finalizadas las pruebas.
20.3	Realizar periódicamente ejercicios de equipo rojo para probar la preparación organizacional para identificar y detener los ataques o para responder con rapidez y eficacia.
20.4	Incluya pruebas para la presencia de información del sistema desprotegida y artefactos que serían útiles para los atacantes, se incluye diagramas de red, archivos de configuración, informes de prueba de penetración más antiguos, correos electrónicos o documentos que contengan contraseñas u otra información crítica para la operación del sistema.
20.5	Planifique metas claras de la prueba de penetración en sí misma con ataques combinados en mente, que identifiquen la meta de la máquina o el activo objetivo. Muchos ataques estilo APT implementan múltiples vectores, a menudo ingeniería social combinada con la explotación de la red o de la red. El equipo rojo o las pruebas automatizadas que capturan ataques pivotados y *multi-vectoriales* ofrecen una evaluación más realista de la postura de seguridad y el riesgo de los activos críticos.
20.6	Utilice las herramientas de análisis de vulnerabilidad y penetración. Los resultados de las evaluaciones de escaneo de vulnerabilidad deben utilizarse como punto de partida para orientar y enfocar los esfuerzos de pruebas de penetración.
20.7	Siempre que sea posible, asegúrese de que los resultados de los Equipos Rojos estén documentados así utilizan estándares abiertos y legibles por máquina (por ejemplo, SCAP). Elaborar un método de puntuación para determinar los resultados de los ejercicios del Equipo Rojo para que los resultados puedan compararse con el tiempo.
20.8	Cree un banco de pruebas que imite un entorno de producción para pruebas de penetración específicas y ataques del Red Team contra elementos que normalmente no se prueban en la producción, como ataques contra el control de supervisión y adquisición de datos y otros sistemas de control.

ANEXO 2 **Cronograma de actividades**

Id	Modo de tarea	EDT	Nombre de tarea	Duración	Comienzo	Fin
1		**1**	**Cronograma Proyecto**	**183 días**	**mié 01/05/19**	**vie 10/01/20**
2		**1.1**	**INVESTIGACION TESIS**	**31 días**	**mié 01/05/19**	**mié 12/06/19**
3		1.1.1	Investigacion fundamentación teórica	18 días	mié 01/05/19	vie 24/05/19
4		1.1.2	Investigación Marco metodológico	4 días	lun 20/05/19	jue 23/05/19
5		1.1.3	Estudio de diseño de redes	13 días	lun 27/05/19	mié 12/06/19
6		**1.2**	**Planteamiento**	**33 días**	**lun 10/06/19**	**mié 24/07/19**
7		1.2.1	Selección y análisis de personal	4 días	lun 10/06/19	jue 13/06/19
8		1.2.2	Análisis de red	5 días	lun 17/06/19	vie 21/06/19
9		1.2.3	Análisis de servicios habilitados	3 días	lun 24/06/19	mié 26/06/19
10		1.2.4	Análisis de productos	10 días	lun 01/07/19	vie 12/07/19
11		1.2.5	Estudio de la red	10 días	jue 11/07/19	mié 24/07/19
12		**1.3**	**Definición de alcances**	**10 días**	**lun 22/07/19**	**vie 02/08/19**
13		1.3.1	Elaboración de cronograma base	2 días	lun 22/07/19	mar 23/07/19
14		1.3.2	Análisis de puntos clave	9 días	mar 23/07/19	vie 02/08/19
15		1.3.3	Reunión de kickoff	2 días	jue 01/08/19	vie 02/08/19
16		**1.4**	**Revisión de propuesta y diseño**	**20 días**	**sáb 03/08/19**	**vie 30/08/19**
17		1.4.1	Elaboración de diseño	13 días	sáb 03/08/19	mar 20/08/19
18		1.4.2	Borrador entregable de diseño de la red	8 días	vie 16/08/19	mar 27/08/19
19		1.4.3	Propuesta presentada al personal de la empresa	3 días	lun 26/08/19	mié 28/08/19
20		1.4.4	Aprobación y autorización de acceso y configuraciones a los equipos	2 días	jue 29/08/19	vie 30/08/19
21		**1.5**	**Adecuación del área**	**28 días**	**lun 02/09/19**	**mié 09/10/19**
22		1.5.1	Reconocimiento de equipos	9 días	lun 02/09/19	jue 12/09/19



Id	Modo de tarea	EDT	Nombre de tarea	Duración	Comienzo	Fin
23		1.5.2	Reconocimiento del área	3 días	mié 11/09/19	vie 13/09/19
24		1.5.3	Recepción de equipos	6 días	lun 16/09/19	sáb 21/09/19
25		1.5.4	Análisis de servicios habilitados	8 días	dom 22/09/19	mar 01/10/19
26		1.5.5	Análisis de seguridad y control	8 días	lun 30/09/19	mié 09/10/19
27		**1.6**	**Implementación y revisión de cableado**	**25 días**	**mar 08/10/19**	**lun 11/11/19**
28		1.6.1	Revisión de puntos de conexión	9 días	mar 08/10/19	vie 18/10/19
29		1.6.2	Acceso a servicios gestionados	9 días	jue 17/10/19	mar 29/10/19
30		1.6.3	Revisión e implementación de equipos	12 días	vie 25/10/19	lun 11/11/19
31		**1.7**	**Implementación de hardware y software**	**30 días**	**mié 06/11/19**	**mar 17/12/19**
32		1.7.1	Sincronización de productos de seguridad	7 días	mié 06/11/19	jue 14/11/19
33		1.7.2	Asignación de equipos para la red	9 días	mié 13/11/19	lun 25/11/19
34		1.7.3	Configuraciones en los equipos	6 días	jue 21/11/19	vie 29/11/19
35		1.7.4	Pruebas de conexión lógica	6 días	jue 28/11/19	jue 05/12/19
36		1.7.5	Implementación de plataforma de seguridad y control	10 días	mié 04/12/19	mar 17/12/19
37		**1.8**	**Fin del diseño, paso a producción**	**20 días**	**sáb 14/12/19**	**vie 10/01/20**
38		1.8.1	Entregables y verificación	21 días	sáb 14/12/19	vie 10/01/20



C20	P28	C20.P28	Servicios de Ethical Hacking	Servicios de evaluación de vulnerabilidades y pruebas de penetración para identificar escenarios de riesgo de ataques e impacto	Informes de resultados de la evaluación Planes de tratamiento de brechas	Política para la Respuesta a Incidentes de Seguridad de la Información	Pruebas semestrales	Número de brechas identificadas por período Cumplimiento de planes de tratamiento No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información

ANEXO 3 Análisis de controles con el diseño propuesto

ID CONTROL	ID PROYECTO	ID	Proyectos	Producto / Servicio	Documentación	Normativa	Seguimiento	Indicadores	Mejora Continua
C01	P01	C01.P01	Implementación de Herramienta de Inventario de Hardware y Software	Herramienta automatizada de inventario de hardware y software	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de Inventarios Política de Auditoría	Actividades de auditoría cada 3 meses Actividades de actualización una vez por año	Activos no autorizados identificados por período Porcentaje de efectividad de inventario	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C01	P02	C01.P02	Implementación de control de acceso de infraestructura tecnológica	Herramienta NAC (*network access* control)	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de Control de acceso a las redes privadas Política de Auditoria	Actividades de auditoría cada 3 meses Monitoreo persistente	Activos no autorizados identificados por período	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C01	P03	C01.P03	Implementación de Correlación de Eventos	Herramienta de Correlación de eventos: Procesamiento de Logs Monitoreo de *Netflow* Monitoreo de disponibilidad de activos de red Monitoreo de IDS	Manual de Operación Informe de configuración Información de capacitación	Política de Respuesta a Incidentes de Seguridad de la Información	Monitoreo persistente	Activos no autorizados identificados por período Alarmas detectadas por período	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C01	P04	C01.P04	Operación de Respuesta a incidentes de seguridad	Personal operativo en monitoreo, investigación y gestión de alarmas e incidentes de seguridad de información	Proceso de gestión de alarmas o incidentes de seguridad Roles y responsabilidades en escenarios críticos	Política de Respuesta a Incidentes de Seguridad de la Información	Monitoreo persistente	Número de alarmas identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información

C02	P01	C02.P01	Implementación de Herramienta de Inventario de Hardware y Software	Herramienta automatizada de inventario de hardware y software	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de Inventarios Listado de software autorizado Política de Auditoría	Actividades de auditoría cada 3 meses Actividades de actualización una vez por año	Software no autorizado identificado por período Porcentaje de efectividad de inventario	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C02	P05	C02.P05	Implementación de seguridad de *endpoint*	Herramienta para protección de *endpoint*, control de dispositivos y aplicaciones	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política para el Control de Aplicaciones Listado de software autorizado Política de Auditoría	Actividades de auditoría cada 3 meses Actividades de actualización una vez por año	Software no autorizado identificado por período Porcentaje de efectividad de inventario	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C02	P17	C02.P17	Gestión de distribución de actualizaciones y parches de seguridad	Herramientas de distribución de actualizaciones y parches de seguridad para sistemas operativos, aplicaciones, bases de datos y hardware de comunicaciones	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de Actualizaciones Política de Auditoría	Actividades de auditoría cada 3 meses Actividades de actualización una vez por año	Activos no actualizados identificado por período	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C03	P06	C03.P06	Gestionar protocolos de *Hardening* y configuraciones seguras para *endpoints* y servidores	Procedimiento de *Hardening* y Configuración Segura de Estaciones de trabajo y servidores	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de *Hardening* Política de Auditoría	Actividades de auditoría cada 3 meses	Configuraciones no seguras identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información

C03	P07	C03.P07	Gestionar respaldos de sistema operativo, software de aplicaciones y los datos, incluidos en el procedimiento de copia de seguridad general de Endpoints y servidores	Herramienta de respaldo, pruebas de verificación de integridad, gestión de información antigua y planes de recuperación de datos	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política para Respaldos y para la Gestión de Archivos Política de Auditoría	Respaldo de información Actividades de auditoría cada 3 meses	Pruebas de efectividad de respaldos No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C03	P03	C03.P03	Implementación de monitoreo de integridad de archivos orientado a validar configuraciones críticas de sistema	Herramienta de Correlación de eventos: Procesamiento de Logs File Integrity Monitoring activado	Manual de Operación Informe de configuración Información de capacitación	Política para Respuesta a Incidentes de Seguridad de la Información	Monitoreo persistente	Activos no autorizados identificados por período Alarmas detectadas por período	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C03	P04	C03.P04	Operación de Respuesta a incidentes de seguridad	Personal operativo en monitoreo, investigación y gestión de alarmas e incidentes de seguridad de información	Proceso de gestión de alarmas o incidentes de seguridad Roles y responsabilidades en escenarios críticos	Política para Respuesta a Incidentes de Seguridad de la Información	Monitoreo persistente	Número de alarmas identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C03	P08	C03.P08	Implementación de gestión centralizada de configuraciones y perfiles de usuario	Implementación de Active Directory, gestión de usuarios, perfiles y configuraciones centralizado	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de *Hardening* Política de gestión de usuarios Política de Auditoría	Actividades de auditoría cada 3 meses	Configuraciones no seguras identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C04	P09	C04.P09	Implementar un proceso de evaluación y remediación de vulnerabilidades periódico	Implementación de herramientas de escaneo de vulnerabilidades que permita la identificación tanto a nivel de IP como a nivel de aplicación	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política para la Gestión de Vulnerabilidades Política de Auditoría	Tareas de escaneo de vulnerabilidades periódicas Actividades de auditoría cada 3 meses	Número de vulnerabilidades identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información

C04	P03	C04.P03	Implementación de Correlación de Eventos	Herramienta de Correlación de eventos: Monitoreo de vulnerabilidades por activo Seguimiento de tareas de remediación	Manual de Operación Informe de configuración Información de capacitación	Política para la Respuesta a Incidentes de Seguridad de la Información	Monitoreo persistente	Número de vulnerabilidades identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C04	P04	C04.P04	Operación de Respuesta a incidentes de seguridad	Personal operativo en monitoreo, investigación y gestión de alarmas e incidentes de seguridad de información	Proceso de gestión de alarmas o incidentes de seguridad Roles y responsabilidades en escenarios críticos	Política para la Respuesta a Incidentes de Seguridad de la Información	Monitoreo persistente	Número de alarmas identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C04	P05	C04.P05	Implementación de seguridad de endpoint	Herramienta para protección de endpoint, control de dispositivos y aplicaciones	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de Gestión de Vulnerabilidades Política de Auditoría	Actividades de auditoría cada 3 meses	Número de vulnerabilidades identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C04	P08	C04.P08	Implementación de gestión centralizada de configuraciones y perfiles de usuario	Implementación de Active Directory, gestión de usuarios, perfiles y configuraciones centralizado	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de Hardening Política para la gestión de los usuarios Política de Auditoría	Actividades de auditoría cada 3 meses	Configuraciones no seguras identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C04	P10	C04.P10	Implementación de herramientas de protección de aplicaciones y bases de datos	Implementación de herramientas de protección de aplicaciones y bases de datos, a través de parchado virtual, mitiguen riesgos de	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios	Política de Seguridad interna Política de Auditoría	Actividades de auditoría cada 3 meses	Número de vulnerabilidades identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información

				ataques internos o externos	Información de capacitación				
C05	P08	C05.P08	Implementación de gestión centralizada de configuraciones y perfiles de usuario	Implementación de Active Directory, gestión de usuarios, perfiles y configuraciones centralizado	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de *Hardening* Política para la gestión de los usuarios Política de Auditoría	Actividades de auditoría cada 3 meses	Configuraciones de usuarios y perfiles gestionados por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C05	P11	C05.P11	Gestión de contraseñas seguras	Implementación de protocolos de contraseñas seguras en todos los sistemas críticos de la organización	Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política para la gestión de los usuarios Política de contraseñas Política de Auditoría	Actividades de auditoría cada 3 meses	No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C05	P03	C05.P03	Implementación de Correlación de Eventos	Herramienta de Correlación de eventos: Monitoreo de accesos de usuarios	Manual de Operación Informe de configuración Información de capacitación	Política para la Respuesta a Incidentes de Seguridad de la Información	Monitoreo persistente	Número de accesos identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C05	P04	C05.P04	Operación de Respuesta a incidentes de seguridad	Personal operativo en monitoreo, investigación y gestión de alarmas e incidentes de seguridad de información	Proceso de gestión de alarmas o incidentes de seguridad Roles y responsabilidades en escenarios críticos	Política para la Respuesta a Incidentes de Seguridad de la Información	Monitoreo persistente	Número de alarmas identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C05	P12	C05.P12	Implementar doble factor de autenticación para acceso a sistemas críticos	Implementar una herramienta de doble factor de autenticación que permita mitigar el riesgo de acceso a	Manual de Operación Informe de configuración Repositorio de	Política para la gestión de los usuarios Política de contraseñas	Actividades de auditoría cada 3 meses	No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de

				sistemas críticos de personal no autorizado	Gestión de Cambios Información de capacitación	Política de Auditoría			seguridad de información
C06	P13	C06.P13	Implementar un servidor NTP para asegurar la sincronía de registros de tiempo para correlación de eventos	Implementar un servidor NTP para la red interna	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de Auditoría	Actividades de auditoría cada 3 meses	No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C06	P03	C06.P03	Implementación de Correlación de Eventos	Herramienta de Correlación de eventos: Monitoreo de accesos de usuarios	Manual de Operación Informe de configuración Información de capacitación	Política de Respuesta a Incidentes de Seguridad de la Información	Monitoreo persistente	Número de accesos identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C06	P04	C06.P04	Operación de Respuesta a incidentes de seguridad	Personal operativo en monitoreo, investigación y gestión de alarmas e incidentes de seguridad de información	Proceso de gestión de alarmas o incidentes de seguridad Roles y responsabilidades en escenarios críticos	Política de Respuesta a Incidentes de Seguridad de Información	Monitoreo persistente	Número de alarmas identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C07	P01	C07.P01	Implementación de Herramienta de Inventario de Hardware y Software	Herramienta automatizada de inventario de hardware y software	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de Inventarios Política de Auditoría	Actividades de auditoría cada 3 meses Actividades de actualización una vez por año	Activos no autorizados identificados por período Porcentaje de efectividad de inventario	Revisiones periódicas de cumplimiento en el comité de seguridad de información

C07	P14	C07.P14	Implementación de seguridad perimetral	Herramienta de gestión de seguridad perimetral para filtrado de navegación, correo, prevención de intrusiones y protección frente a ataques perimetrales	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de Seguridad Perimetral Política de Auditoría	Actividades de auditoría cada 3 meses Monitoreo persistente	Número de eventos de seguridad identificados por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C07	P03	C07.P03	Implementación de Correlación de Eventos	Herramienta de Correlación de eventos: Monitoreo de accesos de usuarios	Manual de Operación Informe de configuración Información de capacitación	Política para la Respuesta a Incidentes de Seguridad de la Información	Monitoreo persistente	Número de accesos identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C07	P04	C07.P04	Operación de Respuesta a incidentes de seguridad	Personal operativo en monitoreo, investigación y gestión de alarmas e incidentes de seguridad de información	Proceso de gestión de alarmas o incidentes de seguridad Roles y responsabilidades en escenarios críticos	Política para la Respuesta a Incidentes de Seguridad de la Información	Monitoreo persistente	Número de alarmas identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C07	P08	C07.P08	Implementación de gestión centralizada de configuraciones y perfiles de usuario	Implementación de Active Directory, gestión de usuarios, perfiles y configuraciones centralizado	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de h*ardening* Política de gestión de usuarios Política de Auditoría	Actividades de auditoría cada 3 meses	Configuraciones de usuarios y perfiles gestionados por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C08	P05	C08.P05	Implementación de seguridad de endpoint	Herramienta para protección de endpoint, control de dispositivos y aplicaciones	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios	Política para Seguridad Interna Política de Auditoría	Actividades de auditoría cada 3 meses	Número de vulnerabilidades identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información

					Información de capacitación				
C08	P03	C08.P03	Implementación de Correlación de Eventos	Herramienta de Correlación de eventos: Monitoreo de accesos de usuarios	Manual de Operación Informe de configuración Información de capacitación	Política para la Respuesta a Incidentes de Seguridad de la Información	Monitoreo persistente	Número de accesos identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C08	P04	C08.P04	Operación de Respuesta a incidentes de seguridad	Personal operativo en monitoreo, investigación y gestión de alarmas e incidentes de seguridad de información	Proceso de gestión de alarmas o incidentes de seguridad Roles y responsabilidades en escenarios críticos	Política para la Respuesta a Incidentes de Seguridad de la Información	Monitoreo persistente	Número de alarmas identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C08	P01	C08.P01	Implementación de Herramienta de Inventario de Hardware y Software	Herramienta automatizada de inventario de hardware y software	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de Inventarios Política de Auditoría	Actividades de auditoría cada 3 meses Actividades de actualización una vez por año	Activos no autorizados identificados por período Porcentaje de efectividad de inventario	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C08	P15	C08.P15	Implementación de protección anti-ataques persistentes avanzados o ataques dirigidos	Herramienta Anti APTs para protección de ataques de cero o de día uno	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política para la Respuesta a Incidentes de Seguridad de la Información	Monitoreo persistente	Número de alarmas identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información

C09	P01	C09.P01	Implementación de Herramienta de Inventario de Hardware y Software	Herramienta automatizada de inventario de hardware y software	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política para Inventarios Política de Auditoría	Actividades de auditoría cada 3 meses Actividades de actualización una vez por año	Activos no autorizados identificados por período Porcentaje de efectividad de inventario	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C09	P06	C09.P06	Gestionar protocolos de *Hardening* y configuraciones seguras para endpoints y servidores	Procedimiento de *Hardening* y configuración segura de estaciones de trabajo y servidores	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de *Hardening* Política de Auditoría	Actividades de auditoría cada 3 meses	Configuraciones no seguras identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C09	P14	C09.P14	Implementación de seguridad perimetral	Herramienta de gestión de seguridad perimetral para filtrado de navegación, correo, prevención de intrusiones y protección frente a ataques perimetrales	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política para la Seguridad Perimetral Política de Auditoría	Actividades de auditoría cada 3 meses Monitoreo persistente	Número de eventos de seguridad identificados por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C09	P03	C09.P03	Implementación de Correlación de Eventos	Herramienta de Correlación de eventos: Monitoreo de accesos de usuarios	Manual de Operación Informe de configuración Información de capacitación	Política para la Respuesta a Incidentes de Seguridad de la Información	Monitoreo persistente	Número de accesos identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C09	P04	C09.P04	Operación de Respuesta a incidentes de seguridad	Personal operativo en monitoreo, investigación y gestión de alarmas e incidentes de seguridad de información	Proceso de gestión de alarmas o incidentes de seguridad Roles y responsabilidades	Política para la Respuesta a Incidentes de Seguridad de la Información	Monitoreo persistente	Número de alarmas identificadas por período No conformidades	Revisiones periódicas de cumplimiento en el comité de seguridad de información

					en escenarios críticos			de auditoría interna	
C09	P16	C09.P16	Gestión de seguridad en red interna	Diseño de red segura: Diseño de VLAN, DMZ de aplicaciones, servicios WEB externos y Bases de Datos, control de puertos y comunicaciones	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política para la Seguridad de comunicaciones Política de Auditoría	Monitoreo persistente	Número de alarmas identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C09	P14	C09.P14	Implementación de seguridad perimetral	Herramienta de gestión de seguridad perimetral para filtrado de navegación, correo, prevención de intrusiones y protección frente a ataques perimetrales	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política para la Seguridad Perimetral Política de Auditoría	Actividades de auditoría cada 3 meses Monitoreo persistente	Número de eventos de seguridad identificados por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C09	P10	C09.P10	Implementación de herramientas de protección de aplicaciones y bases de datos	Implementación de herramientas de protección de aplicaciones y bases de datos, a través de parchado virtual, mitiguen riesgos de ataques internos o externos	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política para la Seguridad Perimetral Política de Auditoría	Actividades de auditoría cada 3 meses	Número de vulnerabilidades identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C10	P07	C10.P07	Gestionar respaldos de sistema operativo, software de aplicaciones y los datos, incluidos en el procedimiento de copia de seguridad general de endpoints y servidores	Herramienta de respaldo, pruebas de verificación de integridad, gestión de información antigua y planes de recuperación de datos	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de Respaldos y Gestión de los Archivos Política de Auditoría	Respaldo de información Actividades de auditoría cada 3 meses	Pruebas de efectividad de respaldos No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información

C11	P16	C11.P16	Gestión de seguridad en red interna	Diseño de red segura: Diseño de VLAN, DMZ de aplicaciones, servicios WEB externos y Bases de Datos, control de puertos y comunicaciones	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de la Seguridad de comunicaciones Política de Auditoría	Monitoreo persistente	Número de alarmas identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C11	P14	C11.P14	Implementación de seguridad perimetral	Herramienta de gestión de seguridad perimetral para filtrado de navegación, correo, prevención de intrusiones y protección frente a ataques perimetrales	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de Seguridad Perimetral Política de Auditoría	Actividades de auditoría cada 3 meses Monitoreo persistente	Número de eventos de seguridad identificados por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C11	P03	C11.P03	Implementación de Correlación de Eventos	Herramienta de Correlación de eventos: Monitoreo de accesos de usuarios	Manual de Operación Informe de configuración Información de capacitación	Política para la Respuesta a Incidentes de Seguridad de la Información	Monitoreo persistente	Número de accesos identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C11	P04	C11.P04	Operación de Respuesta a incidentes de seguridad	Personal operativo en monitoreo, investigación y gestión de alarmas e incidentes de seguridad de información	Proceso de gestión de alarmas o incidentes de seguridad Roles y responsabilidades en escenarios críticos	Política para la Respuesta a Incidentes de Seguridad de la Información	Monitoreo persistente	Número de alarmas identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C11	P17	C11.P17	Gestión de distribución de actualizaciones y parches de seguridad	Herramientas de distribución de actualizaciones y parches de seguridad para sistemas operativos, aplicaciones, bases de datos y	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios	Política para las Actualizaciones Política de Auditoría	Actividades de auditoría cada 3 meses Actividades de actualización una vez por año	Activos no actualizados identificado por período	Revisiones periódicas de cumplimiento en el comité de seguridad de información

				hardware de comunicaciones	Información de capacitación				
C12	P16	C12.P16	Gestión de seguridad en red interna	Diseño de red segura: Diseño de VLAN, DMZ de aplicaciones, servicios WEB externos y Bases de Datos, control de puertos y comunicaciones	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política para la Seguridad de las comunicaciones Política de Auditoría	Monitoreo persistente	Número de alarmas identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C12	P14	C12.P14	Implementación de seguridad perimetral	Herramienta de gestión de seguridad perimetral para filtrado de navegación, correo, prevención de intrusiones y protección frente a ataques perimetrales	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de Seguridad Perimetral Política de Auditoría	Actividades de auditoría cada 3 meses Monitoreo persistente	Número de eventos de seguridad identificados por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C12	P03	C12.P03	Implementación de Correlación de Eventos	Herramienta de Correlación de eventos: Monitoreo de accesos de usuarios	Manual de Operación Informe de configuración Información de capacitación	Política para la Respuesta a Incidentes de Seguridad de la Información	Monitoreo persistente	Número de accesos identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C12	P04	C12.P04	Operación de Respuesta a incidentes de seguridad	Personal operativo en monitoreo, investigación y gestión de alarmas e incidentes de seguridad de información	Proceso de gestión de alarmas o incidentes de seguridad Roles y responsabilidades en escenarios críticos	Política para la Respuesta a Incidentes de Seguridad de la Información	Monitoreo persistente	Número de alarmas identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información

C12	P08	C12.P08	Implementación de gestión centralizada de configuraciones y perfiles de usuario	Implementación de Active Directory, gestión de usuarios, perfiles y configuraciones centralizado	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de *Hardening* Política de gestión de usuarios Política de Auditoría	Actividades de auditoría cada 3 meses	Configuraciones de usuarios y perfiles gestionados por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C12	P01	C12.P01	Implementación de Herramienta de Inventario de Hardware y Software	Herramienta automatizada de inventario de hardware y software	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de Inventarios Política de Auditoría	Actividades de auditoría cada 3 meses Actividades de actualización una vez por año	Activos no autorizados identificados por período Porcentaje de efectividad de inventario	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C13	P18	C13.P18	Gestionar la política de clasificación de información y seguridad de información sensible	Política de clasificación de información	Proceso de clasificación Matriz de información clasificada Metodología de clasificación de información	Política para la Clasificación de información Política de Auditoría	Cumplimiento de proceso de clasificación Actividades de auditoría cada 3 meses	Información clasificada por proceso de negocio	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C13	P19	C13.P19	Cifrado de datos	Herramienta de cifrado de archivos, discos duros o dispositivos de almacenamiento	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de Cifrado de Datos Política de Auditoría	Actividades de auditoría cada 3 meses	Activos cifrados por proceso No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C13	P20	C13.P20	Prevención de fugas de información	Herramienta de control de medios de salida de información para prevención de fuga no autorizada de datos	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios	Política para la Clasificación de información Política de Auditoría	Monitoreo persistente	Alarmas de salida de información sensible no autorizada No conformidades	Revisiones periódicas de cumplimiento en el comité de seguridad de información

					Información de capacitación			de auditoría interna	
C13	P14	C13.P14	Implementación de seguridad perimetral	Herramienta de gestión de seguridad perimetral para filtrado de navegación, correo, prevención de intrusiones y protección frente a ataques perimetrales	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de Seguridad Perimetral Política de Auditoría	Actividades de auditoría cada 3 meses Monitoreo persistente	Número de eventos de seguridad identificados por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C13	P05	C13.P05	Implementación de seguridad de endpoint	Herramienta para protección de endpoint, control de dispositivos y aplicaciones	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de Seguridad Interna Política de Auditoría	Actividades de auditoría cada 3 meses	Número de vulnerabilidades identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C13	P03	C13.P03	Implementación de Correlación de Eventos	Herramienta de Correlación de eventos: Monitoreo de accesos de usuarios	Manual de Operación Informe de configuración Información de capacitación	Política de Respuesta a Incidentes de Seguridad de Información	Monitoreo persistente	Número de accesos identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C13	P04	C13.P04	Operación de Respuesta a incidentes de seguridad	Personal operativo en monitoreo, investigación y gestión de alarmas e incidentes de seguridad de información	Proceso de gestión de alarmas o incidentes de seguridad Roles y responsabilidades en escenarios críticos	Política de Respuesta a Incidentes de Seguridad de Información	Monitoreo persistente	Número de alarmas identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información

C14	P18	C14.P18	Gestionar la política de clasificación de información y seguridad de información sensible	Política de clasificación de información	Proceso de clasificación Matriz de información clasificada Metodología de clasificación de información	Política para la Clasificación de información Política de Auditoría	Cumplimiento de proceso de clasificación Actividades de auditoría cada 3 meses	Información clasificada por proceso de negocio	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C14	P16	C14.P16	Gestión de seguridad en red interna	Diseño de red segura: Diseño de VLAN, DMZ de aplicaciones, servicios WEB externos y Bases de Datos, control de puertos y comunicaciones	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de Seguridad de comunicaciones Política de Auditoría	Monitoreo persistente	Número de alarmas identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C14	P14	C14.P14	Implementación de seguridad perimetral	Herramienta de gestión de seguridad perimetral para filtrado de navegación, correo, prevención de intrusiones y protección frente a ataques perimetrales	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de Seguridad Perimetral Política de Auditoría	Actividades de auditoría cada 3 meses Monitoreo persistente	Número de eventos de seguridad identificados por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C14	P07	C14.P07	Gestionar respaldos de sistema operativo, software de aplicaciones y los datos, incluidos en el procedimiento de copia de seguridad general de endpoints y servidores	Herramienta de respaldo, pruebas de verificación de integridad, gestión de información antigua y planes de recuperación de datos	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de Respaldos y Gestión de Archivos Política de Auditoría	Respaldo de información Actividades de auditoría cada 3 meses	Pruebas de efectividad de respaldos No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C14	P08	C14.P08	Implementación de gestión centralizada de configuraciones y perfiles de usuario	Implementación de Active Directory, gestión de usuarios, perfiles y configuraciones centralizado	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios	Política de Hardening Política de gestión de usuarios Política de Auditoría	Actividades de auditoría cada 3 meses	Configuraciones no seguras identificadas por período No conformidades	Revisiones periódicas de cumplimiento en el comité de seguridad de información

					Información de capacitación			de auditoría interna	
C14	P21	C14.P21	Implementación de control y protección de acceso a servidores de archivos o repositorios compartidos de información sensible	Implementación de Firewall de servidores de Archivos para control y protección de acceso a información compartida	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de Respaldos y Gestión de Archivos Política de Auditoría	Actividades de auditoría cada 3 meses	Alarmas de seguridad identificadas No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C16	P08	C16.P08	Implementación de gestión centralizada de configuraciones y perfiles de usuario	Implementación de Active Directory, gestión de usuarios, perfiles y configuraciones centralizado	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de Hardening Política de gestión de usuarios Política de Auditoría	Actividades de auditoría cada 3 meses	Configuraciones no seguras identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C16	P03	C16.P03	Implementación de Correlación de Eventos	Herramienta de Correlación de eventos: Monitoreo de accesos de usuarios	Manual de Operación Informe de configuración Información de capacitación	Política para la Respuesta a Incidentes de Seguridad de la Información	Monitoreo persistente	Número de accesos identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C16	P04	C16.P04	Operación de Respuesta a incidentes de seguridad	Personal operativo en monitoreo, investigación y gestión de alarmas e incidentes de seguridad de información	Proceso de gestión de alarmas o incidentes de seguridad Roles y responsabilidades en escenarios críticos	Política para la Respuesta a Incidentes de Seguridad de la Información	Monitoreo persistente	Número de alarmas identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información

C16	P21	C16.P21	Implementación de control y protección de acceso a servidores de archivos o repositorios compartidos de información sensible	Implementación de firewall de servidores de archivos para control y protección de acceso a información compartida	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de Respaldos y Gestión de Archivos Política de Auditoría	Actividades de auditoría cada 3 meses	Alarmas de seguridad identificadas No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C16	P12	C16.P12	Implementar doble factor de autenticación para acceso a sistemas críticos	Implementar una herramienta de doble factor de autenticación que permita mitigar el riesgo de acceso a sistemas críticos de personal no autorizado	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de gestión de usuarios Política de contraseñas Política de Auditoría	Actividades de auditoría cada 3 meses	No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C17	P23	C17.P23	Plan de formación y concientización	Implementar un plan de formación periódico de conceptos y prácticas de seguridad de información	Manual de Operación Información de capacitación	Política para las capacitaciones en Seguridad de Información	Evaluación periódica en seguridad de información	Porcentaje de aprobación en evaluaciones	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C17	P24	C17.P24	Plan de formación en seguridad informática	Implementar un plan de formación y especialización de los administradores de seguridad informática en TI	Manual de Operación Información de capacitación	Política para las capacitaciones en Seguridad de Información	Evaluación periódica en seguridad de información	Porcentaje de aprobación en evaluaciones	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C18	P01	C18.P01	Implementación de Herramienta de Inventario de Hardware y Software	Herramienta automatizada de inventario de hardware y software	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política para Inventarios Política de Auditoría	Actividades de auditoría cada 3 meses Actividades de actualización una vez por año	Activos no autorizados identificados por período Porcentaje de efectividad de inventario	Revisiones periódicas de cumplimiento en el comité de seguridad de información

C18	P17	C18.P17	Gestión de distribución de actualizaciones y parches de seguridad	Herramientas de distribución de actualizaciones y parches de seguridad para sistemas operativos, aplicaciones, bases de datos y hardware de comunicaciones	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política para las Actualizaciones Política para Auditoría	Actividades de auditoría cada 3 meses Actividades de actualización una vez por año	Activos no actualizados identificado por período	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C18	P25	C18.P25	Protección de Aplicaciones	Herramienta de Firewall de Aplicaciones para mitigar el riesgo frente a ataques en la capa de aplicación como SQL *Inyection*	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política para la seguridad de las aplicaciones Política de auditoría	Número de alarmas identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C18	P26	C18.P26	Evaluación de vulnerabilidades en código fuente	Herramienta de evaluación de código fuente para identificar vulnerabilidades en la etapa de desarrollo de aplicaciones	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política para la seguridad de las aplicaciones Política de auditoría	Número de alarmas identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C18	P27	C18.P27	Arquitectura de desarrollo seguro	Herramienta de código para aplicar seguridades integradas en el desarrollo de aplicaciones.	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política para la seguridad de las aplicaciones Política de auditoría	Número de alarmas identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C18	P09	C18.P09	Implementar un proceso de evaluación y remediación de vulnerabilidades periódico	Implementación de herramientas de escaneo de vulnerabilidades que permita la identificación tanto a nivel de IP como a nivel de aplicación	Manual de Operación Informe de configuración Repositorio de Gestión de	Política de Gestión de Vulnerabilidades Política de Auditoría	Tareas de escaneo de vulnerabilidades periódicas Actividades de	Número de vulnerabilidades identificadas por período No conformidades	Revisiones periódicas de cumplimiento en el comité de seguridad de información

					Cambios Información de capacitación		auditoría cada 3 meses	de auditoría interna	
C18	P16	C18.P16	Gestión de seguridad en red interna	Diseño de red segura: Diseño de VLAN, DMZ de aplicaciones, servicios WEB externos y Bases de Datos, control de puertos y comunicaciones	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de Seguridad de comunicaciones Política de Auditoría	Monitoreo persistente	Número de alarmas identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C18	P08	C18.P08	Implementación de gestión centralizada de configuraciones y perfiles de usuario	Implementación de Active Directory, gestión de usuarios, perfiles y configuraciones centralizado	Manual de Operación Informe de configuración Repositorio de Gestión de Cambios Información de capacitación	Política de hardening Política de gestión de usuarios Política de Auditoría	Actividades de auditoría cada 3 meses	Configuraciones no seguras identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información
C19	P04	C19.P04	Operación de Respuesta a incidentes de seguridad	Personal operativo en monitoreo, investigación y gestión de alarmas e incidentes de seguridad de información	Proceso de gestión de alarmas o incidentes de seguridad Roles y responsabilidades en escenarios críticos	Política para la Respuesta a Incidentes de Seguridad de la Información	Monitoreo persistente	Número de alarmas identificadas por período No conformidades de auditoría interna	Revisiones periódicas de cumplimiento en el comité de seguridad de información