CENTRO DE POSGRADOS

Tema:

PROPUESTA DE IMPLEMENTACIÓN BASADA EN CONTROLES CIS PARA UNA INFRAESTRUCTURA DE RED: CASO DE ESTUDIO

Proyecto de investigación previo a la obtención del título de Magister en Ciberseguridad

Línea de investigación:

PROTECCIÓN DE DATOS Y COMUNICACIONES

Autor:

Juan Carlos Pardo Sarango

Director:

Mg. Darío Javier Robayo Jácome

Ambato – Ecuador

Mayo 2025

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo: **JUAN CARLOS PARDO SARANGO**, con cédula de ciudadanía **0704014570**, autor del trabajo de graduación intitulado: "PROPUESTA DE IMPLEMENTACIÓN BASADA EN CONTROLES CIS PARA UNA INFRAESTRUCTURA DE RED: CASO DE ESTUDIO", previo a la obtención del título profesional de **MAGISTER EN CIBERSEGURIDAD,** en el centro de **POSGRADOS**.

1. Declaro tener pleno conocimiento de la obligación que tiene la Pontificia Universidad Católica del Ecuador, de conformidad con el artículo 144 de la Ley Orgánica de Educación Superior, de entregar a la SENESCYT en formato digital una copia del referido trabajo de graduación para que sea integrado al Sistema Nacional de Información de la Educación Superior del Ecuador para su difusión pública respetando los derechos de autor.

2. Autorizo a la Pontificia Universidad Católica del Ecuador a difundir a través del sitio web de la Biblioteca de la PUCE Ambato, el referido trabajo de graduación, respetando las políticas de propiedad intelectual de la Universidad.

Ambato, mayo 2025

Firmado electrónicamente por:
JUAN CARLOS PARDO SARANGO
Validar únicamente con FirmaEC

Juan Carlos Pardo Sarango
CC. 0704014570

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

APROBACIÓN DEL TRIBUNAL DE GRADO

Tema:

PROPUESTA DE IMPLEMENTACIÓN BASADA EN CONTROLES CIS PARA UNA INFRAESTRUCTURA DE RED: CASO DE ESTUDIO

Línea de investigación:

PROTECCIÓN DE DATOS Y COMUNICACIONES

Autor:

Juan Carlos Pardo Sarango

Darío Javier Robayo Jácome, Ing. Mg. f._____
Firmado electrónicamente por: DARIO JAVIER ROBAYO JACOME Validar únicamente con FirmaEC

CC.1802842268

CALIFICADOR

José Marcelo Balseca Manzano, Ing. Mg. f._____
Firmado electrónicamente por: JOSE MARCELO BALSECA MANZANO Validar únicamente con FirmaEC

CALIFICADOR

Liliana del Rocío Mena Hernández, Ing. Mg. f._____
Firmado electrónicamente por: LILIANA DEL ROCIO MENA HERNANDEZ Validar únicamente con FirmaEC

CALIFICADOR

Dayamy Lima Rojas, Lic. Mg. f._____
DAYAMY LIMA ROJAS Firmado digitalmente por DAYAMY LIMA ROJAS Fecha: 2025.05.29 11:19:15 -05'00'

DIRECTORA CENTRO DE POSGRADOS

Diego Gonzalo Coca Chanalata, Dr. f._____
DIEGO GONZALO COCA CHANALATA Firmado digitalmente por DIEGO GONZALO COCA CHANALATA Fecha: 2025.05.29 14:11:00 -05'00'

SECRETARIO GENERAL PUCESA

Ambato – Ecuador

Mayo 2025

RESUMEN

El presente estudio busca establecer un marco referencial para realizar una implementación de controles de seguridad en el Grupo Chevez dentro de la red de Minervilla; los Controles de CIS son un conjunto de mejoras prácticas en Seguridad Cibernética; además, de acciones defensivas que previenen ataques peligrosos y de mayor alcance; siendo recomendadas y reconocidas a nivel mundial para colaborar a los profesionales de la seguridad a administrar medidas de seguridad.

El marco de referencia inicia construyéndose a partir del análisis de los antecedentes de la seguridad en informática de la empresa en su sistema de seguridad menguando las vulnerabilidades en la red LAN, a través del análisis se determina que no se puede garantizar que las medidas de seguridad tomadas en la red protejan la misma de ataques externos. Siendo necesario implementar controles dictados por algún estándar, por lo que se tomó de referencia los Controles CIS buscando proveer a la organización pautas claras al momento de implementar algún control gestionando su ciberseguridad con formalidad.

Para la investigación se realiza una simulación en el cual se instala el Firewall Sophos configurándolo, posterior a ello se instala y configura Windows Server 2012 R2; además se generan 3 tipos de ataques para que sean verificados por el firewall Sophos, que fueron reportados. Se recomienda realizar un análisis de vulnerabilidad cada cierto tiempo en los equipos de la red LAN remediando las brechas de seguridad antes de que sean generadas por terceros y ocasionen pérdida de información o fallos en los sistemas.

Palabras clave: ciberseguridad, firewall sophos, controles cis, vulnerabilidades.

ABSTRACT

The present study seeks to establish a referential framework to implement security controls in the Chevez Group within the Minervilla network; CIS Controls are a set of practical improvements in Cyber Security; in addition to defensive actions that prevent dangerous and far-reaching attacks; being recommended and recognized worldwide to help security professionals to manage security measures.

The frame of reference starts building from the analysis of the background of the company's IT security in its security system, reducing the vulnerabilities in the LAN network, through the analysis it is determined that it cannot be guaranteed that the security measures taken in the network protect it from external attacks. It is necessary to implement controls dictated by some standard, so the CIS Controls were taken as a reference, seeking to provide the organization with clear guidelines at the time of implementing any control to manage its cybersecurity with formality.

For the research a simulation is performed in which the Sophos Firewall is installed and configured, then Windows Server 2012 R2 is installed and configured; in addition 3 types of attacks are generated to be verified by the Sophos firewall, which were reported. It is recommended to perform a vulnerability analysis from time to time in the LAN network equipment, remediating security breaches before they are generated by third parties and cause loss of information or system failures.

Keywords: *cybersecurity, sophos firewall, cis controls, vulnerabilities.*

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

En el mundo digital cada vez más complejo y amenazante la ciberseguridad se ha convertido en un factor crucial como protección en el desarrollo de las actividades económicas, impulsando la necesidad de asegurar la integridad, confidencialidad y continuidad de las operaciones empresariales; la protección de las infraestructuras de red sería el factor primordial para la implementación de medidas efectivas de seguridad, en éste contexto la presente propuesta se centra en la aplicación de Controles basados en el marco CIS (*Center for Internet Security*, 2021).

En septiembre del 2021 (Honores, 2021) desarrolla un proyecto que aborda el "Diseño e Implementación de un Sistema de Seguridad mediante Controles CIS para Redes de Acceso LAN", utilizando el Instituto Nacional de Evaluación Educativa (INEVAL) como caso de estudio. La investigación se centró en la mitigación de vulnerabilidades en la red LAN mediante los controles CIS. Se seleccionaron controles específicos para abordar 23 vulnerabilidades, se comprobó que al implementar el Sistema de Seguridad basado en controles CIS hubo una reducción de vulnerabilidades del 42%. El planteamiento del problema destaca la necesidad de mejorar la seguridad ante incidentes cibernéticos, proponiendo la aplicación periódica de controles CIS.

En marzo de 2022, se realiza una investigación del marco de referencia para la implementación de controles de seguridad informática en una organización ecuatoriana de fabricación, comercialización y exportación de muebles, al analizar las normativas vigentes tales como ISO 27001, NIST y CIS; se evidencia que el estándar CIS es el más indicado para implementación de controles de seguridad en empresas que se encuentran en una etapa inicial de la gestión de su ciberseguridad.

La evaluación de las medidas de ciberseguridad en la empresa revela una falta de unidad y organización en su enfoque de seguridad. La carencia de un plan estructurado lleva a que las medidas operaran de manera aislada, sin una integración efectiva entre ellas. Como respuesta a esta situación, por lo que se

concluye que es esencial desarrollar un marco de referencia que proporcionara directrices claras y simples con el objetivo de facilitar la implementación de controles de ciberseguridad en la empresa.

En abril del 2020, la Oficina de Auditorías Estatal de Washington (SAO) utiliza los controles CIS para realizar auditorías que ayudan a mejorar la postura de seguridad tanto de las agencias estatales como de los gobiernos locales. La SAO de Washington citó que las agencias pueden mejorar su postura general de ciberseguridad adoptando los Controles CIS, con el objetivo de proteger la información confidencial dentro de las redes y sistemas del estado de Washington; utilizando los controles CIS como criterio de auditoría que permita hacer ambas cosas.

La aplicación de los controles CIS ha aumentado el valor de las auditorías y remedia los problemas identificados en esas auditorías, mejorando la seguridad de TI tanto a nivel estatal como local, los controles han bridando el soporte para realizar ambas actividades. Los controles CIS proporcionaron un camino claro para que la organización alcance sus metas y objetivos descritos por los marcos jurídicos, reglamentarios y normativos.

En febrero del 2020, el distrito escolar de *Hillsboro-Deering* mejora la higiene cibernética con los controles CIS. Los distritos escolares enfrentan el desafío único de proteger la privacidad de los datos de sus estudiantes contra amenazas cibernéticas como *ransomware* y *phishing*. En *New Hampshire*, existen múltiples regulaciones que protegen la ciberseguridad de los estudiantes, pero puede resultar complicado para los administradores técnicos elaborar un plan de cumplimiento.

El Distrito Escolar de *Hillsboro-Deering* encontró la manera de cumplir con las regulaciones y mejorar su programa de defensa cibernética aprovechando los Grupos de Implementación de Controles (IG1 e IG2) de CIS, ejemplos de esas medidas de seguridad incluyen el mantenimiento de inventarios de activos, el control de los privilegios administrativos y la aplicación de la protección de datos, llegando a la madurez y aumento de la higiene cibernética en la organización.

La evolución acelerada de entornos digitales, la dependencia de la tecnología y la conectividad global ha provocado un aumento de amenazas cibernéticas a nivel mundial, organizaciones de diversas índoles se han visto afectadas por diversas vulnerabilidades. Hoy en día existen diferentes marcos de referencia para la seguridad de la información, como él (CC) *Common Criteria, (NIST) National Institute of Standards and Technology, (CSF) Cybersecurity Framework y el Center for Internet Security (CIS) Controls*, estos marcos se encuentran disponibles para proporcionar a las organizaciones una serie de directrices y controles fortaleciendo entre otros aspectos la seguridad de la infraestructura de red.

Según la Solarte et al. (2015), la seguridad de la ISO/IEC 27001 con información se define como aquellos procesos, buenas prácticas y metodologías que buscan proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizada. Es un componente esencial de la gestión de riesgos y es fundamental para proteger los activos de la organización, su importancia radica en varias razones como ayudar a proteger la privacidad de los datos personales, ayudar a proteger la propiedad intelectual y ayudar a proteger la continuidad del negocio.

Según *SolarWinds* (2023), la infraestructura de red es el conjunto más amplio de componentes fundamentales que funcionan de manera coherente para ejecutar una red de TI, es una parte fundamental de la infraestructura de TI de una organización. Por lo que es fundamental garantizar que la infraestructura de red subyacente sea confiable, segura, sólida y escalable. La infraestructura de red es el conjunto de componentes físicos y lógicos que permiten la comunicación entre los dispositivos de una red; es un punto vulnerable que debe protegerse de las amenazas cibernéticas, errores humanos y problemas técnicos; es esencial para el funcionamiento de las organizaciones modernas debido a que permite la comunicación, el acceso a recursos compartidos y el acceso a internet.

Los componentes físicos de la infraestructura de red son los elementos tangibles que permiten la conectividad como cables, *routers*, *switches*, *firewalls*, servidores, computadoras, impresoras, en tanto que los componentes lógicos son los

elementos que rigen la comunicación entre los dispositivos como los protocolos, software, políticas y procedimientos, entre otros. Un diseño de topología de red adecuado puede ayudar a garantizar que la red sea eficiente, segura y escalable.

Para *Center for Internet Security* (2021), los controles de Seguridad Crítica de CIS son un conjunto prescriptivo y prioritario de mejores prácticas en la seguridad cibernética y acciones defensivas que pueden ayudar a prevenir los ataques más peligrosos y de mayor alcance. Estos controles se centran en la protección de las infraestructuras de red, y proporcionan a las organizaciones un marco para implementar medidas de seguridad efectivas.

La protección de datos y comunicaciones es de vital importancia para Minervilla CIA Ltda. que utiliza medios inalámbricos, cableados y radiales. Las redes de área amplia (WAN) o redes de área local (LAN) son un elemento fundamental en la interconexión de diferentes sucursales, debido a la falta de atención a las diversas vulnerabilidades de los productos tanto hardware como software, desatención en políticas de seguridad, falta de conciencia de seguridad. Se han experimentado problemas de accesos no autorizados, infección y propagación de malware, uso indebido de los recursos tecnológicos, tráfico no autorizado y lentitud en toda la red, todo esto conlleva a la inactividad de los procesos operativos de la compañía, la no disponibilidad e inseguridad en el trato de la información (Figueroa-Suárez et al., 2018).

Muchas empresas al no contar con mecanismos de protección en sus redes se exponen a constantes amenazas cibernéticas como ransomware que según una reconocida empresa británica especializada en seguridad informática en su informe anual sobre el estado del ransomware sophos (2023), revela que ha crecido un 66% para el año 2023, la causa raíz más común de los ataques de ransomware fue la explotación de una vulnerabilidad (36 %), seguida del compromiso de credenciales (29%), los correos electrónicos fueron la causa raíz del 30% de los ataques: El 18% empezó con un correo malicioso y el 13% con phishing, el 3% comenzó con un ataque por fuerza bruta y solo un 1% con una descarga.

Según CISCO (2023), existen otros tipos de ataques cibernéticos que pueden dirigirse hacia las empresas con el objetivo de comprometer la seguridad, robar datos valiosos o causar daño operativo, algunos de los tipos más comunes incluyen: ataques de ingeniería social, malware, ataques de denegación de Servicio (DDoS), ataques a la Cadena de Suministro, ataques de *Man-in-the-Middle* (MitM), ataques de Exfiltración de Datos.

Las vulnerabilidades son debilidades en un sistema que pueden ser explotadas por los atacantes para obtener acceso no autorizado o causar daños, las vulnerabilidades pueden existir en los componentes físicos de la infraestructura de red o en los componentes lógicos siendo variados y que pueden clasificarse según su naturaleza, las más comunes son las vulnerabilidades de configuración, de software y de hardware. De acuerdo a esto se plantea el siguiente problema a investigar: las vulnerabilidades que se exponen en la infraestructura de la red de Grupo Chevez no permiten garantizar la seguridad de la información.

De acuerdo al problema planteado se propone la siguiente idea a defender: la implementación de una propuesta basada en el uso de controles CIS la cual mejora la seguridad de la infraestructura del Grupo Chevez específicamente en la red de Minervilla CIA Ltda., los controles CIS son un conjunto de recomendaciones de seguridad que están diseñadas para abordar una amplia gama de amenazas y vulnerabilidades, estos controles están organizados en 20 categorías que abarcan desde la gestión de activos hasta la respuesta a incidentes.

La implementación de controles CIS puede ayudar a las organizaciones a mejorar la seguridad de su infraestructura de red de varias maneras, incluyendo la reducción del riesgo de ataques cibernéticos, mejora de la visibilidad y el control de la infraestructura de red y cumplimiento de requisitos normativos, por lo tanto, la implementación de controles CIS es una medida eficaz para mejorar la seguridad de la infraestructura de red. Por ende, el objetivo principal de este proyecto de desarrollo es presentar una propuesta de implementación basada en el uso de controles en el marco CIS para el aseguramiento de la infraestructura de la red del Grupo Chevez.

Los objetivos específicos se desglosan en etapas clave de la investigación, desde el análisis teórico hasta el desarrollo práctico de la propuesta, teniendo:

1. Documentar bibliográficamente los métodos vigentes de seguridad para las infraestructuras de red.
2. Diagnosticar el estado actual de la seguridad de la infraestructura en la red corporativa del Grupo Chevez.
3. Compilar un conjunto de técnicas basado en el uso de controles CIS para el aseguramiento en infraestructuras de redes.
4. Desarrollar la propuesta de implementación para la seguridad de la infraestructura de la red del Grupo Chevez.

La metodología propuesta se basa en una investigación bibliográfica para la seguridad de redes, acompañado con una investigación de tipo exploratoria para realizar el diagnóstico de la organización; según Hernández-Sampieri & Mendoza (2018), la investigación bibliográfica o documental es detectar, obtener y consultar la biografía y otros materiales que parten de otros conocimientos y/o informaciones recogidas moderadamente de cualquier realidad, de manera selectiva, de modo que puedan ser útiles para los propósitos del estudio.

En una investigación de tipo exploratoria de acuerdo con Rodríguez et al. (2017), los estudios exploratorios se efectúan normalmente cuando, el objetivo es examinar un tema o problema de investigación poco estudiado o que no ha sido abordado antes. La implementación de metodologías de seguridad se centra en la aplicación de controles basados en el marco CIS (*Center for Internet Security*) a un entorno de red como prueba piloto permitiendo identificar vulnerabilidades, evaluar riesgos potenciales y proponer soluciones adecuadas.

La importancia de este proyecto radica en la necesidad crítica de salvaguardar la infraestructura de red del Grupo Chevez específicamente en la sucursal de Minervilla CIA Ltda., por medio de un marco sólido ante las crecientes amenazas cibernéticas. La implementación de controles CIS no solo fortalecerá la seguridad,

sino que también promoverá la confianza, la integridad y la eficiencia operativa en un entorno digital en constante evolución.

CAPÍTULO I. ESTADO DE ARTE Y LA PRÁCTICA

1.1. Seguridad de la información

A lo largo de la historia, los seres humanos han buscado proteger lo que consideraban valioso, siendo la seguridad un concepto antiguo arraigado en la protección de bienes. En la sociedad actual, la información se ha convertido en uno de los activos más preciados, especialmente para los negocios, dado el aumento de la interconexión global y la sofisticación de los ataques cibernéticos a infraestructuras y sistemas informáticos. Proteger esta información se ha vuelto fundamental para muchas organizaciones que destinan considerables recursos para salvaguardar sus datos, reconociendo así su importancia como activo principal.

La información, como un elemento más al interior de una organización, es considerada un activo valioso, de ahí se toman decisiones importantes para el desarrollo de los objetivos corporativos y, a su vez, se le brindan al usuario elementos de juicio para su permanencia como cliente; de ahí, la necesidad de ser protegida (Juan José Ripoll Samper, 2015). Para entender qué es la seguridad de la información, es necesario comprender qué es la seguridad. En general, la seguridad es el estado de estar protegido y libre de peligro. En términos más simples, es la protección contra cualquier adversario u oponente que pueda causar daño, con o sin intención (Mahn et al., 2022).

Una expresión más amplia es que la seguridad de la información protege los activos de información y todo lo relacionado con ellos. La seguridad incluye la seguridad personal, entre otras cosas, pero la seguridad de la información se centra en los activos de información. En ocasiones, se percibe la seguridad de la información como seguridad informática, sin embargo, va más allá. La seguridad de la información abarca la seguridad informática, entre otros aspectos. (Whitman, 2012)

En este sentido, Vega (2021) define a la seguridad de la información como una disciplina "que se encarga de la implementación técnica de la protección de la

información, el despliegue de las tecnologías que establecen de forma que se aseguran las situaciones de fallas parciales o totales, cuando la información es el activo que se encuentra en riesgo, la disciplina que trata de los riesgos, de las amenazas, de los análisis de escenarios, de las buenas prácticas y los esquemas normativos, que nos exigen niveles de aseguramiento de procesos y de tecnología para elevar el nivel de confianza en la creación, utilización, almacenaje, transmisión, recuperación y disposición final de la información".

La inclusión de la seguridad personal en el contexto de la seguridad general podría ocasionar confusión, porque no se establece claramente cómo estos dos conceptos se relacionan o difieren. La distinción entre seguridad de la información y seguridad informática es abordada, pero la explicación es breve y podría beneficiarse de ejemplos específicos que ilustren las diferencias. En cuanto a la definición de ISOTools, si bien se enfoca en la implementación técnica, podría considerarse que subestima otros aspectos esenciales de la seguridad de la información (*National Institute of Standards and Technology*, 2018).

Según la (Solarte et al., 2015), la seguridad de la información se podría definir como aquellos procesos, buenas prácticas y metodologías que busquen proteger la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación o destrucción no autorizada. Esta definición básicamente significa que debemos proteger nuestros datos y nuestros recursos de infraestructura tecnológica de aquellos quiénes intentarían hacer un mal uso de ellos (Guijarro, 2023).

1.2. Seguridad informática

Desde el sitio web de *Hewlett Packard Enterprise* (2023), define que la seguridad de la tecnología de la información constituye un amplio conjunto de medidas multidisciplinares de protección para evitar que una red informática y sus datos sufran algún tipo de vulneración, filtración, publicación de información privada o ataque

De acuerdo con Montesino et al. (2013), define la seguridad informática como cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados al sistema.

La seguridad informática (también conocida como seguridad digital) se refiere a las diversas técnicas, aplicaciones y dispositivos encargados de asegurar la confidencialidad, integridad, privacidad y disponibilidad de la información de un sistema informático y por consiguiente de sus usuarios.

Se resume que la seguridad de la información es el conjunto de medidas de prevención y reactivas que aplican las organizaciones para evitar que la información, en cualquier formato que produce incida en las manos equivocadas; mientras que la seguridad informática forma parte de la información y se define como la parte concreta del plan general de seguridad que se encarga de la protección del contenido de los equipos informáticos (Figueroa-Suárez et al., 2018).

La seguridad de la información y la seguridad informática son utilizados con bastante frecuencia, suelen considerarse como sinónimos cuando en realidad son conceptos distintos, aunque se encuentran relacionados; de igual modo ambos conceptos persiguen la misma finalidad que es proteger la confidencialidad, la integridad y la disponibilidad de la información sensible de la organización abarcando hardware y software.

Comprender la seguridad de la información va más allá de simplemente conocer su definición. Es esencial reconocer que saber qué es la seguridad de la información no es suficiente para captar la dimensión completa de este concepto dinámico y crucial en el entorno actual. Para profundizar en su significado y aplicación efectiva, resulta fundamental familiarizarse con los pilares fundamentales que sustentan este campo.

1.3. Pilares de la seguridad de la información e infraestructura de red

Según la norma ISO/IEC 27001 (ISO/IEC, 2022) la seguridad de la información se puede dividir en tres pilares fundamentales. Estos pilares representan un conjunto de principios que respaldan la seguridad de la información y ayudan a definir las mejores prácticas para que las organizaciones logren sus objetivos de seguridad, ver Figura 1.

Confidencialidad

La confidencialidad es uno de los pilares fundamentales de la seguridad de la información según la norma ISO/IEC 27001 (ISO/IEC, 2022), este pilar tiene como objetivo garantizar que la información sea accesible solo para personas autorizadas, protegiéndola contra la divulgación no autorizada y el uso indebido.

La información tiene confidencialidad cuando está protegida de la divulgación o exposición a personas o sistemas no autorizados, la confidencialidad garantiza que sólo aquellos con los derechos y privilegios para acceder a la información pueden hacerlo; cuando no está autorizado individuos o sistemas pudiendo ver la información, se viola la confidencialidad (Mahn et al., 2022).

Para garantizar la confidencialidad de la información la ISO/IEC 27001 (ISO/IEC, 2022), establece requisitos como el control de acceso, cifrado, implementación de políticas de seguridad de datos y la verificación periódica de los sistemas de seguridad. Además, es importante que las empresas cuenten con un plan de contingencia para enfrentar incidentes de seguridad que puedan comprometer la confidencialidad de la información.

Integridad

La información tiene integridad cuando es completa y no está corrupta. La integridad de la información se ve amenazada cuando la información se expone a corrupción, daño, destrucción u otra alteración de su estado auténtico. La

corrupción puede ocurrir mientras se almacena o transmite información (Solarte et al., 2015).

Según (Urbina, 2018) la integridad significa que la información que se recibe sea precisa y esté completa (su contenido es el necesario) para los fines que se persiguen con su procesamiento, así como con su validez, de acuerdo con los valores y las expectativas del negocio.

Para garantizar la integridad de la información ISO/IEC 27001 requiere que las empresas adopten medidas de control para prevenir, detectar y corregir errores y modificaciones no autorizadas, a lo largo de todo su ciclo de vida, desde la creación hasta la eliminación segura.

Disponibilidad

La disponibilidad permite a los usuarios autorizados (personas o sistemas informáticos) acceder a la información sin interferencias ni obstrucciones y recibirla en el formato requerido. Como menciona (Briceño, 2021) la disponibilidad se refiere a la capacidad de acceder a nuestros datos cuando los necesitamos. La pérdida de disponibilidad puede referirse a una amplia variedad de interrupciones en cualquier parte de la cadena de comunicaciones que nos permite acceder a nuestros datos. Tales problemas pueden ser el resultado de pérdida de energía, problemas del sistema operativo o de la aplicación, ataques a la red de datos, compromiso de un sistema u otros problemas que impidan a los usuarios acceder a su información.

Para garantizar la disponibilidad de la información Solarte et al. (2015) recomienda a las empresas implementar medidas de seguridad para evitar interrupciones o indisponibilidades. Esto incluye la implementación de medidas de redundancia para recursos críticos, tales como: circuitos de internet, dispositivos de red, estructuras de respaldo y recuperación de datos, así como procedimientos y políticas que pueden activarse en caso de fallas o incidentes de seguridad.

Figura 1. Pilares de la seguridad de la Información

Fuente: Tomado de (Romero et al., 2018)

En el ámbito de la seguridad de la información, es crucial reconocer la necesidad de administración activa. Gestionar la seguridad de la información de manera efectiva implica la creación y mantenimiento de programas, controles y políticas con el propósito específico de preservar la confidencialidad, integridad y disponibilidad de la información.

Ciberseguridad

La Ciberseguridad se refiere generalmente a la capacidad de controlar el acceso a las redes, sistemas de información y todo tipo de recursos de información (SCHOOL, 2024) en general se podría decir que la ciberseguridad se refiere a métodos de uso, procesos y tecnologías para prevenir, detectar y recuperarse de daños a la confidencialidad, integridad y disponibilidad de la información en el ciberespacio (Leiva, 2015).

Según Newmeyer (2015) la ciberseguridad es el conjunto de políticas de entrenamiento y tecnología diseñadas para proteger el entorno cibernético con el objetivo de asegurar la confidencialidad, integridad y disponibilidad de la información y la habilidad de conectar dispositivos para que operen según su diseño.

Un concepto más apegado a la realidad es la que brinda Leiva (2015), la ciberseguridad es la práctica de defender las computadoras, los servidores, los

dispositivos móviles, los sistemas electrónicos, las redes y los datos de ataques maliciosos. También se conoce como seguridad de tecnología de la información o seguridad de la información electrónica. El término se aplica en diferentes contextos, desde los negocios hasta la informática móvil, y puede dividirse en algunas categorías comunes.

La Ciberseguridad está incluida en el ámbito de la Seguridad de la Información. Mientras que la Ciberseguridad implica llevar a cabo acciones defensivas, de alguna manera ofensivas, para resguardar la información y los sistemas, la Seguridad de la Información busca ser una orientación preventiva frente a los riesgos y amenazas que rodean a la información.

Riesgo informático

Se define como riesgo a la combinación de la probabilidad (oportunidad de que la amenaza se materialice) de que ocurra un evento y sus consecuencias para la organización. Algo que puede ocurrir y sus efectos sobre los objetivos de la organización. Los riesgos informáticos se mencionan a la inseguridad existente por la posible realización de un suceso concerniente con la amenaza de daño relacionado a los bienes o servicios informáticos como periféricos, instalaciones, proyectos, programas de cómputo, archivos, información, datos confidenciales, entre otros (Liberatori, 2018).

El riesgo se define como la posibilidad de que ocurra un incidente de seguridad, donde una amenaza se materializa, causando pérdidas o daños. Se mide asumiendo que existe una cierta vulnerabilidad frente a una determinada amenaza, como ataques de hackers, denegación de servicios o virus; el riesgo depende entonces de los siguientes factores: la probabilidad de que la amenaza se materialice aprovechando una vulnerabilidad y produciendo un daño o impacto. El producto de estos factores representa el riesgo, como se observa en la Figura 2.

Amenazas

Una amenaza es toda acción que aprovecha una vulnerabilidad para atentar contra la seguridad de un sistema de información. Es decir, que podría tener un potencial efecto negativo sobre algún elemento de nuestros sistemas. Las amenazas pueden proceder de ataques (fraude, robo, virus), sucesos físicos (incendios, inundaciones) o negligencia y decisiones institucionales (mal manejo de contraseñas, no usar cifrado). Desde el punto de vista de una organización pueden ser tanto internas como externas ((INCIBE), 2017).

Se entiende por amenaza una condición del entorno de los sistemas, áreas o dispositivos que contienen información importante (persona, equipo, suceso o idea) que ante determinada circunstancia podría dar lugar a que se produjese una violación de seguridad (no cumplimiento de alguno de los aspectos mencionados), afectando parte de la información y de la TI de la organización (Baca, 2017).

Vulnerabilidad

Las vulnerabilidades son fallas que permiten la aparición de deficiencias en la seguridad general del equipo o de la red. Configuraciones incorrectas en el equipo o en la seguridad también permiten la creación de vulnerabilidades; a partir de esta falla, las vulnerabilidades son explotadas por amenazas que cuando se materializan causan daños al computador, a la organización o a los datos personales.

En términos de informática es una debilidad o fallo en un sistema de información que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la integridad, disponibilidad o confidencialidad de esta, por lo que es necesario encontrarlas y eliminarlas lo antes posible. Estos «agujeros» pueden tener distintos orígenes, por ejemplo: fallos de diseño, errores de configuración o carencias de procedimientos (Incibe, 2023).

Constituye un hecho o una actividad que permite concretar una amenaza, se es vulnerable en la medida en que no hay suficiente protección como para evitar que

llegue a suceder una amenaza. En la actualidad se contempla que hay ataques intencionados y no intencionados, mismos a los que la empresa siempre es vulnerable en mayor o menor medida.

Figura 2. Riesgo

Fuente: Tomado de (Incibe, 2023)

Infraestructura de red

Se refiere a todos los recursos de una red que hacen posible la conectividad, la gestión, las operaciones comerciales y la comunicación de la red o de Internet. Consiste en hardware y software, sistemas y dispositivos, y permite la informática y la comunicación entre usuarios, servicios, aplicaciones y procesos. La infraestructura de red puede ser en la nube, física o virtual (*Center for Internet Security*, 2021).

De igual forma, (*SolarWinds*, 2023), define a la infraestructura de red como un conjunto más amplio de componentes fundamentales que funcionan de manera coherente para ejecutar una red de TI y es una parte fundamental de la infraestructura de TI de una organización. Dado que una organización depende de su red de TI para ejecutar aplicaciones y operaciones comerciales de misión crítica, es fundamental garantizar que la infraestructura de red subyacente sea confiable, segura, sólida y escalable.

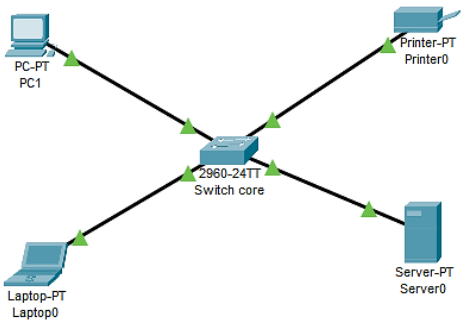
La infraestructura de red es una parte de la infraestructura de la TI que incluye el hardware, software, los sistemas y los dispositivos que posibilitan el flujo de los datos en toda la empresa para conectar a los usuarios, los dispositivos, las aplicaciones y el Internet, entre otras cosas. Debido a su conexión con el mundo exterior, la infraestructura de red es un punto vulnerable que debe protegerse. A medida que las empresas desarrollan cada vez más aplicaciones de la nube que se encuentran distribuidas, utilizan varios datos y responden con rapidez ante eventos específicos, aumenta la importancia de contar con la infraestructura de red adecuada (*Red Hat*, 2023).

Clasificaciones de las redes

De acuerdo con Fuertes (2022), las redes se pueden clasificar de acuerdo con su tamaño y propósito en:

LAN (*Local Área Network*): son redes de propiedad privada que conectan dos o más computadoras en un área local con el propósito de compartir recursos e información. Operan a velocidades de 10, 100 y 1000Mbps, 1 Gbps, 10 Gbps o más. La Figura 3 ilustra una configuración básica de una red LAN

Figura 3. Red LAN

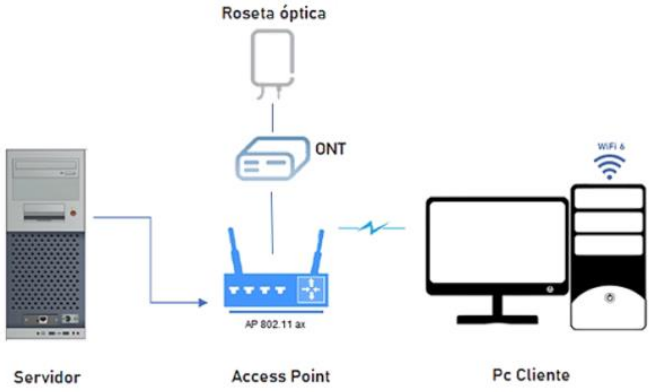


Fuente: elaboración propia.

WLAN (*Wireless Local Area Network*): Es otra LAN, en la cual no se hace uso de cables. El medio de transmisión es el aire, ondas electromagnéticas o radioeléctricas (i.e., aquellas ondas fijadas convencionalmente por debajo de 3000 GHz). El punto central de conexión es el punto de acceso inalámbrico (Access Point, AP) o un enrutador inalámbrico que repite las señales de radio a los

dispositivos cercanos que están dentro de la cobertura local (tecnología WIFI, *Wireless Fidelity*), Figura 4 ilustra un esquema de una WLAN.

Figura 4. Red WLAN

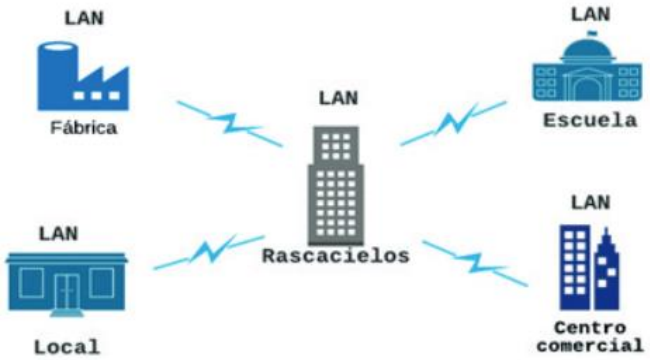


Fuente: Tomado de (Ocaña et al., 2023)

MAN (*Metropolitan Area Network*): Una red MAN integra múltiples LAN dentro de una ciudad, en una red más grande. Las velocidades de transmisión de datos de MAN son más rápidas que las de LAN y WAN. La razón de la existencia de MAN es la necesidad de compartir y acceder a los recursos de una ciudad. Una red MAN representa un grupo de LANs interconectadas dentro del límite geográfico de un pueblo o ciudad (Odom, 2016).

La Figura 5 ilustra cómo en un solo lugar se conectan redes de área local de diferentes partes.

Figura 5. Red MAN



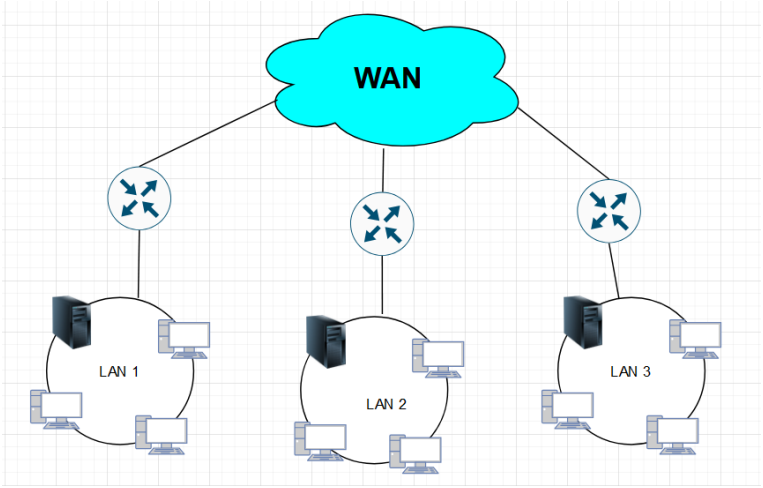
Fuente: Tomado de (Fuertes, 2022)

WAN (*Wide Area Network*): Es una red informática que cubre una amplia área geográfica, por lo general un país o continente, al utilizar líneas de

telecomunicaciones dedicadas tales como como líneas telefónicas, líneas arrendadas o vía satélite. En general las WAN son redes que tienen un gran alcance en su señal, es decir las WAN están compuestas por redes PAN, LAN y MAN.

Las empresas debido al crecimiento de sus negocios instalan redes WAN para su comunicación privada con sistemas de radioenlaces, satélites o por el mismo proveedor de internet, uniendo así varias sucursales de distintas ubicaciones geográfica, cada sucursal se puede interpretar como una red LAN, la Figura 6 ilustra la conformación de una red WAN con varias redes LAN.

Figura 6. Red WAN



Fuente: elaboración propia.

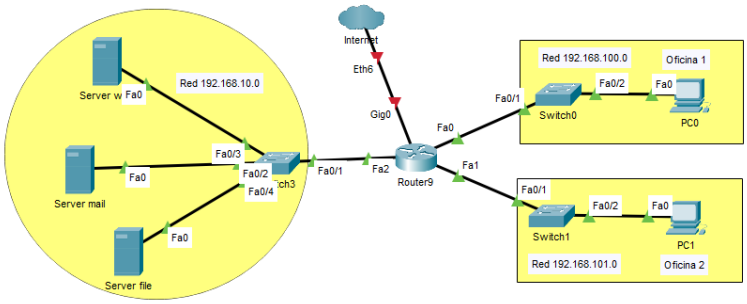
Topologías en redes

La topología de red define su estructura física, es decir la manera en que los hosts están organizados, conectados y cómo se comunican entre sí para intercambiar datos. Como señala (Pineda & Morales, 2020), topología de red es el arreglo físico o lógico en el cual los dispositivos o nodos de una red (computadoras, impresoras, servidores, *hubs, switches*, enrutadores, etc.) se interconectan entre sí a través de un medio de comunicación. Está compuesta por dos partes: La topología lógica y topología física.

Topología lógica: se refiere a la forma en que una red transfiere tramas de un nodo al siguiente. Esta topología identifica conexiones virtuales mediante interfaces de dispositivo y esquemas de direccionamiento IP de capa 3 (Walton, 2023).

La topología lógica se define como la forma en que los hosts acceden a los medios, independiente de la distribución física de los dispositivos; en la figura 7 se observa un ejemplo de topología lógica.

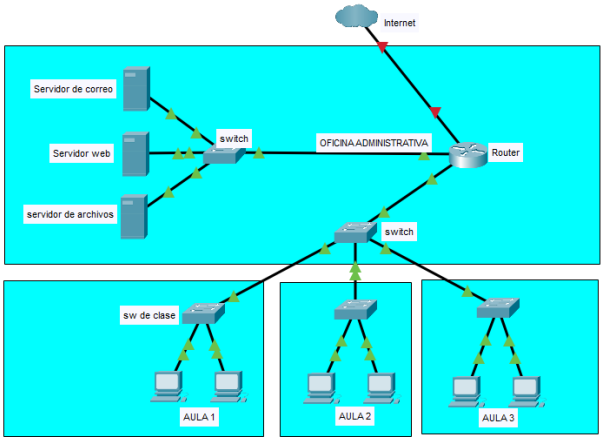
Figura 7. Topología Lógica



Fuente: elaboración propia

Topología física: identifica las conexiones físicas y cómo se interconectan los dispositivos finales y los dispositivos intermedios (es decir, routers, switches y puntos de acceso inalámbrico). En esta topología se puede incluir la ubicación específica del dispositivo, como el número de habitación y la ubicación en el bastidor del equipo. Las topologías físicas suelen ser punto a punto o estrella, se puede visualizar en la Figura 8 el esquema de una topología física (Walton, 2023).

Figura 8. Topología Física



Fuente: elaboración propia

Existen diversos tipos de topologías físicas de red, cada una con características que ofrecen ventajas y desventajas únicas que las hacen adecuadas para distintos escenarios de red. Las topologías físicas que se utilizan comúnmente son de bus, de anillo, en estrella, en estrella extendida, árbol y en malla; en la figura 9 se observa las topologías físicas descritas.

Topología tipo bus: una de las topologías más sencillas que utiliza un único cable al que se conectan todos los componentes directamente. El cable debe terminarse apropiadamente en ambos extremos para evitar desadaptaciones. Todos los dispositivos comparten el mismo canal, por lo que debe existir una forma apropiada de ingreso al medio, quedando limitada tanto la cantidad de dispositivos como la longitud física de la red. La rotura del cable deja fuera de servicio el sistema, ejemplo: LAN de cable coaxial (Liberatori, 2018).

Topología tipo anillo: conecta un elemento con el siguiente y el último con el primero. En este tipo de red la comunicación depende del paso de un paquete especial, denominado testigo o token, que se utiliza para ordenar la comunicación y permitir un acceso equitativo a todos los componentes. Si uno de los componentes falla o uno de los enlaces cae, la red queda fuera de servicio ejemplo: redes de fibra óptica como columna vertebral o *backbone* de red WAN (Liberatori, 2018).

Topología tipo estrella: las computadoras, periféricos y dispositivos de red están conectados de forma independiente con un dispositivo central conocido como concentrador *hub, switch,* conmutador. Para este tipo de topología se utiliza principalmente un cable de par trenzado o una fibra óptica (Odom, 2016).

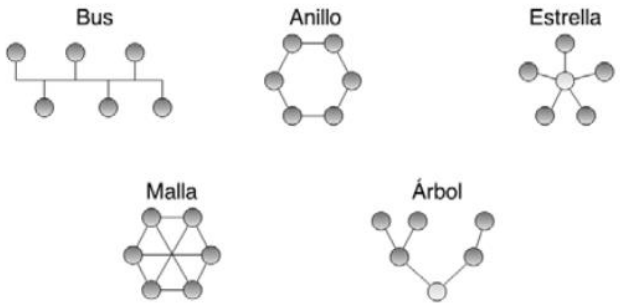
Topología tipo malla: Cada computadora está conectada con otra para formar la red. Por lo general, una red de área extendida (WAN) utiliza este tipo de topología para interconectar LANS entre ciudades, países y continentes (Odom, 2016).

Topología tipo árbol: se trata de una topología centralizada, desarrollada a partir de un nodo raíz, a partir del cual se van desplegando los demás componentes como

ramas. Los elementos de la red se ordenan en una estructura jerárquica, en donde se destaca un elemento predominante o raíz. El resto de los elementos comparte una relación tipo padre-hijo. El encaminamiento de los mensajes de este tipo de redes debe realizarse de tal manera de evitar lazos en la comunicación. Si falla un elemento podrían presentarse complicaciones, quedando parte de la estructura aislada, pero si falla la raíz, la propia red quedaría dividida en dos partes que no podrían comunicarse entre sí (Liberatori, 2018).

Topología tipo estrella extendida: las computadoras, periféricos y dispositivos de red están conectados en dos o más redes de topología en estrella cuyos componentes centrales (es decir, los switches) se interconectan a través de un bus. En apariencia, este tipo de topología combina estrella y bus, se usa un par de cables trenzados para la topología en estrella, mientras que para la topología de bus se usa una fibra óptica (Odom, 2016).

Figura 9. Topologías



Fuente: Tomado de (Liberatori, 2018)

Métodos de aseguramiento para la infraestructura de red

Los métodos de aseguramiento para la infraestructura de red son técnicas y prácticas utilizadas para proteger las redes y garantizar su funcionamiento seguro. Estos métodos se aplican para prevenir ataques, mitigar riesgos y asegurar la integridad, confidencialidad y disponibilidad de la información transmitida. (Briceño, 2021)

Tipos de controles de seguridad

Desde el punto de vista de Gobierno Electrónico (2020), los controles de seguridad son los mecanismos técnicos o administrativos que se llevan a cabo para implementar los estándares. Todos los controles de seguridad se ajustan a los estándares, pero no todos los estándares se ajustan a los controles de seguridad. Las pruebas de los controles de seguridad se han diseñado para monitorear y medir si se cumplen de manera efectiva los estándares definidos, existen cuatro tipos de controles de seguridad principales:

Controles preventivos

Los controles preventivos son aquellos que se han elaborado para evitar que suceda un evento. Estas barreras de protección son la primera línea de defensa para evitar el acceso que no esté autorizado o los cambios que no se encuentren en el parámetro deseado en la red. (AWS, 2024)

Controles proactivos

Los controles proactivos son controles de seguridad diseñados o elaborados para evitar la creación de recursos que estén fuera del cumplimiento con las normas. Estos controles reducen la cantidad de eventos de seguridad que gestionan los controles de respuesta y de detección; además, de garantizar que los recursos implementados cumplan con las normas antes de realizar la implementación. (AWS, 2024)

Controles de detección

Los controles de detección fueron diseñados para detectar, registrar y alertar después que se produzca un evento, estos tipos de control son una parte fundamental de los marcos de gobernanza, siendo una segunda línea de defensa, notificando los problemas de seguridad que han eludido los controles preventivos. (AWS, 2024)

Controles de respuesta

Los controles de respuesta diseñados para corregir eventos adversos o desviaciones con respecto a su base de seguridad; como ejemplos de controles de respuesta técnica incluyen la aplicación de revisiones a un sistema, el aislamiento de un virus, el cierre de un proceso o el reinicio de un sistema. (AWS, 2024)

Marcos de referencia de ciberseguridad

Son sistema de pautas, estándares y buenas prácticas para gestionar los riesgos cibernéticos de una organización, aplicando un plan de acción que ayuda a identificar, evaluar y mitigar las amenazas.

Marco de ciberseguridad de NIST

El Marco de ciberseguridad de NIST según Mahn et al. (2022), puede ayudar a una organización a mejorar su programa de ciberseguridad. El Marco ofrece un lenguaje común para entender, gestionar y comunicar el riesgo de seguridad permitiendo identificar y priorizar acciones para reducir dicho riesgo, sirve como herramienta para alinear las estrategias de políticas, negocios y tecnología, y es aplicable a la gestión del riesgo cibernético en toda la organización.

De acuerdo con Mahn et al. (2022), el marco está organizado en cinco funciones clave: identificar, proteger, detectar, responder, recuperar; que son los cinco términos que se describen en la tabla 1; funciones del marco de seguridad NIST, cuando se consideran conjuntamente proporcionan una visión integral del ciclo de vida para la gestión del riesgo de ciberseguridad en el tiempo.

Tabla 1. Funciones del marco de seguridad NIST

FUNCIÓN	DESCRIPCIÓN
IDENTIFICAR	Desarrollar una comprensión organizacional para la gestión del riesgo de ciberseguridad de: sistemas, activos, datos y capacidades**.**
PROTEGER	Desarrollar e implementar las protecciones apropiadas para garantizar la entrega de servicios.
DETECTAR	Desarrollar e implementar las actividades apropiadas para identificar cuando ocurra un evento de ciberseguridad.
RESPONDER	Desarrollar e implementar las actividades apropiadas para tomar acción en relación con un evento de ciberseguridad detectado.
RECUPERAR	Desarrollar e implementar las actividades apropiadas para mantener planes para la resiliencia y para reestablecer cualesquiera capacidades o servicios que hayan sido afectados durante un evento de ciberseguridad.

Fuente: elaboración propia

1.4. Controles CIS

Los Controles Críticos de Seguridad (*CIS Controls*) se desarrollaron en 2008 como una respuesta a la creciente necesidad de un enfoque estructurado y efectivo para combatir las amenazas cibernéticas. Fueron creados bajo la colaboración del gobierno de los Estados Unidos, a través de agencias especializadas en seguridad cibernética, junto con organizaciones del sector privado dedicadas a la investigación y desarrollo de tecnologías de seguridad. Esta alianza público-privada busca diseñar un conjunto de directrices que no solo fueran teóricas, sino aplicables de manera práctica y efectiva en diferentes tipos de organizaciones (Marchand-Niño & Vega Ventocilla, 2020).

El principal objetivo de los Controles CIS es detener los ciberataques más frecuentes y dañinos mediante la implementación de técnicas y acciones específicas. Estas técnicas no se limitan a medidas generales de seguridad, sino que abordan las áreas más vulnerables de los sistemas de información que, de no ser protegidas adecuadamente, podrían ser fácilmente comprometidas por atacantes (Montesino et al., 2013). Los controles proporcionan pasos claros y específicos que cualquier organización, independientemente de su tamaño o sector, puede seguir para reducir significativamente su exposición a las ciber amenazas.

El enfoque inicial detrás de los Controles CIS como menciona (Granados, 2016) fue identificar los ataques más comunes que las organizaciones enfrentan en su día a día. Para ello, se basaron en un análisis exhaustivo de incidentes de seguridad a nivel global, con datos recopilados de una amplia gama de fuentes, incluyendo incidentes documentados por agencias gubernamentales y estudios de seguridad realizados por empresas privadas. Esta información permitió crear una base de controles que actúan como defensa fundamental frente a las tácticas y técnicas más utilizadas por los cibercriminales.

Evolución y Comunidad de los Controles CIS

Desde su creación, Honores (2021) menciona que los Controles CIS han evolucionado y madurado gracias a la colaboración de una comunidad internacional de personas e instituciones que:

- **Compartición de Información:** Se comparte información sobre ataques y atacantes para identificar sus causas y tomar acciones defensivas.
- **Recursos Colaborativos:** Se proporcionan herramientas, ayudas y traducciones para resolver problemas de seguridad.
- **Monitoreo de Amenazas:** Se da seguimiento a la evolución de las amenazas, las capacidades de los adversarios y los vectores actuales de intrusiones.
- **Resolución Comunitaria:** Se identifican y resuelven problemas comunes de forma colectiva.

Este enfoque comunitario garantiza que los Controles CIS no sean solo una lista de buenas prácticas, sino un conjunto de acciones priorizadas, con soporte internacional, que los hace implementables, utilizables, escalables y compatibles con los requerimientos de seguridad actuales.

Controles CIS (versión 7)

En la versión 7 de los Controles CIS, se han establecido 20 controles distribuidos en tres categorías clave para una implementación, medición y automatización eficiente.

Controles básicos

Los primeros seis controles CIS son los más esenciales y permiten la gestión de activos, vulnerabilidades y la configuración segura de hardware y software. En la tabla 2 se muestra los controles básicos con su respectiva descripción.

Tabla 2. Controles básicos

Control	Descripción
CCS1	Inventario de dispositivos autorizados y no autorizados
CCS2	Inventario de software autorizado y no autorizado
CCS3	Gestión continua de vulnerabilidades
CCS4	Uso controlado de privilegios administrativos
CCS5	Configuración segura para hardware y software en dispositivos móviles, portátiles, estaciones de trabajo y servidores
CCS6	Mantenimiento, monitoreo y análisis de logs de auditoría

Fuente: Tomado de (Honores, 2021).

Controles funcionales

Esta categoría incluye 10 controles orientados a la protección de redes, datos y el control de accesos. En la tabla 3 se muestra los controles funcionales vs la descripción.

Tabla 3. Controles funcionales

Control	Descripción
CCS7	Protección de correo electrónico y navegador web
CCS8	Defensa contra malware
CCS9	Limitación y control de puertos de red, protocolos y servicios
CCS10	Capacidad de recuperación de datos
CCS11	Configuración segura de equipos de red (cortafuegos, enrutadores, conmutadores)
CCS12	Defensa de borde
CCS13	Protección de datos
CCS14	Control de acceso basado en la necesidad de conocer
CCS15	Control de acceso inalámbrico
CCS16	Monitoreo y control de cuentas

Fuente: Tomado de (Honores, 2021).

Controles organizacionales

Los controles organizacionales incluyen actividades clave para la capacitación, seguridad de aplicaciones y la respuesta ante incidentes. Como se muestra en la tabla 4 los controles organizacionales y su descripción.

Tabla 4. Controles organizacionales

Control	Descripción
CCS17	Implementar un programa de concienciación y capacitación en seguridad
CCS18	Seguridad del software de aplicación
CCS19	Respuesta y gestión de incidentes
CCS20	Pruebas de penetración y ejercicios de Equipo Rojo

Fuente: Tomado de (Honores, 2021).

CAPÍTULO II. DISEÑO METODOLÓGICO

2.1. Caracterización de la institución

El Grupo Chevez es el conjunto o la unión de varias Empresas debidamente constituidas, en la cual cada oficina de las diferentes empresas y áreas se conecta a la misma red de datos hacia el *DATA* center el mismo se encuentra ubicado en la oficina principal de Minervilla; desde esta se establecen las comunicaciones con los diferentes campamentos a través de enlaces radiales.

Grupo Chevez está conformada por 5 empresas, las mismas que cuentan con un servicio diferente que se detalla a continuación:

ICBINEN S.A; que tiene como actividad la explotación de criaderos de camarones (camaroneras) y además es un criadero de larvas de camarón (laboratorios de larvas de camarón)

Joffre Javier Chévez Chacón (Maquinarias); su actividad principal es el alquiler de maquinarias pesadas y transporte de material pétreo.

GRUMINEP CIA LTDA; se dedica a la producción de metales preciosos básicos, producción y refinación de metales preciosos sin labrar y labrados como el oro, plata, platino a partir de minerales y residuos.

COMPAÑIA DE TRANSPORTE PESADO CHEVEZ TRANSPCHEVEZ S.A; dedicado a todas las actividades de transporte de carga por carretera, incluido camionetas en las que se transporta troncos, ganado, transporte refrigerado, carga pesada, carga a granel, transporte de cisternas, automóviles, desperdicios y materiales de desecho.

MINERVILLA CIA LTDA; trabaja en la explotación de recursos minerales de cobre, níquel, plomo y zinc, se encuentra ubicada con su sede principal en Camilo Ponce

Enríquez. Fue fundada el 02 de abril del 2012 y actualmente cuenta con 312 personas laborando.

Misión

Minervilla Cía. Ltda., es una empresa creada para explorar, explotar, procesar y comercializar recursos minerales, desarrollando una minería modelo a través de operaciones seguras, de bajo costo, con tecnología innovadora, con compromiso social y respeto por el medio ambiente, creando valor para los accionistas, los empleados, la localidad en la que opera y el país.

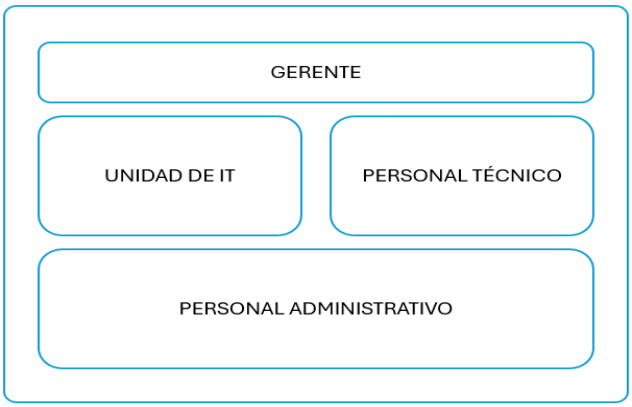
Visión

En el 2028, Minervilla Cía. Ltda. Será una empresa minera reconocida en el país por sus buenas habilidades y manejo técnico, operacionales, ambiental y de responsabilidad social en las actividades que desarrolla de exploración, explotación, proceso y comercialización de minerales.

Descripción general

Minervilla CIA Ltda. es una sucursal del Grupo Chevez, la cual es una empresa en Ecuador, con sede principal en Camilo Ponce Enríquez. Opera en Minería de Cobre, Níquel, Plomo y Zinc. La empresa fue fundada en 02 de abril de 2012; dentro de su apartado organizacional está dividida en bloques que permiten gestionarse al momento de asignar acceso a la maquinaria tecnológica que se usa en la misma como se muestra en la figura 10.

Figura 10. Estructura Organizacional



Fuente: elaboración propia

Dentro de la distribución se han colocado las responsabilidades inherentes al cargo siendo:

Gerente

Revisar y aprobar el documento de Normas de Seguridad para el Manejo del Sistema Informático; además, de gestionar y proveer de los recursos materiales y económicos necesarios, para implantar y mantener el desarrollo permanente del proceso.

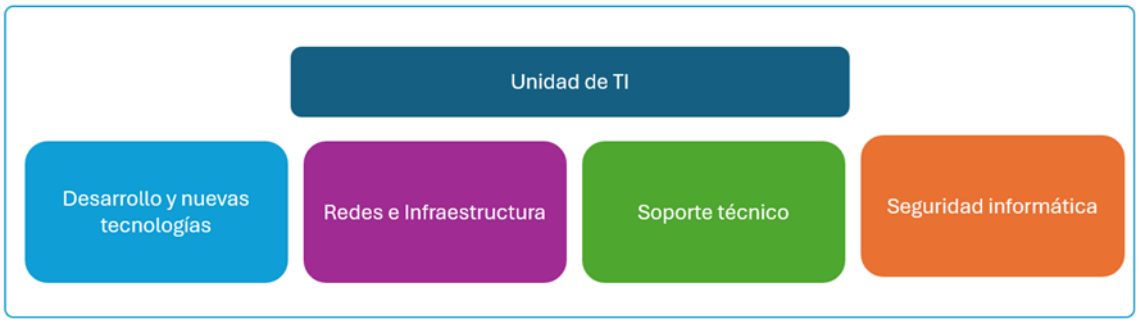
Promover la participación con compromiso y responsabilidad en el cumplimiento de los objetivos, así como de las responsabilidades contenidas en el documento.

Unidad de TI

Garantiza el correcto funcionamiento de la infraestructura tecnológica con las herramientas brindadas por MINERVILLA CIA. LTDA tanto en software como en hardware.

Capacita al personal para la correcta aplicación de las normativas, así como de controlar el buen uso de los recursos informáticos y reportar los casos de incumplimiento.

Figura 11. Estructura organizacional Unidad de TI



Fuente: elaboración propia

El área se encuentra dividida internamente como se muestra en la figura 11, contando con un total de 4 áreas departamentales:

- **Desarrollo y nuevas tecnologías**

Encargada del desarrollo de nuevos aplicativos, control de calidad, mantenimientos de sistemas informáticos y análisis de nuevas tecnologías que se pueden aplicar a la empresa.

- **Redes e Infraestructura**

Se encarga de gestionar las redes internas/externas, monitorear la tecnología de red, así como de garantizar que la red de área local (LAN), red amplia (WAN) y los servicios en la nube funcionen de manera correcta; además, está encargado de instalaciones y contratos con los proveedores de comunicaciones.

- **Soporte técnico**

Brinda soporte a los empleados en los aspectos técnicos relacionados con las tecnologías que empleen en cualquier área de su trabajo a nivel de software y hardware como actualizaciones, instalaciones, mantenimientos asegurándose de que todo funcione de manera óptima.

- **Seguridad Informática**

Se encargan de proteger los datos confidenciales de la organización, detección y respuesta a incidentes, planificación de medidas preventivas (como el cifrado). Además, administran la seguridad de la red (LAN y WAN), la seguridad de internet (como documentos y archivos descargados de Internet), así como de terminales (computadoras, celulares y tabletas).

Personal administrativo y técnico

Cumplen todas las normas descritas, así como de reportar a la unidad de Información Tecnológica cualquier novedad que implique el no cumplimiento de las diferentes normas indicadas.

Normativa

Dentro de Minervilla se busca garantizar el adecuado funcionamiento de los equipos tecnológicos tanto de software como de hardware en los diferentes departamentos de la Empresa, por lo que actualmente la empresa cuenta con las siguientes normativas:

- La Unidad de IT deberá planificar y ejecutar procedimientos de mantenimientos preventivos y/o correctivos a nivel de hardware y software cada 3 meses.
- El uso del equipo será exclusivamente para realizar las actividades relacionadas con las funciones asignadas.
- El computador de escritorio deberá estar conectado a un Sistema de Alimentación Ininterrumpida de energía UPS, en caso de equipos tipo Servidor deben estar conectados a UPS con características *ON LINE*.
- Los equipos portátiles e impresoras de tinta a inyección siempre deberán estar conectadas a tomacorrientes normales y protegidos con tierras físicas, en caso de que no cuenten con tomacorrientes de este tipo el equipo deberá ser conectado a un regulador de voltaje adecuado a la carga del equipo.

- Se prohíbe conectar aparatos o equipos que no sean computadoras a los reguladores o fuentes ininterrumpidas de energía UPS.
- Se prohíbe fumar e ingerir alimentos o bebidas cerca de los equipos de cómputo.
- El cuarto de comunicación deberá estar aclimatado con aire acondicionado.
- Se dará preferencia al uso de software libre en los equipos de cómputo con autorización de la unidad de TI.
- Cada equipo deberá tener instalado sus licencias originales del sistema operativo y paquetes de Office.
- Se prohíbe el uso de archivos activadores o crack en los computadores
- La Unidad de TI debe velar por la correcta instalación de las actualizaciones propias del sistema operativo.
- Se prohíbe instalar o hacer uso de programas de cómputo sin la licencia del propietario ni autorización de la Unidad de TI.
- Todo equipo deberá tener instalado un programa de antivirus debidamente actualizado.
- Se prohíbe la manipulación de equipos de telecomunicaciones sin previa autorización de la Unidad de TI.
- Cualquier falla en los equipos y programas de cómputo el empleado deberá reportar a la Unidad de TI.
- La Unidad de TI, asignará equipos de cómputo a nuevos empleados previa solicitud enviada por la Unidad de Gestión de Talento Humano.
- El empleado que renunciare debe acercarse a la Unidad de TI para entregar el equipo de cómputo el mismo que será revisado, posterior a ello se remitirá el documento de entrega-recepción firmado que permitirá el trámite de salida.
- Los equipos de cómputo que sean liberados por los empleados quedaran bajo custodia del departamento de Bodega.
- Se prohíbe el uso de los equipos de cómputo a personas ajenas a la compañía.

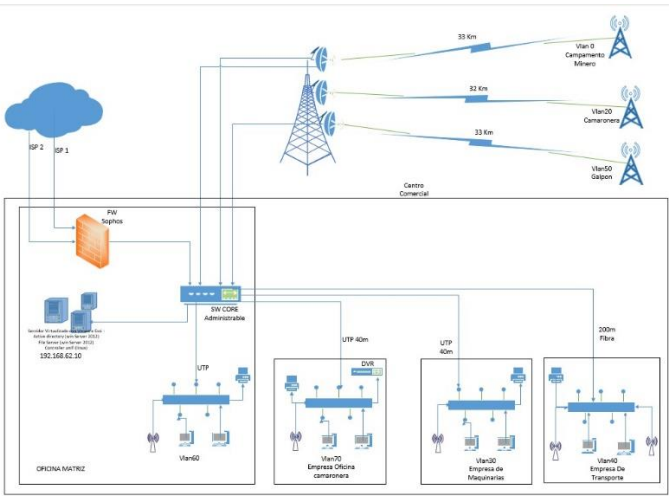
- Se prohíbe la salida de equipos de cómputo de propiedad de la compañía de las instalaciones sin previa autorización de la Unidad de TI o de bodega excepto quienes por su perfil laboral requieren movilizarse con su equipo.
- Cualquier daño que sufra el equipo por causas humanas con alevosía y ventaja, serán puestos a evaluación para efectuar el pago de los daños.

Se prohíbe el ingreso de equipos de cómputo personales sin autorización del Jefe de Campamento de la Unidad de TI o Unidad de Gestión de Talento Humano.

Análisis de la infraestructura de red

Como se observa en la figura 12, la infraestructura de red es la propuesta planteada para la optimización de recursos y mejor análisis.

Figura 12. Infraestructura de red



Fuente: elaboración propia

Conexión a Internet

Existen dos proveedores de servicios de Internet (ISP 1 e ISP 2), lo que proporciona redundancia. Además, la conexión pasa a través de un firewall (Sophos) antes de llegar al *switch core*.

Equipos en la oficina matriz

En los equipos que se encuentran en la oficina matriz esta la presencia de servicios virtualizados (*Active Directory y File Server*). Con una subred principal con dirección IP 192.168.62.10.

Conexión entre sitios

Enlaces de fibra y UTP que conectan diversas ubicaciones:

- Oficinas locales (VLAN 60 y VLAN 70).
- Empresa de maquinaria (VLAN 30).
- Empresa de transporte (VLAN 40).

Uso de enlaces inalámbricos para sitios remotos (Campamento Minero, Camaronera y Galpón) asociados a VLAN 0, 20 y 50.

Segmentación de red

La segmentación de red esta generada mediante VLANs como, por ejemplo: VLAN 30, 40, 60, etc.

Otros elementos

Dentro de otros elementos se tiene DVR para el uso de cámaras de seguridad, además de una conexión inalámbrica en algunas oficinas.

Tipo de red

La infraestructura de red de Minervilla corresponde a una red híbrida, que combina red cableada (LAN) y red inalámbrica (WAN):

- **Red cableada (LAN):** Utiliza enlaces UTP y fibra óptica para interconectar oficinas, servidores y dispositivos dentro de un entorno local.
- **Red inalámbrica (WAN):** Emplea enlaces inalámbricos para conectar ubicaciones remotas como el Campamento Minero, la Camaronera y el Galpón.

Componentes principales

Servidores

- **Servidor virtualizado:**
  - Rol Active Directory: para la gestión de usuarios y recursos.
  - Rol File Server: para almacenamiento centralizado.
- **Características destacadas:** Virtualización en ESXi con sistemas operativos Windows Server 2021.

Dispositivos de red

- **Firewall (Sophos):**
  - Es control perimetral de seguridad.
  - Posiblemente configurado para reglas NAT (*Network Address Translation*) que son conjunto de condiciones y acciones que se aplica a los paquetes de red; también está configurado para el filtrado de tráfico y VPN (*Virtual Private Network – Red Privada Virtual*).
- ***Switch Core* administrable:**
  - Centraliza la conexión entre oficinas y enlaces remotos.
  - Permite segmentación mediante VLANs.
- **Switches distribuidos:**
  - Conectan estaciones de trabajo y dispositivos finales en cada oficina.

Dispositivos inalámbricos y enlaces

- Torres de comunicación para enlaces de 32-33 km hacia ubicaciones remotas.
- Equipos de red inalámbrica en oficinas y otras ubicaciones.

Estaciones de trabajo y periféricos

- PCs conectadas a la red en oficinas locales y remotas.
- DVR para cámaras de video vigilancia.

Dichos ítems presentan la generalidad de los equipos, detallando a continuación la zona del campamento, ubicación, equipos que utilizan; así como su marca, modelo y serie además del estado en que se encuentran, como se presenta en la tabla 5.

Tabla 5. Infraestructura tecnológica

ZONA	UBICACIÓN	EQUIPO	MARCA	MODELO		SERIE	ESTADO
CAMPAMENTO	OFICINAS PARTE ALTA	ACCESS POINT	UBIQUITI	UAP-AC-Lite	POE	74ACB993EF0C	
CAMPAMENTO	NUEVAS OFICINAS	ACCESS POINT	UBIQUITI	UAP-AC-Lite	POE	74ACB993EF17	
CAMPAMENTO	CAMARA 470	DSL	NETSYS	NV-500	DSL CONECTION	93003CB310070195	
CAMPAMENTO	TORRE COMUNICACIÓN	DSL	NETSYS	NV-500	DSL CONECTION	93003CB310070194	
C.C.UNIORO	OFICINAS MINERVILLA	FIREWALL	SOPHOS	XG115		C190A2DKJ6Y4T57	
CAMPAMENTO	SISTEMAS	ROUTER	NEEXT	NEBULA		4904U2180702240	SALA DE

				AC1200			REUNIONES
CAMPAMENTO	SISTEMAS	ROUTER	TP-LINK	TL-WR940N	450MBPS	2172158011532	MINERVILLA FREE
CAMPAMENTO	SISTEMAS	ROUTER	TP-LINK	TL-WR941HP	4LAN/1WAN	2197327001214	BACKUP
CAMPAMENTO	SISTEMAS	ROUTER	TENDA	N301 EASY	3 PUERTOS	S/S	BACKUP
CAMPAMENTO	PRODUCCION	SWITCH	TRENDNET	TEG-424WS	24 PUERTOS	CA1CW215001198	
C.C.UNIORO	MINERVILLA-RACK SISTEMAS	SWITCH	TRENDNET	TEG-424WS		C21751GW00090	OK
CAMPAMENTO	TORRE COMUNICACIÓN	SWITCH	TRENDNET	TEG-082WS/A	8 PUERTOS	CA9JWS2100054	OPERATIVO

Fuente: elaboración propia

Topología de red

La topología es de orden jerárquico y se generaliza de la presente manera:

- **Nivel central (*core*):** Conexión principal gestionada desde el *switch core* administrable en la oficina matriz, los *Firewalls* y servidores también están ubicados en este nivel.
- **Nivel intermedio (distribución):** Uso de enlaces de fibra óptica y UTP hacia oficinas y ubicaciones remotas.
- **Nivel de acceso:** Switches distribuidos en cada ubicación, conectando estaciones de trabajo, dispositivos inalámbricos y cámaras.

2.2. Metodología de diagnóstico

Auditoría de seguridad física

La presente tiene como objetivo evaluar el estado actual de los dispositivos y sistemas tecnológicos de la organización identificando fortalezas, debilidades y riesgos asociados con su infraestructura de TI. El análisis abarca aspectos claves como el cumplimiento de actualizaciones del sistema operativo, implementación de medidas de seguridad, uso de software con licencia y la capacitación del personal en respuesta a incidentes como se muestra en la tabla 6. Los resultados obtenidos permitirán establecer un plan de acción que fomente la mejora continua en la gestión de tecnologías de la información, asegurando la protección de los activos digitales y el cumplimiento de estándares de seguridad obteniendo los siguientes resultados:

Tabla 6. Auditoría realizada en la empresa Minervilla

Departamento	Equipo	Sistema Operativo	Actualizado	Licencia	Soporta W11	Antivirus	Autenticación y acceso	Contraseña segura	Correo Empresarial	Implementación MFA	Acceso a red inalámbrica con dispositivo personal	Capacitación en respuesta a incidentes	Office Licenciado	Software sin licencia	Configuración BIOS/UEFI	Vulnerabilidades Identificadas	Cumplimiento de Políticas	Monitoreo de tráfico

ASISTENTE SSA	PMINUSSA3	W10PRO	SI	NO	NO	SI	LOCAL	SI	SI	NO	NO	NO	NO	Acrobat, Winrar, anydesk	NO	Ninguna detectada	SI	NO
GESTION AMBIENTAL	LMINGAM1	W10PRO	SI	NO	NO	SI	LOCAL	SI	SI	NO	NO	NO	NO	Acrobat, Winrar, anydesk	NO	Ninguna detectada	SI	NO
GESTION TALENTO H	LMINGAM2	W10PRO	SI	NO	NO	SI	LOCAL	SI	SI	NO	NO	NO	NO	Acrobat, Winrar, anyde	NO	SI	SI	NO

														sk				
MANTENIMIENTO	LMINMAN1	W10HSL	SI	SI	SI	SI	LOCAL	SI	SI	NO	NO	NO	NO	Acrobat, Winrar, anydesk	SI	Ninguna detectada	SI	NO
SISTEMAS	LMINIT01	W11PRO	SI	SI	SI	SI	ADMINISTRADOR	SI	SI	NO	SI	SI	NO	Autocad, acrobat, Winrar, anydesk	SI	Ninguna detectada	NO	NO
JEFATURA SSA	LMINUSSA	W11PRO	SI	SI	SI	SI	LOCAL	SI	SI	NO	NO	NO	NO	Acrobat, W	SI	Ninguna detectada	SI	NO

														inrar, anydesk			
TECNICO SSA	LMINUSSA2	W10 PRO	SI	NO	NO	SI	LOCAL	SI	SI	NO	NO	NO	NO	Acrobat, Winrar, anydesk	NO	Ninguna detectada	SI	NO
SISTEMAS	PMINSIS03	W10 PRO	NO	NO	SI	SI	ADMINISTRADOR	SI	NO	NO	NO		NO	Autocad, acrobat, Winrar, anyde	NO	Ninguna detectada	NO	NO

														sk				
BODEGA	LMINBOD1	W11HSL	SI	SI		SI	LOCAL	SI	SI	NO	NO	NO	NO	Acrobat, Winrar, anydesk	SI	SI	SI	NO
PRODUCCIÓN	LMINAPRO2	W10H	SI	SI	NO	SI	LOCAL	SI	SI	NO	NO	NO	SI	Autocad, acrobat, Winrar, anydesk	SI	Ninguna detectada	SI	NO
PRODUCCIÓN	LMINPRO2	W11H	SI	SI		SI	LOCAL	SI	SI	NO	SI	NO	SI	Autocad, a	SI	Ninguna detectada	NO	NO

														crobat, Winrar, anydesk				
PRODUCCIÓN	PMINAGEO1	W11PRO	SI	SI	SI	SI	LOCAL	SI	SI	NO	NO	NO	SI	Autocad, acrobat, Winrar, anydesk	SI	Ninguna detectada	SI	NO
PRODUCCIÓN	PMINGEO1	W11PRO	SI	SI	SI	SI	LOCAL	SI	SI	NO	NO	NO	SI	Autocad, acrob	SI	Ninguna detectada	SI	NO

														at, Winrar, any desk				
PRODUCCIÓN	LMINAPRO1	W10 HSL	SI	SI	NO	SI	LOCAL	SI	NO	NO	NO	NO	SI	Autocad, acrobat, Winrar, any desk	SI	Ninguna detectada	SI	NO
SECRETARIA GENERAL	LMINSEG1	W11 HSL	SI	SI	SI	SI	LOCAL	SI	SI	NO	NO	NO	NO	Autocad, acrobat, W	SI	Ninguna detectada	SI	NO

														inrar, anydesk				
TRABAJO SOCIAL	LMINTS01	W10 HSL	NO	SI	SI	SI	LOCAL	SI	SI	NO	NO	NO	NO	Acrobat, Winrar, anydesk	SI	Ninguna detectada	SI	NO
RECURSOS HUMANOS	PMINRHH1	W11 PRO	SI	SI	SI	SI	LOCAL	SI	SI	NO	SI	NO	NO	Acrobat, Winrar, anydesk	SI	Ninguna detectada	SI	NO
PARAMEDICOS	PMINM	W10 PRO	SI	SI	NO	SI	LOCAL	SI	SI	NO	NO	NO	NO	Acrobat	NO	Ninguna dete	SI	NO

	ED 2													, Winrar, anydesk		ctada		
MEDICO OCUPACIONAL	LMIN MED 1	W11 HSL	SI	SI	SI	SI	LOCAL	SI	SI	NO	NO	NO	NO	Acrobat, Winrar, anydesk	SI	Ningun a detectada	SI	NO
JEFE DE CAMPAMENTO	PMINJCAMP	W10 PRO	NO	NO	NO	SI	ADMINISTRADOR	SI	NO	NO	NO	NO	NO	Autocad, acrobat, Winrar, anyd	NO	Ningun a detectada	SI	NO

													esk					
SISTEMAS		Vmware ESXI 7.0.2	NO	OPENSOURCE		NO	ADMINISTRADOR	SI	NO	NO	NO		NO		NO	Ninguna detectada	NO	NO
TECNICO SSA	LMINUSA4	W11 PRO	SI	NO	SI	SI	LOCAL	SI	SI	NO	NO	NO	NO	Acrobat, Winrar, anydesk	SI	Ninguna detectada	SI	NO
CONTABLE	PMINFIN02	W10 PRO	SI	SI	NO	SI	ADMINISTRADOR	NO	SI	NO	NO	NO	NO	Acrobat, Winrar, anydesk	NO	Ninguna detectada	SI	NO
CONTABLE	PMINFIN01	W10 PRO	SI	SI	SI	SI	ADMINISTRADOR	SI	SI	NO	SI	NO	SI	Acrobat,	SI	Ninguna detectada	NO	NO

														Winrar, anydesk				
CONTABLE	LMINFIN02	W10HSL	SI	SI	SI	SI	ADMINISTRADOR	SI	SI	NO	NO	NO	SI	Acrobat, Winrar, anydesk	SI	Ninguna detectada	NO	NO
COMPRAS	LMINCOM01	W10PRO	NO	NO	SI	SI	ADMINISTRADOR	SI	SI	NO	SI	NO	NO	Acrobat, Winrar, anydesk	SI	Ninguna detectada	NO	NO
PRODUCCIÓN	PMINP	W10PRO	NO	SI	NO	SI	LOCAL	NO	NO	NO	NO	NO	NO	Acrob	NO	Ninguna dete	SI	NO

	RO 3												at, Winrar, anydesk		ctada		
PROYECTO	PMINPGAB1	W10PRO	NO	NO	SI	SI	LOCAL	NO	NO	NO	NO	NO	NO	Acrobat, Winrar, anydesk	SI	Ninguna detectada	SI	NO
	SRV-AD	W.Server 2016 - v1607	NO	NO		NO	ADMINISTRADOR	SI	NO	NO	NO		NO		NO	SI	NO	NO
	SRV-FILE	W.Server 2016 - v1607	NO	NO		NO	ADMINISTRADOR	SI	NO	NO	NO		NO		NO	SI	NO	NO
	UNIFI	Ubuntu 22.04.03 LTS	NO	OPENSOURCE		NO	ADMINISTRADOR	SI	NO	NO	NO		NO		NO	SI	NO	NO

Fuente: elaboración propia

Análisis de auditoria física

A continuación, se desglosa e interpreta los datos proporcionados para identificar las áreas claves evaluadas en la auditoría.

Campos principales del análisis:

- **Departamento y equipo:** Indica el área funcional y los dispositivos a ser evaluados.
- **Sistema operativo y licencia:** Verifica el software principal en uso y su legalidad (licencia).
- **Actualización y soporte para W11:** Comprueba si los sistemas están actualizados y si cumplen los requisitos de compatibilidad con Windows 11.
- **Antivirus y autenticación:** Evalúa la implementación de medidas básicas de seguridad.
- **Contraseña segura y MFA (autenticación multifactor):** Determina si se aplican mejores prácticas para acceso seguro.
- **Capacitación en respuesta a incidentes:** Evalúa si los usuarios están preparados para manejar incidentes.
- **Software y licencias:** Identifica aplicaciones instaladas, incluidas aquellas que no tienen licencia.
- **Vulnerabilidades detectadas y cumplimiento de políticas:** Examina el estado de seguridad y adherencia a normativas internas.

Tendencias observadas:

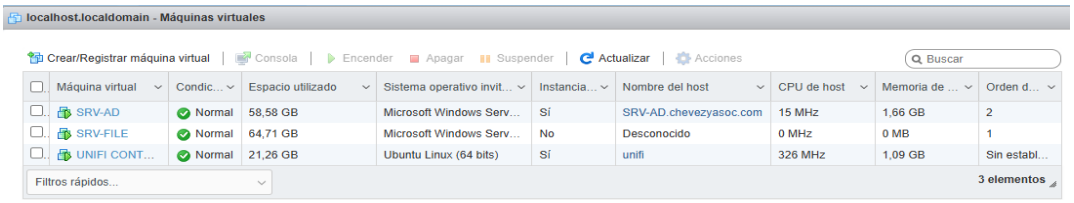
- En actualización de software, la mayoría de los dispositivos tienen sistemas operativos actualizados, pero algunos no soportan Windows 11.
- El antivirus está presente en la mayoría, pero algunas estaciones carecen de esta protección básica.
- La implementación de un Autenticador Multifactor (MFA) es limitada, lo que indica una oportunidad importante para mejorar la seguridad.

- Varias estaciones cuentan con software sin licencia, lo que representa un riesgo legal y de seguridad.

Auditoría de seguridad virtual

Adicional a los equipos físicos, Minervilla presenta los siguientes servicios virtuales a través del servidor principal en el data center que tienen como sistemas operativos a Windows y a Ubuntu Linux; cada uno en condiciones normales, tal como se observa en la figura 13.

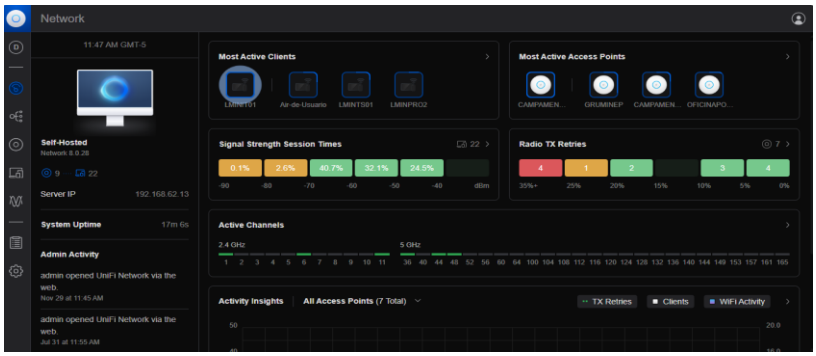
Figura 13. Las máquinas virtuales del servidor principal en el data center



Fuente: elaboración propia

Donde, la consola de gestión de los puntos de acceso (AP) Ubiquiti permite la administración centralizada de toda la red inalámbrica, brindando herramientas para monitorear, configurar y gestionar los dispositivos desde una interfaz intuitiva, pudiendo observar los clientes y los *Access Points* más activos en el momento de la revisión; así como el servidor IP y el tiempo de actividad del sistema. Como se puede verificar en la Figura 14.

Figura 14. Consola de gestión Ubiquiti



Fuente: elaboración propia

Panel desde Sophos Firewall

El panel de gestión de *Sophos Firewall* proporciona una visión integral del estado de la seguridad de la red. Este panel incluye monitoreo en tiempo real del tráfico de datos, detección de amenazas, configuración de reglas de *firewall*, y gestión de usuarios y dispositivos conectados. Además, permite administrar políticas de acceso, supervisar aplicaciones y gestionar conexiones VPN de forma eficiente. La interfaz está diseñada para ofrecer una experiencia fácil de usar, con gráficos y alertas que ayudan a priorizar la atención en posibles vulnerabilidades. Como se puede observar en la Figura 15.

Figura 15. Panel de gestión Sophos

Fuente: elaboración propia

Paneles de informes en Sophos

El panel de informes de Sophos presenta datos detallados sobre eventos de seguridad, tráfico de red, usuarios y amenazas detectadas; así como los VPN (*Virtual Private Network* – Red Privada Virtual) y el cumplimiento de las normativas, como se aprecia en la figura 16.

Figura 16. Panel de informes Sophos

Fuente: elaboración propia

Normas o estándares utilizados

Controles CIS (*Center for Internet Security*)

Los controles CIS (*Center for Internet Security* – Centro de Seguridad de Internet) enfocan los controles clave como configuraciones seguras, gestión de acceso y defensa contra ataques de red, además permiten mejorar prácticas para la ciberseguridad que ayudan a las organizaciones a identificar, gestionar y mitigar amenazas cibernéticas; además de prevenir ataques peligrosos, cumplir con marcos jurídicos, reglamentarios y normativos, así como proteger activos críticos. Dentro de los controles CIS se tiene la tabla 7 donde indica el tipo de control y su descripción, los cuales serán los analizados dentro de la presente investigación.

Tabla 7. Tipos de controles CIS y su descripción

Control CIS	Descripción del Control
CIS Control 1: Inventario y control de activos	Identificar y registrar todos los dispositivos autorizados y no autorizados conectados a la red.
CIS Control 3: Gestión continua de vulnerabilidades	Identificar y remediar vulnerabilidades conocidas mediante escaneo periódico y parches de software.
CIS Control 4: Control de uso de privilegios administrativos	Asegurar que los privilegios administrativos sean controlados y monitoreados para reducir riesgos.
CIS Control 8: Defensa contra malware	Implementar herramientas anti-malware y prácticas para proteger contra software malicioso.
CIS Control 9: Limitación y control de puertos, protocolos y servicios	Asegurar que solo se utilicen puertos, protocolos y servicios necesarios en los sistemas.
CIS Control 17: Implementación de un programa de seguridad	Establecer un programa formal para responder y gestionar incidentes de ciberseguridad.

Fuente: elaboración propia

ISO/IEC 27001

La ISO/IEC 27001, permite garantizar un enfoque integral de la gestión de la seguridad de la información y ayuda a la empresa a establecer la política y los objetivos de gestión de la seguridad de la información comprendiendo cómo gestionar los aspectos importantes, desarrollando controles necesarios para mejorar la seguridad de la información.

Identificación de vulnerabilidades y brechas

Registro de amenazas detectadas por el antivirus

En las figuras 17 y 18 se muestra las revisiones de los equipos LMINGAM1 y LMINGAM2 respectivamente; en los cuales se detalla la gravedad del equipo, fecha y hora en que la consola recibe el evento, la categoría y descripción del evento, usuario, componente, descripción del resultado, nombre, objeto, tipo de objeto,

nombre del objeto, Dirección MAC del equipo atacante, fecha de lanzamiento de la base de datos, usuario y dispositivo. Los mismos datos que se detallan en las tablas 8 y 9.

Figura 17. Revisión de equipo LMINGAM1

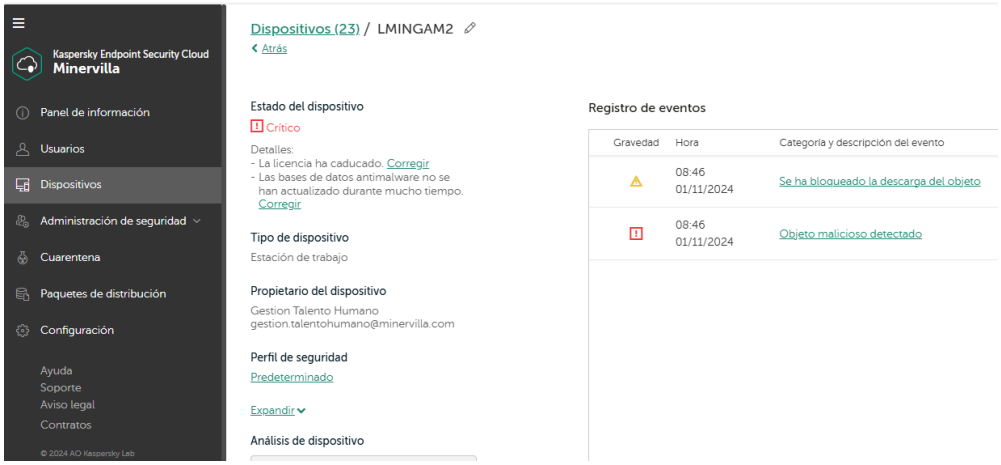
Fuente: elaboración propia

Tabla 8. Información del evento del dispositivo LMINBOD1

Información del evento Gravedad: Crítico Fecha y hora: Fecha y hora en que la consola recibe el evento 08/11/2024 16:04 Categoría y descripción del evento: Ataque de red detectado Usuario: LMINBOD1\BODEGA (Usuario activo) Componente: Protección frente a amenazas en la red Descripción del resultado: Bloqueado Nombre: Scan.Generic.PortScan.UDP Objeto: UDP de 192.168.137.214:55785 en 66.231.64.166:8477 Tipo de objeto: Paquete de red Nombre del objeto: UDP de 192.168.137.214:55785 en 66.231.64.166:8477 Dirección MAC del equipo atacante: 52-fa-86-83-3e-72 Avanzado: 66.231.64.166 Fecha de lanzamiento de la base de datos: 20/10/2024 14:49:00 Usuario: bodega@minervilla.com Dispositivo: LMINBOD1

Fuente: elaboración propia

Figura 18. Revisión de equipo LMINGAM2



Fuente: elaboración propia

Tabla 9. Información del evento del dispositivo LMINGAM2

Información del evento Gravedad: Crítico Fecha y hora: Fecha y hora en que la consola recibe el evento 01/11/2024 08:46 Categoría y descripción del evento: Objeto malicioso detectado Descripción del resultado: Detectados Tipo: Troyano Nombre: HEUR:Trojan-PSW.Script.Generic Usuario: LMINGAM2\PASANTE-AMBIENTAL (Iniciador) Objeto: https://tagmanager.apigruporsa.com/RSATAG\js.php?cid=5&dl=rsaLayer&ru=https%3A%2F%2Fwww.tiendanimal.es%2Farticulos%2Fdesparasitar-cachorros-cuando-hacerlo%2F&t=44 Razón: Análisis experto Fecha de lanzamiento de la base de datos: 19/10/2024 13:05:00 SHA256: BD845641939D89AD0C073068809A179FA3A0C3CCCA2CDB7E3C0AB8F345675184 MD5: EBD56ADCF28410DF40E34DA24E2A3A6C Usuario: gestion.talentohumano@minervilla.com Dispositivo:

Fuente: elaboración propia

Identificación de vulnerabilidades y brechas

En la tabla 10 de detalla las vulnerabilidades como configuraciones débiles, falta de actualizaciones, falta de segmentación de red, entre otras; además de la descripción de cada una y de su impacto potencial que tendrían en los sistemas. Y

mediante esta tabla se puede identificar qué tipo de vulnerabilidad y/o brecha tiene la empresa.

Tabla 10. Identificación de vulnerabilidades y brechas

Vulnerabilidad	Descripción	Impacto Potencial
Configuraciones débiles	Configuraciones predeterminadas o inseguras en sistemas y aplicaciones.	Exposición de datos, accesos no autorizados, compromiso de sistemas.
Falta de actualizaciones	Software desactualizado que contiene vulnerabilidades conocidas.	Permite explotación de fallos conocidos, ataques de malware o ransomware.
Carencia de monitoreo	Falta de sistemas que registren y supervisen eventos de red y sistemas.	Incapacidad de detectar actividades maliciosas o anomalías a tiempo.
Gestión deficiente de contraseñas	Uso de contraseñas débiles o falta de autenticación multifactor (MFA).	Accesos no autorizados, robo de cuentas privilegiadas.
Falta de segmentación de red	Redes no segmentadas que permiten el movimiento lateral de atacantes.	Incremento del alcance de los ataques en caso de un compromiso inicial.
Ausencia de plan de respuesta	Sin procedimientos documentados para responder ante incidentes.	Retraso en la mitigación de incidentes, mayor impacto de los ataques.

Fuente: elaboración propia

Análisis de riesgo

Evaluación de riesgo

Detectadas las vulnerabilidades existentes se procede a realizar la evaluación de las mismas buscando medir la probabilidad que ocasionó el impacto y el nivel de riesgo ya sea alto, medio o bajo. Como se detalla en la tabla 11.

Tabla 11. Evaluación de riesgos

Vulnerabilidad	Probabilidad (Alta/Media/Baja)	Impacto (Alta/Media/Baja)	Nivel de Riesgo (Alto/Medio/Bajo)
Configuraciones débiles	Alta	Alta	Alto
Falta de actualizaciones	Media	Alta	Alto
Carencia de monitoreo	Alta	Media	Alto
Gestión deficiente de contraseñas	Alta	Media	Alto
Falta de segmentación de red	Media	Media	Medio
Ausencia de plan de respuesta	Media	Alta	Alto

Fuente: elaboración propia

Matriz de riesgos

La matriz de riesgos permite tener un versus entre el impacto y la probabilidad, determinando si es baja, media o alta; es decir, si el impacto es alto y la probabilidad baja se tiene un riesgo medio; si el impacto es alto y su probabilidad es alta se tiene un riesgo alto; como se observa en la tabla 12.

Tabla 12. Tabla de impactos vs probabilidad

Impacto / Probabilidad	Baja	Media	Alta
Alta	Medio	Alto	**Alto**
Media	Bajo	Medio	**Alto**
Baja	Bajo	Bajo	Medio

Fuente: elaboración propia

Implementación

El presente apartado describe la implementación de Controles CIS a fin de identificar, gestionar y mitigar las vulnerabilidades de Minervilla.

Adaptación de controles CIS

En la tabla 13 se detalla el control CIS que existe para el problema al que está relacionado y junto a su descripción de control; para así poder generar la solución al problema que se esté presentando.

Tabla 13. Adaptación de controles CIS

Control CIS	Problema Relacionado	Descripción del Control
CIS Control 1: Inventario y control de activos	Falta de monitoreo	Identificar y registrar todos los dispositivos autorizados y no autorizados conectados a la red.
CIS Control 3: Gestión continua de vulnerabilidades	Falta de actualizaciones	Identificar y remediar vulnerabilidades conocidas mediante escaneo periódico y parches de software.
CIS Control 4: Control de uso de privilegios administrativos	Gestión deficiente de contraseñas	Asegurar que los privilegios administrativos sean controlados y monitoreados para reducir riesgos.
CIS Control 8: Defensa contra malware	Configuraciones débiles	Implementar herramientas anti-malware y prácticas para proteger contra software malicioso.
CIS Control 9: Limitación y control de puertos, protocolos y servicios	Falta de segmentación de red	Asegurar que solo se utilicen puertos, protocolos y servicios necesarios en los sistemas.
CIS Control 17: Implementación de un programa de seguridad	Ausencia de plan de respuesta	Establecer un programa formal para responder y gestionar incidentes de ciberseguridad.

Fuente: elaboración propia

Metodología de implementación

A fin de poder gestionar el manejo de vulnerabilidades se procede a usar los estándares seleccionados anteriormente, describiendo los mismos como: fase y relación con el estándar a ser utilizado, tomando en cuenta que están desarrollados mediante parámetros ISO 27001. Tal como se menciona en la tabla 14.

Tabla 14. Descripción de estándares

Fase	Descripción	Relación con el estándar
1. Planificación	Definir objetivos, analizar el entorno actual y establecer recursos necesarios.	NIST CSF - Identificar e ISO 27001 A.6
Identificar activos críticos y riesgos asociados.	**ISO 27001 A.8**: Gestión de activos.	
Establecer responsables para la implementación de cada control CIS.	**ISO 27001 A.7**: Roles y responsabilidades.	
2. Ejecución	Implementar las configuraciones, instalar herramientas y establecer políticas.	NIST CSF - Proteger
Configurar herramientas de seguridad, como MFA, escáneres de vulnerabilidades, SIEM, etc.	**ISO 27001 A.9**: Control de acceso.	
Establecer políticas de segmentación y configuración segura.	**ISO 27001 A.12**: Seguridad de operaciones.	
3. Monitoreo	Garantizar que las medidas de seguridad permanezcan efectivas a lo largo del tiempo.	NIST CSF - Detectar y Responder
Implementar herramientas de monitoreo continuo y alertas.	**ISO 27001 A.16**: Gestión de incidentes.	
Revisar la efectividad de los controles mediante auditorías periódicas.	**ISO 27001 A.15**: Auditoría de proveedores.	
Realizar simulacros de respuesta a incidentes.	**NIST CSF - Recuperar**	

Fuente: elaboración propia

Plan de acción

El plan de acción permitirá llevar a cabo la investigación, como la actividad a ser desarrollada, que se va a realizar en esta actividad; es decir, la descripción de la misma, quien va a ser el responsable. Además, se presente la fecha de inicio y

finalización, así como el estado de la actividad; llevando un mejor control de la investigación, tal como se detalla en la tabla 15.

Tabla 15. Cronograma o plan de acción

Actividad	Descripción	Responsable	Fecha de Inicio	Fecha de Finalización	Estado
1. Inventariar activos y aplicaciones	Crear un listado de dispositivos y software conectados a la red.	Administrador de TI	10/12/2024	20/12/2024	Pendiente
Identificar dispositivos autorizados y no autorizados	Escanear y documentar todos los dispositivos activos en la red.	Administrador de TI	10/12/2024	18/12/2024	Pendiente
Clasificar aplicaciones críticas	Evaluar el software que se considera crítico para las operaciones de negocio.	Analista de Sistemas	15/12/2024	20/12/2024	Pendiente
2. Configurar escaneo automático de vulnerabilidades	Implementar herramientas de escaneo como Nessus o OpenVAS.	Especialista en Red	15/12/2024	22/12/2024	Pendiente
Configurar informes periódicos	Automatizar reportes para evaluar las vulnerabilidades identificadas semanalmente.	Especialista en Red	17/12/2024	22/12/2024	Pendiente
Priorizar remediaciones	Establecer una lista prioritaria para corregir vulnerabilidades críticas.	Coordinador de Seguridad	18/12/2024	22/12/2024	Pendiente
3. Implementar autenticación multifactor (MFA)	Habilitar autenticación multifactor para usuarios con privilegios administrativos.	Equipo de Seguridad	18/12/2024	28/12/2024	Pendiente

Evaluar opciones de MFA disponibles	Revisar herramientas como Google Authenticator, Duo o Microsoft MFA.	Analista de Seguridad	18/12/2024	20/12/2024	Pendiente
Capacitar al personal	Instruir a los empleados sobre cómo usar MFA en sus cuentas.	Equipo de Formación	21/12/2024	23/12/2024	Pendiente
Implementar MFA en sistemas críticos	Activar MFA en servidores, aplicaciones y sistemas sensibles.	Administrador de TI	24/12/2024	28/12/2024	Pendiente
4. Segmentar la red mediante VLANs	Crear segmentación lógica para separar redes críticas y generales.	Administrador de Red	20/12/2024	30/12/2024	Pendiente
Identificar segmentos de red	Determinar qué dispositivos y usuarios necesitan estar en segmentos separados.	Ingeniero de Redes	20/12/2024	23/12/2024	Pendiente
Configurar VLANs en el switch principal	Implementar la segmentación lógica en los switches de la red.	Administrador de Red	24/12/2024	28/12/2024	Pendiente
Actualizar políticas de firewall	Asegurar que el tráfico entre segmentos sea monitoreado y controlado.	Especialista en Seguridad	29/12/2024	30/12/2024	Pendiente
5. Crear y documentar un plan de respuesta a incidentes	Definir procesos para identificar, contener y mitigar incidentes de seguridad.	Coordinador de Proyecto	25/12/2024	10/1/2025	Pendiente

Definir roles y responsabilidades	Asignar tareas específicas al personal en caso de incidentes.	Gerente de Seguridad	25/12/2024	28/12/2024	Pendiente
Establecer un procedimiento de notificación	Crear flujos de trabajo para informar incidentes a las partes interesadas.	Analista de Seguridad	29/12/2024	3/1/2025	Pendiente
Realizar simulaciones de respuesta a incidentes	Probar el plan mediante simulaciones para validar su efectividad.	Equipo de Seguridad	4/1/2025	10/1/2025	Pendiente
6. Implementar monitoreo continuo	Establecer herramientas y procesos para garantizar la seguridad continua.	Administrador de Seguridad	5/1/2025	15/1/2025	Pendiente
Configurar un SIEM para la recolección de datos	Implementar Splunk o Graylog para analizar eventos de seguridad.	Especialista en TI	5/1/2025	8/1/2025	Pendiente
Crear alertas en tiempo real	Definir umbrales críticos que generen notificaciones automáticas.	Administrador de TI	9/1/2025	12/1/2025	Pendiente
Revisar logs regularmente	Establecer un calendario para revisar y analizar logs de sistemas y aplicaciones críticas.	Analista de Seguridad	13/1/2025	15/1/2025	Pendiente

Fuente: elaboración propia

2.3. Metodología de investigación

La metodología de investigación para la propuesta de implementación de los Controles Críticos de Seguridad (CIS) en una infraestructura de red se basa en un enfoque mixto que combina tanto el análisis bibliográfico como exploratorio. En el enfoque bibliográfico se busca recopilar, organizar, evaluar, juzgar e informar los

datos obtenidos en investigaciones científicas que permitan dar soluciones a los problemas relacionados con seguridad de redes; mientras que el método exploratorio indaga la producción académica, este enfoque permitirá obtener una visión integral de la seguridad de la red, evaluando tanto las condiciones técnicas de la infraestructura como las percepciones, experiencias de los usuarios y el equipo de TI involucrado. La combinación de datos, es decir, el análisis de vulnerabilidades y métricas de rendimiento con información (bibliográfica y observaciones) proporcionará una comprensión completa y detallada del estado de seguridad actual y de los efectos de la implementación de los controles.

Enfoque de investigación

Se emplearán herramientas de análisis automatizado, como escáneres de vulnerabilidades y sistemas de monitoreo, para recopilar datos objetivos sobre el estado de la infraestructura de red. Estos datos incluirán métricas como el número de vulnerabilidades detectadas, la frecuencia de actualizaciones de seguridad, los intentos de acceso no autorizado y la efectividad de las configuraciones de seguridad aplicadas. El análisis estadístico de estos datos permitirá identificar patrones y áreas de mayor riesgo en la red.

La decisión de adoptar una implementación basada en los controles CIS se basa en varios factores importantes. En primer lugar, constituyen un marco estandarizado y reconocido globalmente, lo que simplifica la incorporación de buenas prácticas en materia de ciberseguridad. Además, están orientados a abordar amenazas comunes y críticas, lo que fortalece la capacidad de la organización para gestionar riesgos. Su flexibilidad permite que se adapten a diversas infraestructuras, beneficiando a organizaciones de diferentes tamaños y sectores. También fomentan un enfoque de mejora continua, lo que posibilita ajustar las medidas de seguridad a medida que evolucionan las amenazas. Por último, varios marcos regulatorios exigen prácticas de seguridad que son similares a las sugeridas por los controles CIS, lo que facilita el cumplimiento normativo. Es por todas estas razones, su implementación es una opción efectiva para mejorar la seguridad de la infraestructura de red.

2.4. Metodología de Desarrollo

Fase de diagnóstico y evaluación inicial

Para iniciar la implementación, se realizará un inventario exhaustivo de todos los activos conectados a la red, tanto de hardware como de software. Este proceso incluirá servidores, estaciones de trabajo, dispositivos móviles, *routers* y cualquier equipo que esté en uso dentro de la infraestructura de TI. La recopilación de esta información se llevará a cabo mediante herramientas de escaneo de red y entrevistas con los responsables del área de TI, los cuales proporcionarán detalles específicos sobre los dispositivos y programas autorizados en la red. Asimismo, se mapeará la topología completa de la red, identificando los flujos de datos críticos y los puntos de conexión entre sistemas, lo que permitirá detectar vulnerabilidades potenciales, como puertos abiertos o servicios innecesarios.

En paralelo, se procederá a una evaluación de las políticas y procedimientos de seguridad vigentes. Esta revisión implicará verificar si la organización cuenta con medidas claras para la protección de la red, como protocolos de acceso, autenticación multifactorial y respuesta ante incidentes. También se analizarán los procedimientos operativos estándar para garantizar que estén alineados con las mejores prácticas del sector, y se identificarán áreas donde puedan existir lagunas o debilidades que podrían ser aprovechadas por atacantes. En esta etapa, es fundamental establecer una línea base sobre el nivel actual de seguridad.

Una vez completadas estas evaluaciones, se procederá al análisis de vulnerabilidades. Esta fase implicará el uso de herramientas automáticas de escaneo de vulnerabilidades para identificar posibles riesgos en los sistemas y redes, tales como configuraciones incorrectas, software desactualizado o puntos de acceso vulnerables. Adicionalmente, se realizarán pruebas manuales para complementar los análisis automáticos y confirmar los hallazgos. Todo este proceso permitirá tener una visión clara del estado de seguridad actual de la infraestructura y servirá como base para la planificación de los controles a implementar (Vasco, 2024).

Fase de planificación de la implementación

Con los resultados del diagnóstico, el siguiente paso será priorizar los controles de seguridad que se implementarán según las vulnerabilidades detectadas. En esta fase, los controles CIS más esenciales, como el inventario de activos, gestión de vulnerabilidades y configuración segura de hardware y software; serán los primeros en ser considerados. Esta priorización se basará en los riesgos de seguridad más críticos que enfrentan los sistemas de la organización, garantizando que las primeras medidas aborden los problemas más urgentes.

Seguidamente, se establecerán objetivos claros para la implementación de los controles CIS, que incluirán metas específicas, como la creación de inventarios completos de hardware en un plazo de 30 días o la aplicación de parches de seguridad en sistemas vulnerables en un plazo de 60 días. Estos objetivos se valorarán mediante indicadores clave de rendimiento (KPIs), como la reducción del número de vulnerabilidades críticas o el tiempo de respuesta ante incidentes. La definición de estos KPIs será esencial para medir el éxito de la implementación.

Para asegurar una implementación efectiva, se diseñará una estrategia de despliegue que defina los roles y responsabilidades de cada miembro del equipo. Se establecerá un cronograma detallado con fechas clave para la ejecución de cada control, asegurando que todos los pasos se realicen de manera coordinada y según los plazos establecidos. La planificación incluirá la asignación de recursos y la identificación de las herramientas necesarias para llevar a cabo las tareas de manera eficiente (Cyberzaintza, 2024).

Fase de implementación de los controles CIS

En esta fase, se procederá a la implementación de los controles CIS priorizados. El primer paso será la ejecución de los controles básicos, como el inventario de dispositivos autorizados y no autorizados (CIS 1), el inventario de software (CIS 2) y la gestión continua de vulnerabilidades (CIS 3). Para ello, se utilizarán

herramientas automatizadas que faciliten el monitoreo y control de estos activos, asegurando que cualquier anomalía sea detectada y corregida rápidamente.

Se implementarán medidas para controlar el uso de privilegios administrativos (CIS 4), estableciendo restricciones claras sobre quién puede acceder a funciones críticas del sistema. Además, se asegurará que todos los dispositivos de hardware y software estén configurados de manera segura (CIS 5), lo que incluirá la actualización de configuraciones en servidores, estaciones de trabajo y dispositivos móviles, siguiendo las recomendaciones de seguridad más actuales.

A continuación, se procederá con la implementación de controles funcionales, como la protección de correo electrónico y navegadores web (CIS 7), la defensa contra malware (CIS 8) y la configuración segura de equipos de red (CIS 11). Estas medidas garantizarán que los usuarios finales y la infraestructura de red estén protegidos contra amenazas comunes, como el phishing o el malware, y que los puntos críticos de la red, como *routers* y *firewalls*, tengan configuraciones adecuadas para evitar intrusiones.

Finalmente, se aplicarán los controles organizacionales, que incluyen la implementación de programas de capacitación y concienciación en seguridad (CIS 17), y la preparación para la respuesta a incidentes mediante la mejora de los procesos de gestión de incidentes y pruebas de penetración (CIS 19 y CIS 20). La capacitación del personal será clave para garantizar que todos los empleados entiendan los riesgos de seguridad y sepan cómo actuar en caso de un incidente. (Cyberzaintza, 2024)

Fase supervisión y mejora continua

La etapa de Monitoreo y Mejora Continua es crucial para la efectividad de los controles CIS en una infraestructura de red. Primero, es fundamental establecer métricas clave e indicadores de rendimiento (KPIs) que permitan evaluar la efectividad de los controles de seguridad, como la frecuencia de incidentes, el

tiempo de respuesta y la cantidad de vulnerabilidades detectadas y resueltas. (Salcedo, 2023)

Luego, se debe implementar un monitoreo proactivo utilizando herramientas que ayuden a identificar actividades sospechosas y posibles brechas de seguridad, como sistemas de detección de intrusiones y la supervisión de registros.

Se deben realizar auditorías tanto internas como externas de manera regular para verificar el cumplimiento de los controles CIS, utilizando técnicas como pruebas de penetración y análisis de vulnerabilidades. Para salvaguardar la red, es necesario implementar soluciones de supervisión continua, como sistemas de detección de intrusiones (IDS) y herramientas de gestión de eventos de seguridad (SIEM), que ayuden a identificar comportamientos anómalos en tiempo real.

Adicionalmente, es fundamental contar con un plan de gestión de incidentes que especifique los procedimientos a seguir ante cualquier incidente de seguridad, abarcando desde la identificación hasta la recuperación. Este plan debe incluir la documentación de cada incidente para facilitar el análisis posterior y el aprendizaje. Asimismo, es importante revisar y actualizar periódicamente las políticas y procedimientos de seguridad para que se adapten a los cambios tecnológicos y a las nuevas amenazas que puedan surgir.

La formación y sensibilización del personal son aspectos esenciales; se deben llevar a cabo capacitaciones regulares para asegurar que todos comprendan las mejores prácticas de seguridad y sus roles en la protección de la infraestructura. Fomentar un entorno donde el personal pueda ofrecer comentarios sobre los controles y procesos permitirá realizar ajustes y mejorar continuamente la estrategia de seguridad. Por último, es vital mantener una documentación detallada de las configuraciones, cambios efectuados y resultados de las auditorías, lo que no solo contribuye al cumplimiento normativo, sino que también facilita la toma de decisiones informadas en el futuro. Este enfoque integral refuerza la seguridad de la infraestructura y permite a la organización adaptarse a un panorama de amenazas que está en constante evolución. (Secureframe, 2024)

CAPÍTULO III. ANÁLISIS DE LOS RESULTADOS DE INVESTIGACIÓN

3.1. Validación CIS

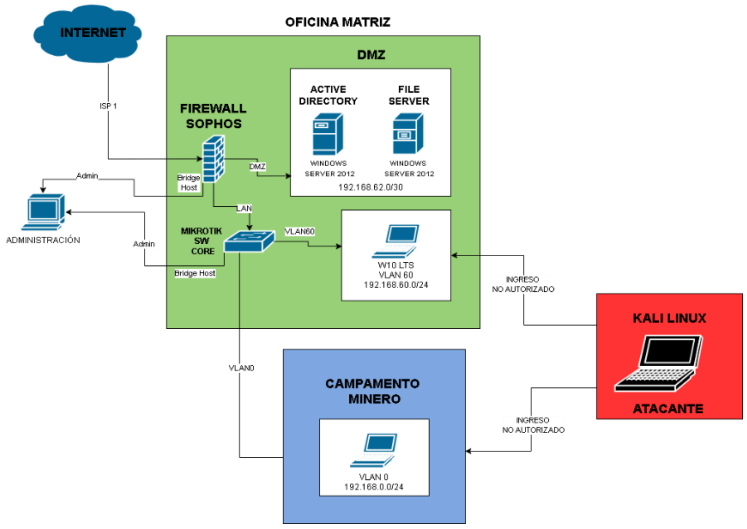
Para validar la implementación del CIS, se desarrolla una simulación tomando la parte del entorno de producción de la empresa Minervilla.

Configuración de entorno simulado

Diagrama de esquema de simulación

En el diagrama de esquema de simulación de la figura 19 se observa que el Firewall Sophos se encuentra conectado al DMZ (Zona desmilitarizada – red perimetral que protege una red de área local LAN de tráfico no confiable), donde se encuentran los directorios activos y los archivos del servidor. Y el firewall a su vez a la administración que está conectado a un bridge host. Pudiendo observar al atacante; además, en la tabla 16 se encuentran las características de Host Anfitrión en la cual se crearán las máquinas de entorno simulado.

Figura 19. Diagrama de esquema de simulación



Fuente: elaboración propia

Tabla 16. Características de Host Anfitrión donde se crearán todas las máquinas virtuales del entorno simulado

Procesador: Intel Core I5 8265U 1,6 – 1,8 GHz. Memoria RAM: 8GB Disco Duro: HDD 512 GB Sistema Operativo: Windows 10

Fuente: elaboración propia

Configuración del entorno de simulación

Firewall Sophos

Para iniciar con la configuración del entorno de simulación se debe configurar el Firewall Sophos, para lo cual se obtiene el mismo mediante el link: https://www.sophos.com/es-es/support/downloads/firewall-installers

Nota: Al ser una versión de prueba solo durara 1 mes fecha de inicio 3 de diciembre.

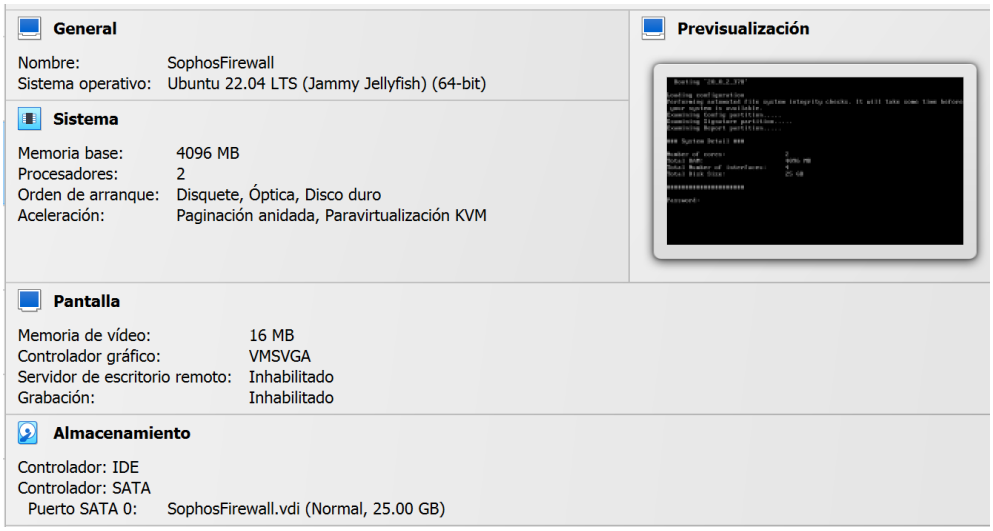
La configuración se realiza a 4 adaptadores de red:

- **Adaptador Bridge:** Permite la configuración con el equipo anfitrión.
- **Adaptador Bridge:** Es el cual se usa para simular el ISP (proveedor de internet).
- **Red Interna (DMZ):** Con IP 192.168.62.0/30 red configurada para dar servicio de internet a los servidores de la red el *File Server y el Active Directory*.
- **Red Interna (LAN):** Con IP 192.168.100.0/24 red configurada para dar salida de internet a toda la red interna de la empresa, brindando servicio de internet al *SW Core (Mikrotik*).

El requisito para firewall es de 4 GB de RAM y 25GB de almacenamiento.

En la figura 20 se desarrolla la configuración del firewall Sophos en el sistema operativo Ubuntu de 64 bits, con una memoria base de 4096 MB, con 2 procesadores, memoria de video de 16 MB y un controlador gráfico VMSVGA.

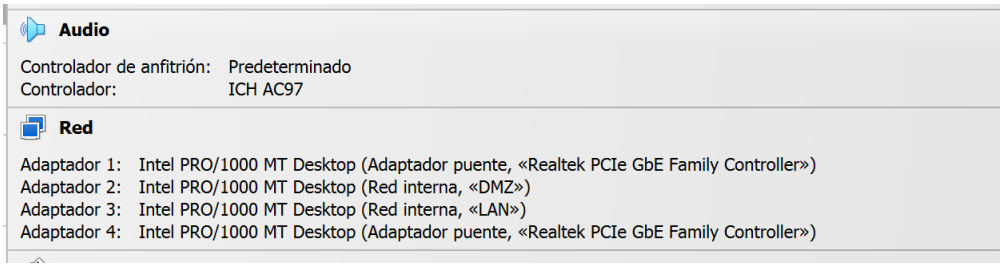
Figura 20. Configuración *Firewall Sophos*



Fuente: elaboración propia

En la figura 21 se desarrolla la configuración del firewall Sophos donde se observa el controlador del anfitrión como determinado, el controlador ICH AC97 y los adaptadores de cada red que se encuentran conectados.

Figura 21. Configuración *Firewall Sophos*



Fuente: elaboración propia

DMZ Servidores

Link para descargar imagen ISO de Windows server 2012 R2

https://www.microsoft.com/es-es/evalcenter/download-windows-server-2012-r2

Se utilizará la misma imagen ISO para los 2 servidores uno para el File Server, y otro para el *Active Directory*.

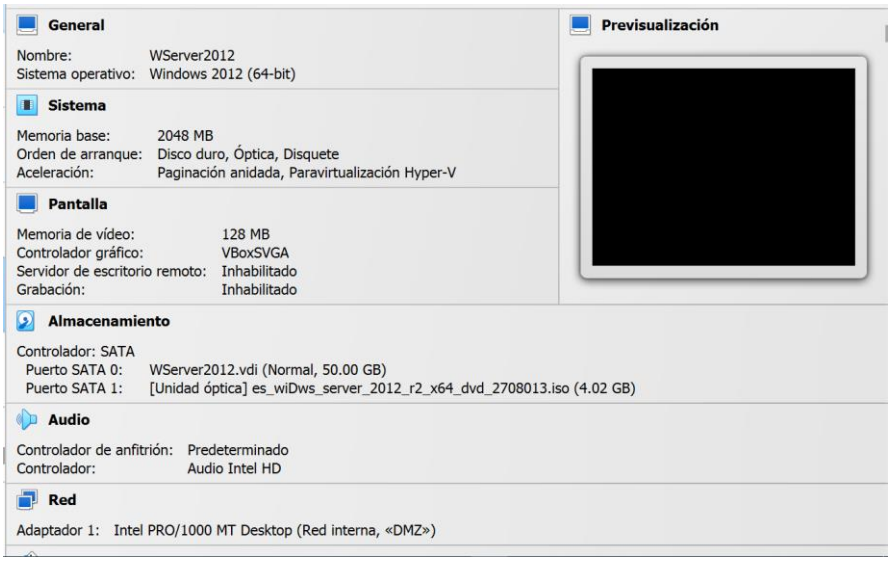
Nota: Imagen ISO de prueba, tendrá una duración de 1 mes.

Los requisitos de sistema utilizados son de 2 GB de Memoria RAM, 50 GB de Disco Duro y 1 adaptador de Red Interna (DMZ) configurada para dar acceso a internet desde el *firewall*.

Active Directory

En la figura 22 se observa la configuración de *Active Directory* en el sistema operativo Windows de 64 bits, con una memoria base de 2048 MB, memoria de video de 128 MB y un controlador gráfico VBoxSVGA, así como que controladores SATA se encuentran activados.

Figura 22. *Active Directory*



Fuente: elaboración propia

File Server

En la figura 23 se configura File Server en el sistema operativo Windows de 64 bits, con una memoria base de 2048 MB, memoria de video de 128 MB y un controlador gráfico VBoxSVGA, así como que controladores SATA se encuentran activados. Se observa en la previsualización WServer2012 *FileServer* se encuentra activado.

Figura 23. *File Server*

Fuente: elaboración propia

Configuración del SW CORE

A través del Link https://mikrotik.com/download de ISO se emular SW CORE.

Se descarga el sistema operativo de RouterOS, Mikrotik para emular el Switch Core Administrable, además se configura 4 adaptadores de red:

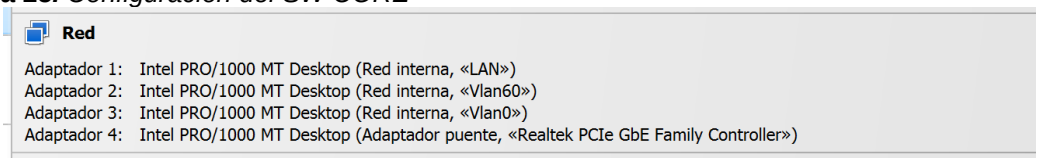
- **Red Interna (LAN):** Llega el internet desde el firewall de Sophos.
- **Red Interna (Vlan 60):** Servirá para dar internet al segmento de red 192.168.60.0/24, la misma que pertenece a la parte administrativa.
- **Red Interna (Vlan 0):** Simula el segmento de red del Campamento minero Minervilla, para la red 192.168.0.0/24.
- **Adaptador Bridge:** Permite configurar el Switch.

Los requisitos del sistema deben ser 512 memoria RAM y 5 GB de almacenamiento. Tal como se observa en la figura 24 y 25.

Figura 24. Configuración del SW CORE

Fuente: elaboración propia

Figura 25. *Configuración del SW CORE*

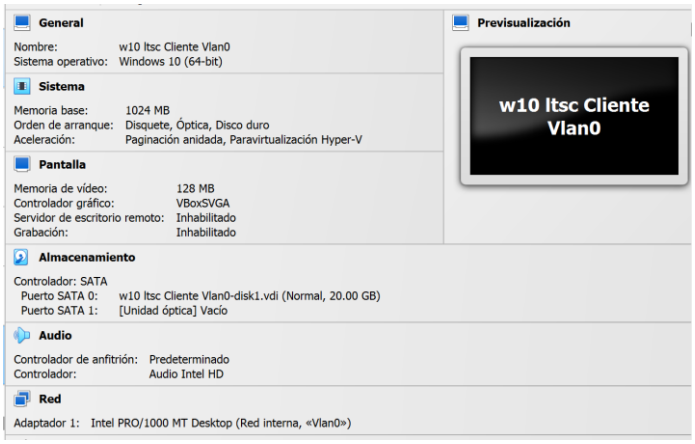


Fuente: elaboración propia

Equipos conectados Vlan 60 y Vlan 0

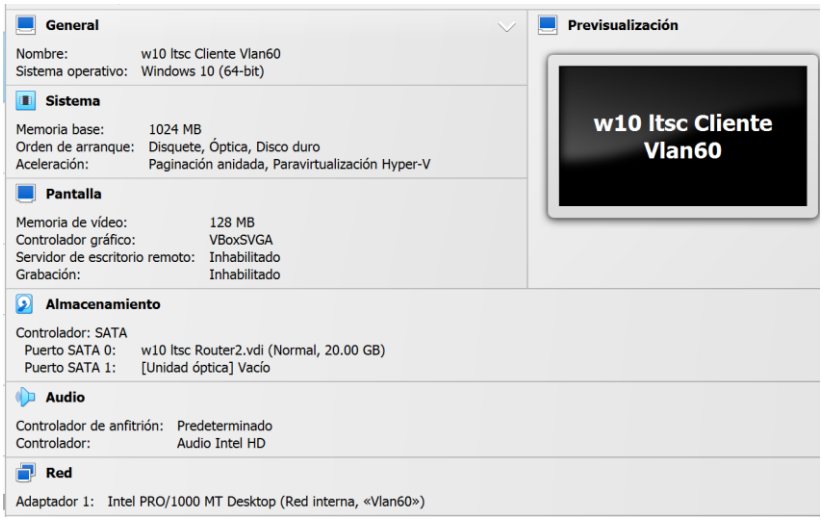
Para conectar equipos Vlan 60 y Vlan 10 se utiliza un w10 LTS para los equipos conectados a estos segmentos de red, con requisitos de sistema de 1GB de memoria RAM y 20 GB de almacenamiento. El Cliente Vlan 0 con IP 192.168.0.0/24 se muestra en la figura 26 y el cliente Vlan 60 con IP 192.168.60.0/24 se muestra en la figura 27.

Figura 26. Cliente Vlan 0



Fuente: elaboración propia

Figura 27. Cliente Vlan 60



Fuente: elaboración propia

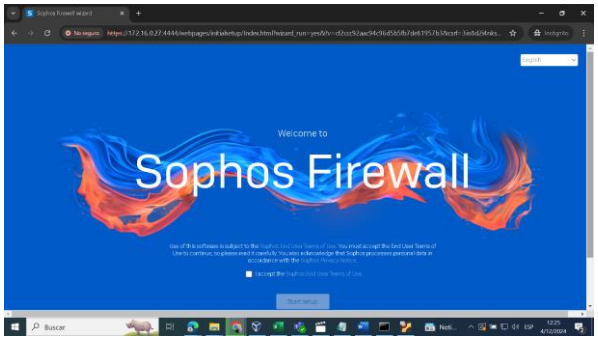
Ambos equipos tendrán una red interna configurada respectivamente para el segmento de red correspondiente, con su respectiva IP que es asignado automáticamente por el *SW Core Mikrotik* configurado.

Configuración y credenciales de acceso al *firewall SOPHOS*

En las figuras 28 y 29 se muestra la interface de Firewall Sophos, en la figura 29 en la interface se observa que se debe introducir el nombre de usuario y contraseña para poder ingresar al mismo. Teniendo las siguientes autenticaciones:

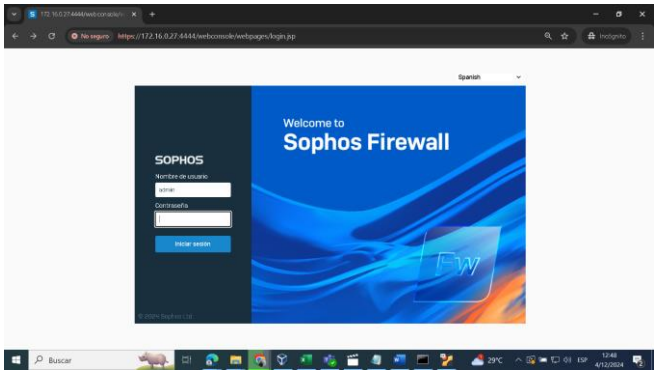
IP de acceso: 172.16.0.27:4444 (acceder por http)
Username: admin
Password: 1!2”3#4$5%caBS

Figura 28. Interface *Firewall Sophos*



Fuente: elaboración propia

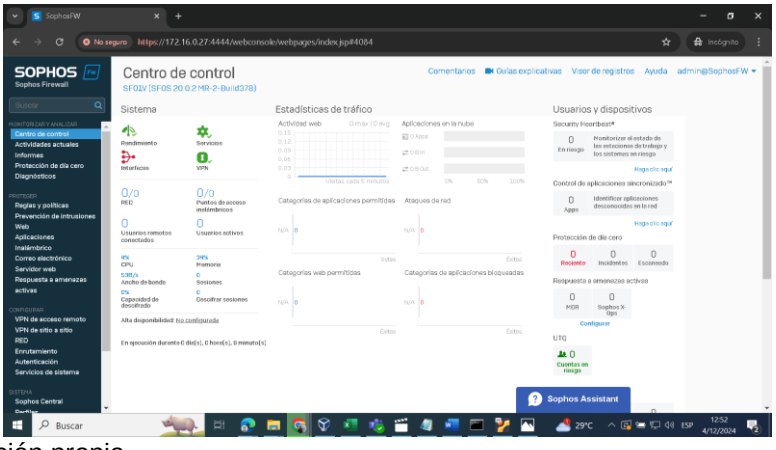
Figura 29. Interface de acceso a Firewall Sophos



Fuente: elaboración propia

En la figura 30 en el portal de administración de Firewall Sophos, se tiene el centro de control, actividades actuales, informes, diagnósticos. Además, se puede configurar las VPN de acceso remoto, las VPN de sitio a sitio, así como la RED.

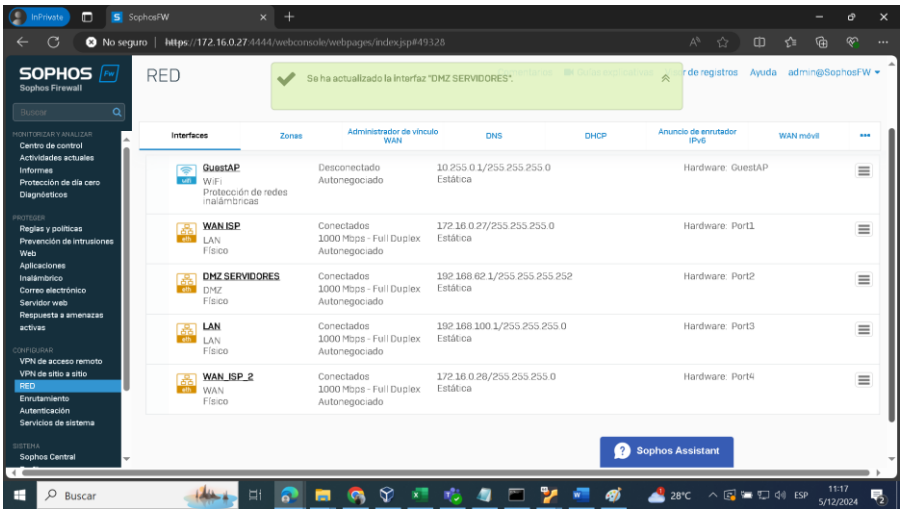
Figura 30. Portal de administración de *Sophos firewall*



Fuente: elaboración propia

En la figura 31 se configura los 4 adaptadores de red WAN ISP, DMZ SERVIDORES, LAN, WAN_ISP_2. Enrutados al Port 1, Port 2, Port 3 y Port 4 respectivamente.

Figura 31. Configuración de 4 adaptadores de red



Fuente: elaboración propia

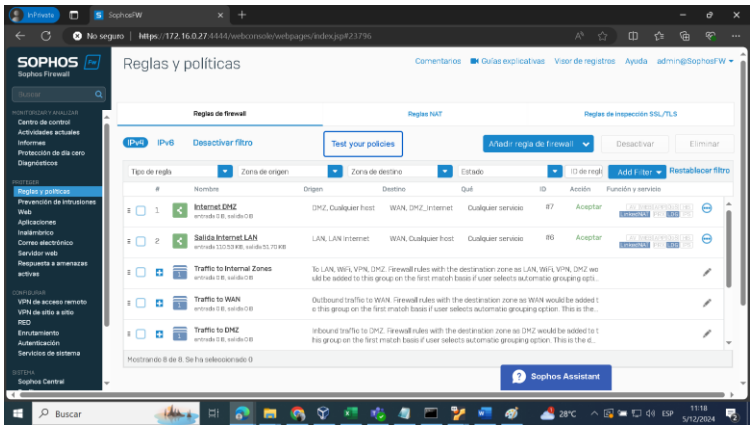
Donde:

WAN IPS, sirve para configurar el firewall desde el host anfitrión
WAN ISP 2 permite dar acceso a internet al firewall.
DMZ, red para dar internet a los servidores de la red.
LAN, permitirá dar acceso a inter al Switch Core Administrable de la oficina Matriz.

Configuración de reglas y políticas de navegación

La configuración de reglas y políticas de navegación permite dar salida a internet a la LAN y DMZ configurando las reglas y políticas de navegación como se muestra en la figura 32.

Figura 32. Configuración de reglas y políticas de navegación

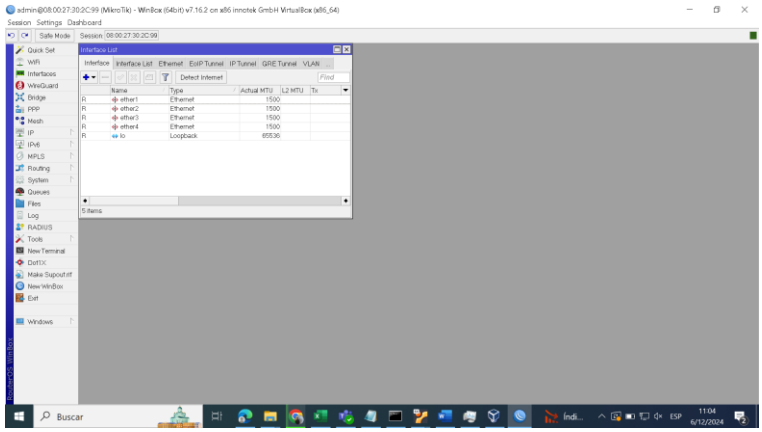


Fuente: elaboración propia

Configuración del switch Core Mikrotik

En la configuración del *Switch Core Mikrotik* se realiza la configuración de 4 adaptadores de red de tipo Ethernet con MTU de 1500. Como se observa en la figura 33.

Figura 33. Configuración de adaptadores de red

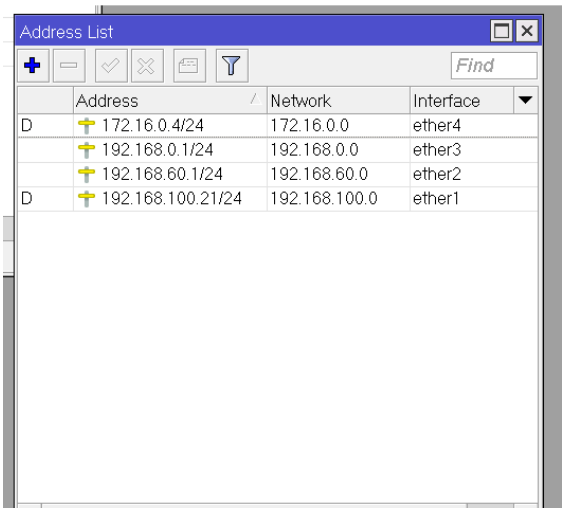


Fuente: elaboración propia

Se concede Dirección IP a cada una de las interfaces de red para mejor configuración.

Ethernet4: 172.16.0.4 permite la conexión con el equipo host anfitrión para la configuración del switch por medio de Winbox. Se muestra en la figura 34 las direcciones IP de cada una de las interfaces de red.

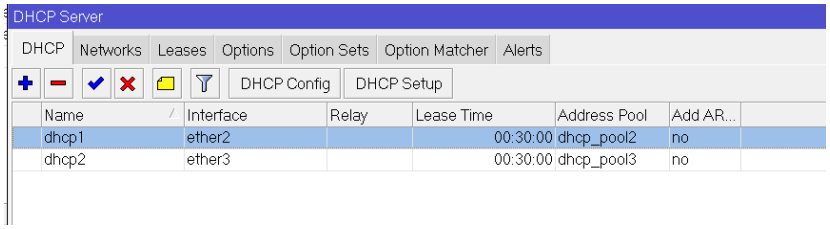
Figura 34. Direcciones IP de cada una de las interfaces de red



Fuente: elaboración propia

En la figura 35 se configura el servidor DHCP para las dos Vlans (60 y 0), teniendo un *lease time* de 00:30:00, la Interface ether2 con *Address Pool* de dhcp_pool2 y la *Interface* ether3 con *Address Pool* de dhcp_pool3.

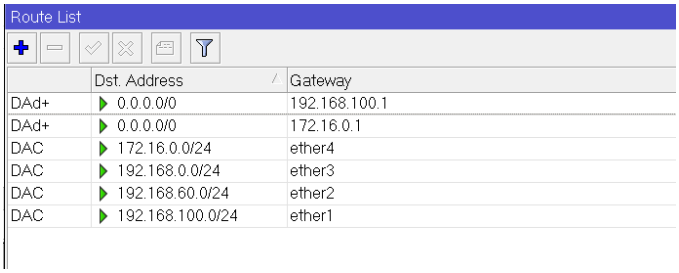
Figura 35. Configuración de servidor DHCP para la VLAN60 y VLAN0



Fuente: elaboración propia

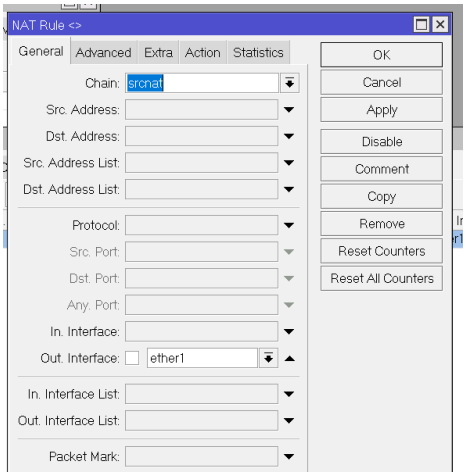
En las figuras 36, 37 y 38 se configura la salida a la red mediante la ethernet 1 donde llega el servicio de internet desde firewall Sophos

Figura 36. Configuración de salida a la red



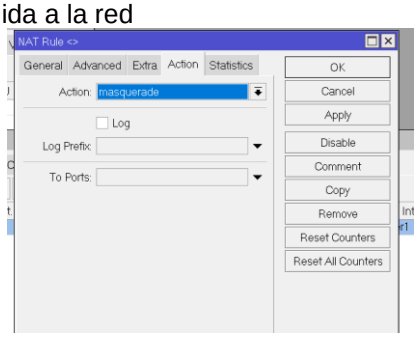
Fuente: elaboración propia

Figura 37. Configuración de salida a la red



Fuente: elaboración propia

Figura 38. Configuración de salida a la red



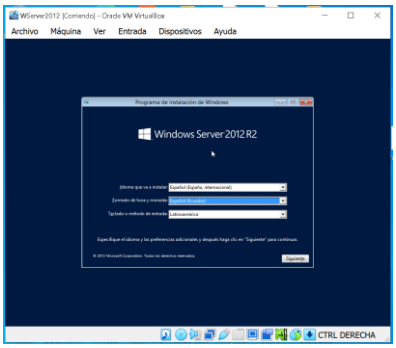
Fuente: elaboración propia

Configuración de *Windows Server* 2012 R2

Windows Server 2012 R2 es una plataforma de Microsoft utilizada para construir centros de datos, nubes empresariales, infraestructura de servicios web, redes y aplicaciones que permite la clasificación automatizada, soporte integrado, máquinas virtuales, de duplicación de datos para VHD.

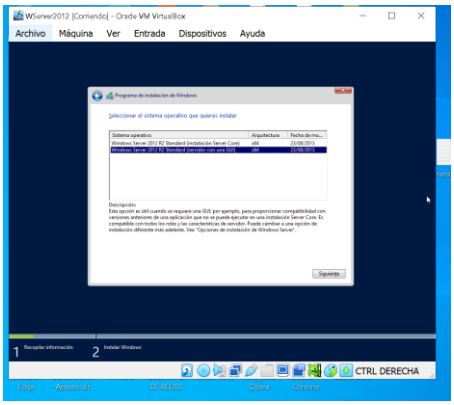
Se realiza la configuración de Windows Server 2012 R2 en VM VirtualBox, se coloca el idioma que se va a instalar, formato de hora, método de entrada; luego se escoge el sistema operativo requerido; se acepta los términos y condiciones de licencia del software, se espera que la instalación concluya; ¡finalmente se coloca las autenticaciones donde el Nombre de Usuario es Administrador y la contraseña es 1!2”3#4$5%caBS. Tal como se muestran en las figuras 39, 40, 41, 42, 43 y 44; siendo la última donde se observa Windows Server corriendo de manera correcta.

Figura 39. Instalación de *Windows Server* 2012R2



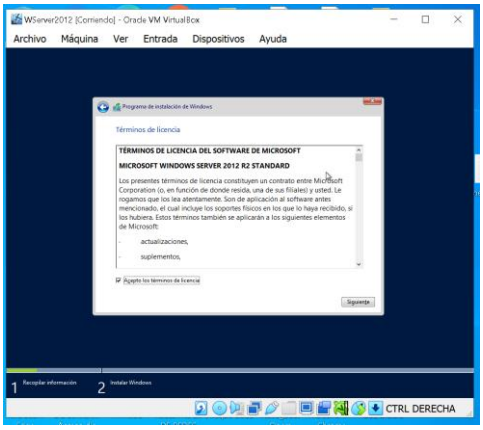
Fuente: elaboración propia

Figura 40. Instalación de Windows Server 2012R2



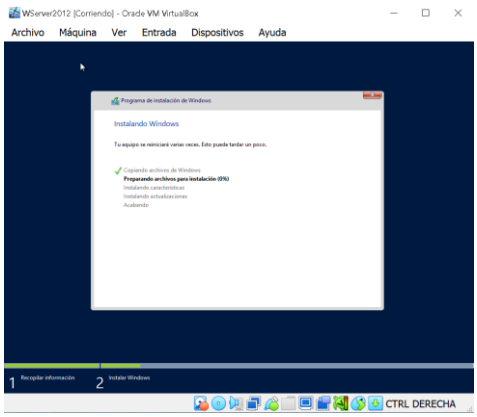
Fuente: elaboración propia

Figura 41. Instalación de Windows Server 2012R2 – Aceptación de términos y condiciones



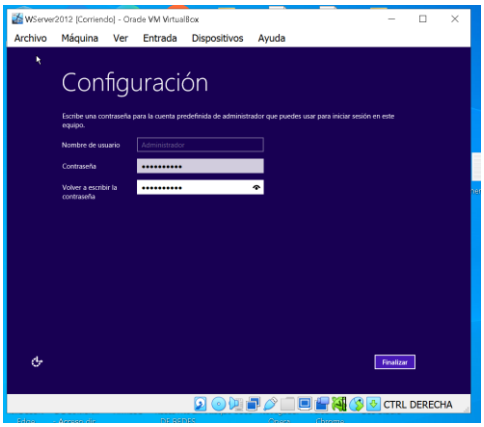
Fuente: elaboración propia

Figura 42. Instalación de Windows Server 2012R2 – Proceso de instalación



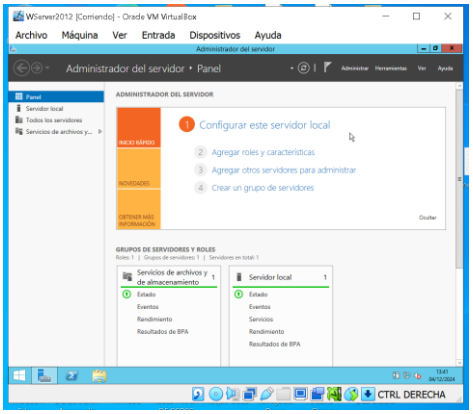
Fuente: elaboración propia

Figura 43. Configuración de autenticadores en Windows Server 2012R2



Fuente: elaboración propia

Figura 44. Windows Server 2012R2 corriendo – Panel del administrador del servidor

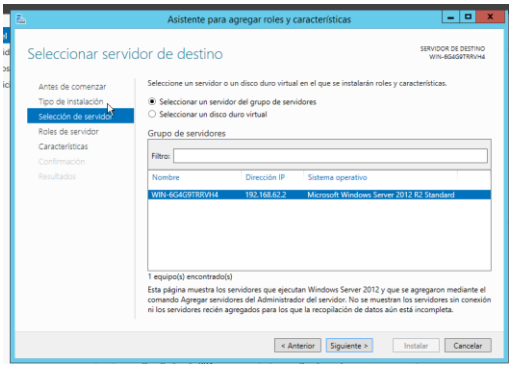


Fuente: elaboración propia

Agregar características y roles

En la figura 45 se realiza la configuración de selección de servidor de destino el cual se toma un servidor del grupo de servidores: WIN-6G4G9TRRVH4 con dirección IP 192.168.62.2 de Sistema Operativo Microsoft *Windows Server 2012 R2 Standard*.

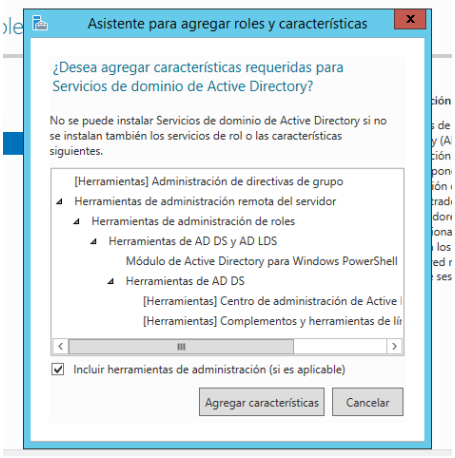
Figura 45. Selección de servidor de destino



Fuente: elaboración propia

En la figura 46 se configura las características que requiere para Servicios de Dominio de *Active Directory*; si este no se activa o se instalan no podrá funcionar correctamente, por lo cual se agregan las características de: herramientas de administración remota del servidor, herramientas de administración de roles, herramientas de AD DS y AD LDS, módulo de *Active Directory* para *Windows PowerShell*, herramientas de AD DS.

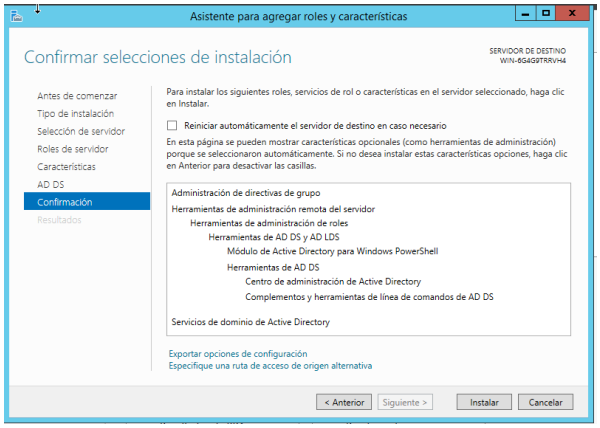
Figura 46. Características requeridas para Servicios de dominio de *Active Directory*



Fuente: elaboración propia

En la figura 47 se confirma los roles, servicios de rol o características en el servidor seleccionado, por lo cual se hace clic en instalar.

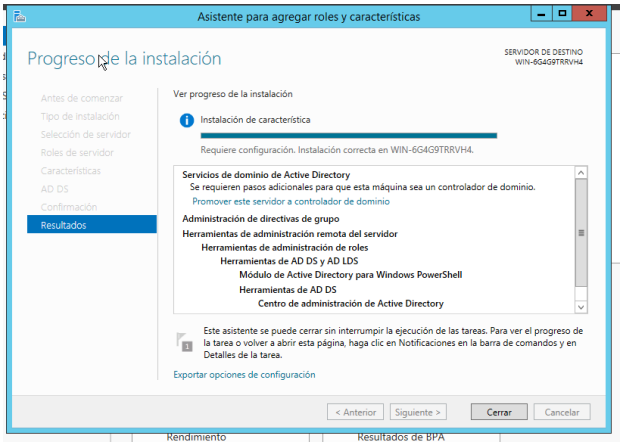
Figura 47. Confirmación de selecciones de instalación



Fuente: elaboración propia

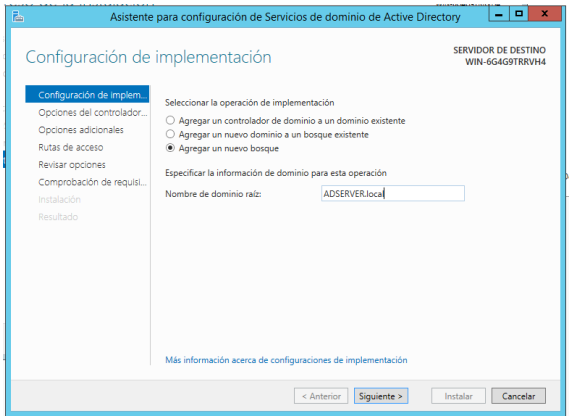
En el progreso de instalación se da la configuración de implementación, opciones de controlador de dominio en donde se escribe la contraseña de modo de restauración de servicios de directorio (DSRM) la cual es 1!2”3#4$5%caBS, posterior de desarrolla las rutas de acceso y finalmente se crea el nuevo objeto: Usuario ADSERVER.local/Users con nombre de pila Cliente01_vlan60, Iniciales C01V60, apellidos Vlan60-cliente01, nombre completo Vlan60-cliente01. Todo esto se puede observar en las figuras 48, 49, 50, 51 y 52.

Figura 48. Progreso de instalación



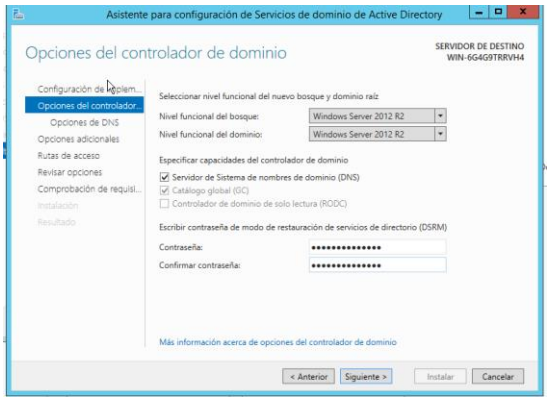
Fuente: elaboración propia

Figura 49. Configuración de implementación



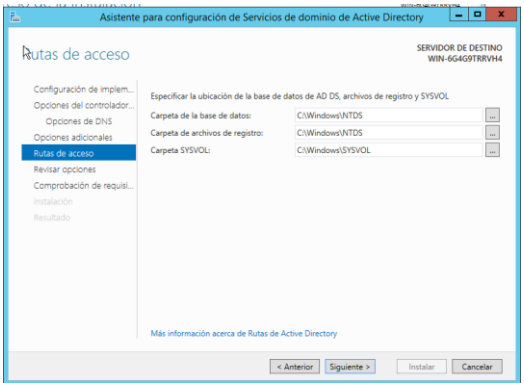
Fuente: elaboración propia

Figura 50. Opciones del controlador de dominio



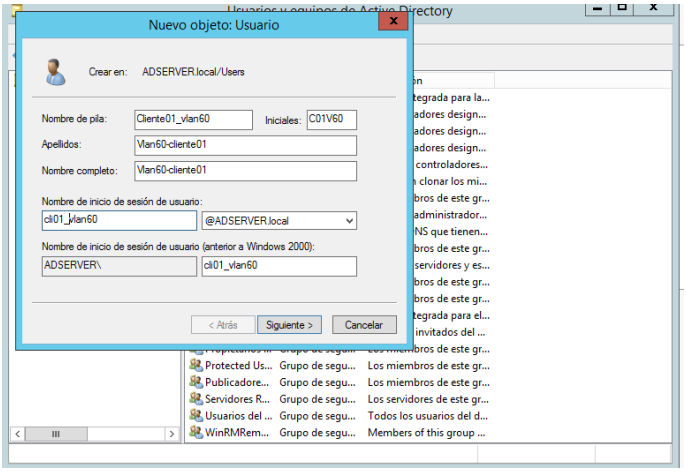
Fuente: elaboración propia

Figura 51. Rutas de acceso



Fuente: elaboración propia

Figura 52. Nuevo Objeto: Usuario



Fuente: elaboración propia

3.2. Ataque desde dentro de la LAN

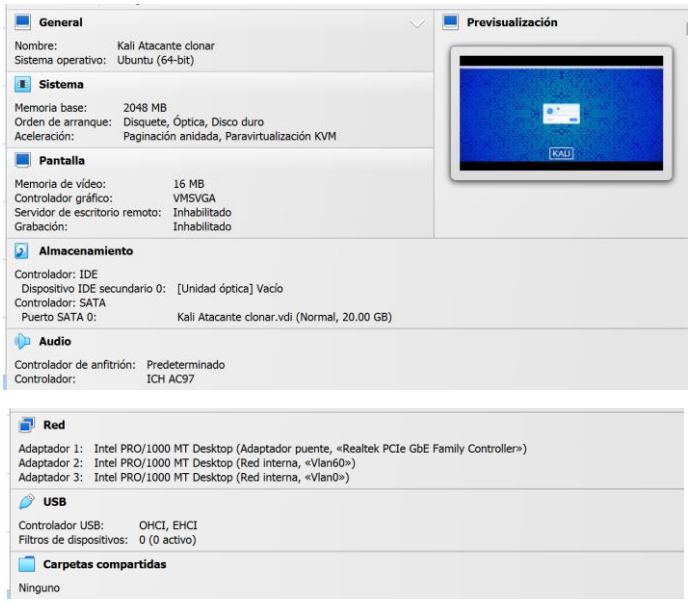
Configuración del atacante

Se realizar el ataque al cliente en la vlan60 de la oficina matriz, asumiendo que el atacante tuvo acceso ya sea por medio de algún empleado que le facilito el ingreso o por algún medio de filtración de información.

Se configura el nombre del atacante Kali Atacante Clonar dentro del sistema operativo Ubuntu (64 bits) con memoria base en su sistema de 2048 MB, aceleración Paginación anidada, Para virtualización KVM, en su pantalla una memoria de video de 16 MB, controlador gráfico VMSVGA, puerto SATA 0 de nombre Kali Atacante clonar. Vdi de 20GB Normal, conectado a la red del adaptador

1 Intel PRO/1000 MT Desktop (Adaptador puente, “*Realtek PCIe GbE Family Controller*”); adaptador 2 Intel PRO/1000 MT Desktop (Red Interna “Vlan60”) y adaptador 3 Intel PRO/1000 MT Desktop (Red Interna “Vlan0”) como se observa en la figura 53.

Figura 53. Configuración del atacante



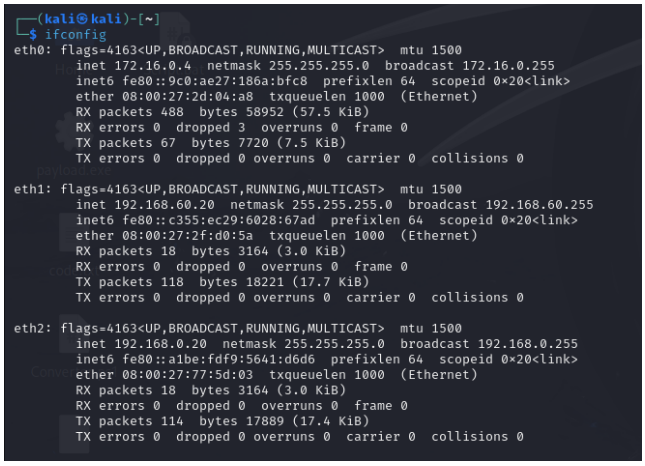
Fuente: elaboración propia

Ataque desde dentro de la LAN a Vlan60

Para realizar el ataque lo primero es verificar que se tenga el acceso a la red y se haya asignado un IP del servidor DHCP.

Con el comando “ifconfig” dentro del panel de control de Kali, se observa que se ha asignado la IP 192.168.60.20, para la red Vlan60, Figura 54.

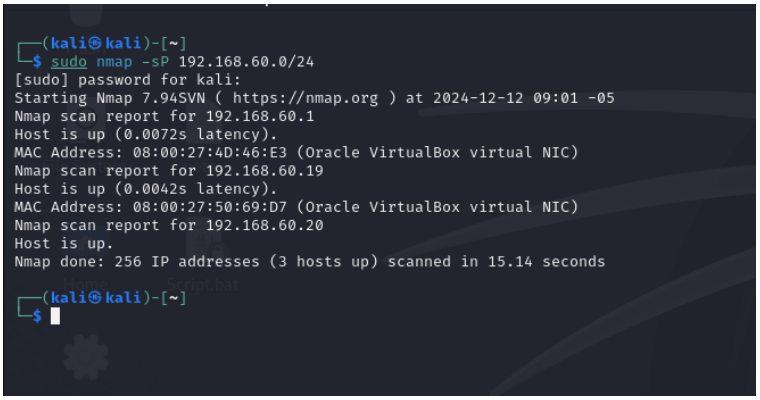
Figura 54. Asignación de IP



Fuente: elaboración propia

Posterior se procede a analizar la red e iniciar con los respectivos ataques, se escanea la red con el comando “sudo nmap” identificando 3 equipos conectados a la red. Figura 55.

Figura 55. Análisis de red



Fuente: elaboración propia

Detectando las siguientes redes:

192.168.60.1, es el *router*; es decir en este caso es el servidor dhcp.
192.168.60.19, es el cliente de la vlan60 el cual será el objetivo a ser atacado.
Y 192.168.60.20, es el equipo Kali o el atacante.

Ataque – Ataque *Man in the middle* (MitM)

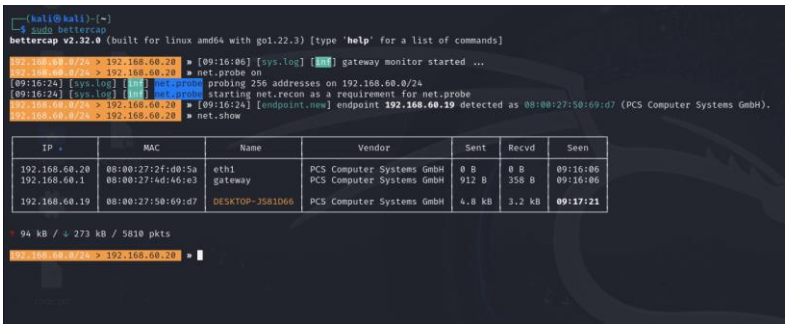
Este ataque permitirá interceptar y potencialmente modificar el tráfico de red, lo cual es ideal para capturar credenciales o analizar el tráfico que pasa entre los dispositivos en la LAN. Para esto re necesita unos prerrequisitos: estar dentro de la red interna.

Dentro de la red interna

Para estar dentro de la red interna primero se analiza los equipos conectados a la red, para este ataque se coloca en medio del cliente y el equipo router para de esta manera capturar todo el tráfico de la red.

El objetivo es atacar a la ip del Router 192.168.60.1. Procediendo con la instalación de la herramienta *bettercap*, con los comandos: "*sudo bettercap*", *net.probe*. Como se muestra en la figura 56.

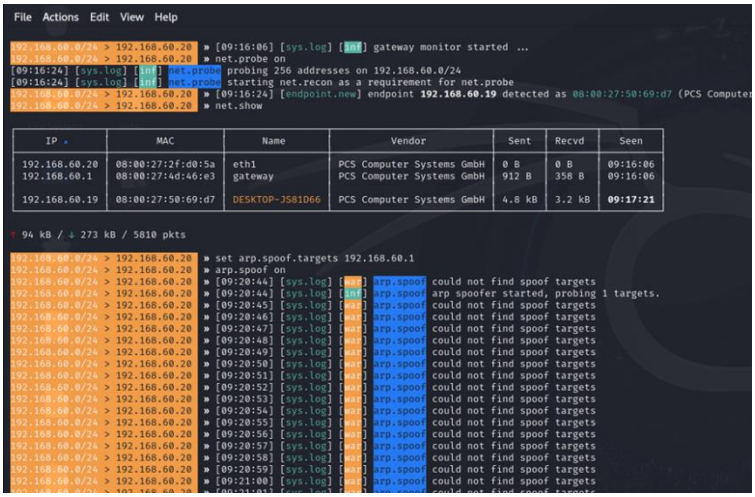
Figura 56. Instalación de la herramienta *bettercap*



Fuente: elaboración propia

Se identifica el Gateway 192.168.60.1, para colocar en medio de la puerta de enlace y del cliente de la vlan60 creando un *arp spoof* a esta IP. Figura 57.

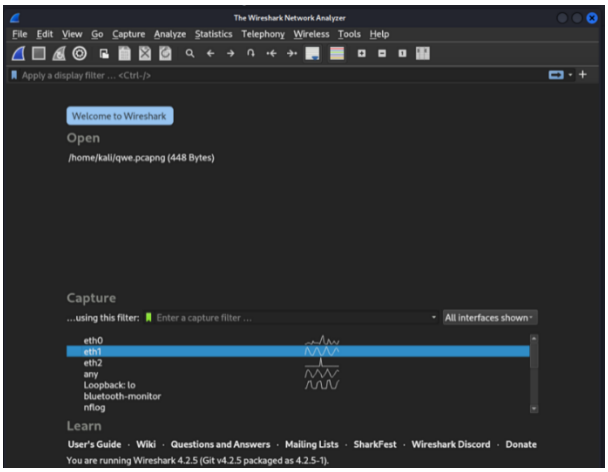
Figura 57. Identificación de *Gateway* – creación de arp spoof



Fuente: elaboración propia

Posterior se debe analizar el tráfico de la red la cual se realiza en el software Wireshark el cual es una herramienta de análisis de redes de código abierto que se usa para capturar y examinar el tráfico de red en tiempo real, permitiendo a los usuarios observar los paquetes de datos que se transmiten a través de una red facilitando la identificación de problemas, análisis de seguridad y la solución de fallos de red. Seleccionando la eth1, la cual es la red de la Vlan60. Como se puede observar en la figura 58.

Figura 58. Análisis de tráfico de datos

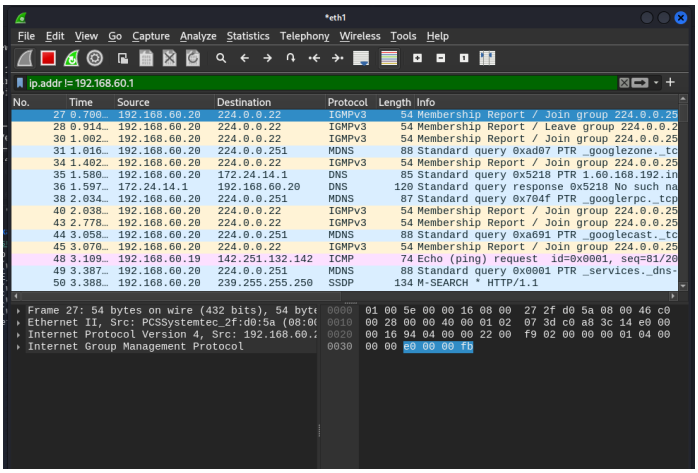


Fuente: elaboración propia

Una vez seleccionada la eth1, se observa todo el tráfico de la red y dispositivos conectados a la 192.168.60.1, de esta manera los atacantes pueden ir escalando niveles, analizando tráfico e identificado servidores o puerto abiertos en la red que

podrían ser víctima de ataque por ello hay se debe tener cuidado con los usuarios que se permite ingresar a la red. Figura 59

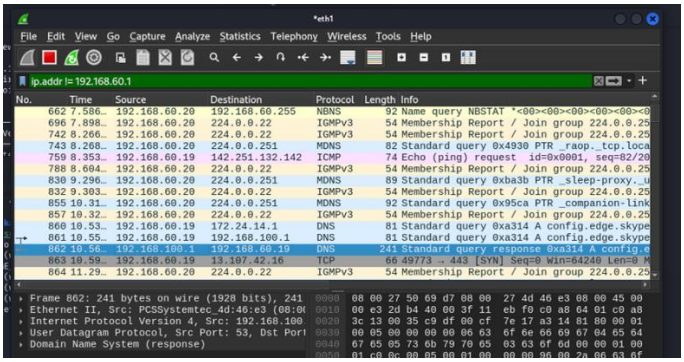
Figura 59. Trafico de la red



Fuente: elaboración propia

En el análisis de tráfico aparece la LAN que provee de internet al *sw core mikrotik*, 192.168.100.1. Con el ataque se suplanta la identidad del router, interceptando todo el tráfico de la red sin que el usuario se dé cuenta. Figura 60.

Figura 60. Revisión de LAN



Fuente: elaboración propia

Ataques a la LAN

Se realiza algunos ataques a la respectiva LAN que provee de internet a las dos subredes la Vlan60 y la Vlan0, por medio del *SW core Mikrotik*.

Ataque 1. *SYN Flood*

Un ataque *SYN Flood* satura una red enviando un número excesivo de solicitudes de conexión TCP, consumiendo recursos en la máquina objetivo. Como se describe en la tabla 17.

Tabla 17. Ataque 1 SYN Flood

Comando: bash Copiar código sudo hping3 -S --flood -p 80 192.168.100.1 **Descripción:** -S: Activa el flag SYN. --flood: Envía paquetes lo más rápido posible. -p 80: Ataca el puerto 80 (se puede cambiar por cualquier otro abierto en el firewall o servidor). **Objetivo:** Generar un alto volumen de solicitudes TCP SYN.

Fuente: elaboración propia

Ataque 2. ICMP *Flood (Ping Flood*)

El ataque ICMP Flood satura el objetivo enviando un gran número de solicitudes ICMP (ping). Tabla 18.

Tabla 18. Ataque 2 ICMP-Flood

Comando: bash Copiar código sudo ping -f -s 65000 192.168.100.1 **Descripción:** -f: Modo flood, envía paquetes ICMP continuamente. -s 65000: Tamaño máximo de paquete ICMP (65,000 bytes). **Objetivo:** Saturar el dispositivo objetivo con tráfico ICMP y observar si Sophos lo detecta como un ICMP Flood.

Fuente: elaboración propia

Ataque 3. *SYN Flood*

Un ataque *SYN Flood* satura una red enviando un número excesivo de solicitudes de conexión TCP, consumiendo recursos en la máquina objetivo. Se detalla en la tabla 19.

Tabla 19. Ataque *SYN Flood*

Comando: bash Copiar código sudo hping3 -S --flood -p 80 192.168.100.1 **Descripción:** -S: Activa el flag SYN. --flood: Envia paquetes lo más rápido posible. -p 80: Ataca el puerto 80 (se puede cambiar por cualquier otro abierto en el firewall o servidor). **Objetivo:** Generar un alto volumen de solicitudes TCP SYN.

Fuente: elaboración propia

Ataques realizados con Kali

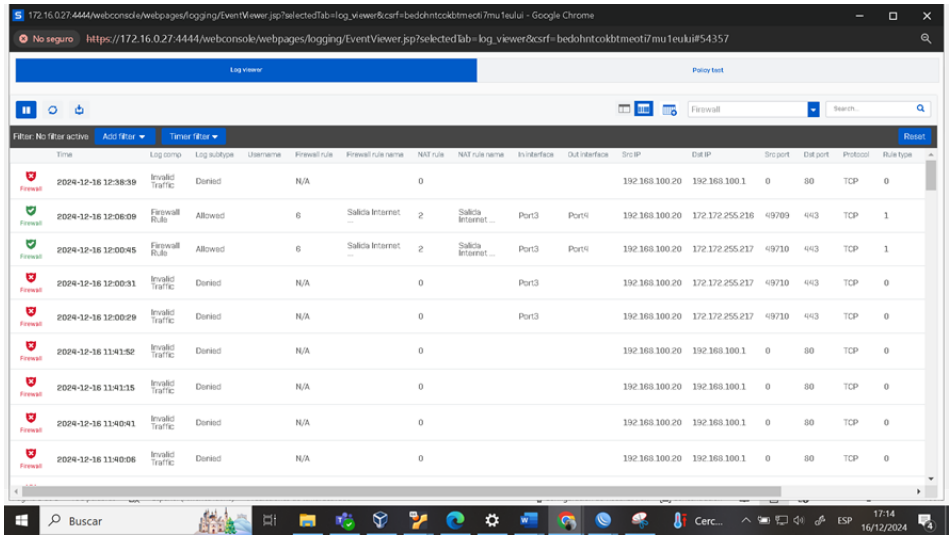
En la figura 61 se puede observar los ataques que se han realizado con Kali

Figura 61. Ataques con Kali

Fuente: elaboración propia

En la figura 62 nuestra como los ataques son registrados y mitigados por el firewall Sophos

Figura 62. Ataques registrados y mitigados



Fuente: elaboración propia

3.3. Resultados de las pruebas realizadas con las herramientas y *software*

En la siguiente tabla se muestra la validación de resultados a raíz de las pruebas de ataques de vulnerabilidad realizadas. Se detalla cada control con el problema relacionado y la solución que se ejerce en el mismo.

Tabla 20. Resultados – Control CIS/Problema relacionado y solución

Control CIS	Problema Relacionado	Solución
CIS Control 1: Inventario y control de activos	Falta de monitoreo	Registro de todos los dispositivos autorizados y no autorizados conectados a la red.
CIS Control 3: Gestión continua de vulnerabilidades	Falta de actualizaciones	Escaneo periódico y parches de software.
CIS Control 4: Control de uso de privilegios administrativos	Gestión deficiente de contraseñas	Privilegios administrativos regulados y controlados.
CIS Control 8: Defensa contra malware	Configuraciones débiles	Firewall implementado y configurado.
CIS Control 9: Limitación y control de puertos, protocolos y servicios	Falta de segmentación de red	Red interna segmentada
CIS Control 17: Implementación de un programa de seguridad	Ausencia de plan de respuesta	Plan de respuesta en desarrollo.

Fuente: elaboración propia

Evaluación de riesgo

Con los controles aplicados en la simulación se reevalúa o se evalúa nuevamente el riesgo de la red institucional, teniendo como resultados los mostrados en la tabla 21.

Tabla 21. Evaluación de riesgos aplicando los controles

Vulnerabilidad	Probabilidad (Alta/Media/Baja)	Impacto (Alta/Media/Baja)	Nivel de Riesgo (Alto/Medio/Bajo)
Configuraciones débiles	Bajo	Medio	Bajo
Falta de actualizaciones	Media	Bajo	Bajo
Carencia de monitoreo	Media	Media	Media
Gestión deficiente de contraseñas	Baja	Media	Baja
Falta de segmentación de red	Media	Baja	Baja
Ausencia de plan de respuesta	Media	Baja	Baja

Fuente: elaboración propia

Se prioriza la importancia de mantener los sistemas, aplicaciones y software actualizados cada cierto tiempo, además se debe tener en cuenta que las configuraciones de seguridad a implementar sean las adecuadas para reducir o minimizar los riesgos potenciales al Grupo Chevez en la estación de Minervilla. Cía. Ltda.

Se detallan los resultados de la evaluación de seguridad de Minervilla, incluyendo los Controles CIS con su respectiva solución. Las herramientas utilizadas en la presente investigación fueron: *Firewall Sophos, DMZ Servidores, Switch Core Mikrotik, Windows Server 2012R2, Wireshark*; permitiendo evaluar la postura de seguridad de la red del Grupo Chevez específicamente de la sección de Minervilla.

3.4. Propuesta de Implementación

En la propuesta de implementación se determina objetivos de alcance: Fortalecer las configuraciones de seguridad en los sistemas críticos; Implementar herramientas para la detección de respuestas a incidentes; Establecer un programa de monitoreo continuo de las medidas de seguridad y finalmente capacitar al personal en buenas prácticas de ciberseguridad y en el uso de nuevas herramientas implementadas.

Alcance del proyecto

La propuesta cubrirá los sistemas y activos críticos de la organización, incluyendo:

- Servidores y estaciones de trabajo.
- Infraestructura de red (routers, switches, firewalls).
- Aplicaciones y bases de datos críticos.

Fases de implementación

En las fases de implementación se tiene: planificación, ejecución, monitoreo y capacitación las cuales se encuentran con sus respectivas actividades y el tiempo de duración, así como los responsables de las mismas. Como de observa en la tabla 22.

Tabla 22. Fases de Implementación

Fase	Actividades	Duración Estimada	Responsables
Planificación	- Reunión inicial para definir objetivos y roles.	2 semanas	Equipo de TI y Seguridad.
	- Identificación de activos y evaluación de riesgos.		
	- Diseño del plan detallado de implementación.		
Ejecución	- Implementación de herramientas de seguridad (antivirus, SIEM, etc.).	6 semanas	Proveedores externos y TI.
	- Configuración de políticas de acceso y segmentación de red.		
	- Instalación de actualizaciones críticas.		
Monitoreo	- Configuración de alertas y generación de reportes automáticos.	Continuo	Equipo de Seguridad.
	- Realización de auditorías internas.		
Capacitación	- Talleres y simulacros para usuarios finales y administradores.	3 semanas	Consultores externos.

Fuente: elaboración propia

Recursos necesarios

Los recursos necesarios para la presente propuesta son el personal especialista en el área, las herramientas para la ejecución, infraestructura que son los servidores de monitoreo y la capacitación del personal mediante programas de entrenamiento. Tal como se muestra en la tabla 23.

Tabla 23. Recursos necesarios

Recurso	Descripción	Costo Estimado
Personal	Especialistas en ciberseguridad, administradores de red y consultores externos.	Dependiente del alcance.
Herramientas	SIEM, escáneres de vulnerabilidades, firewalls y antivirus avanzados.	$20,000 - $50,000 USD.
Infraestructura	Servidores para monitoreo y almacenamiento de logs.	$10,000 USD.
Capacitación	Programas de entrenamiento para el personal.	$5,000 USD.

Fuente: elaboración propia

Cronograma propuesto

Se realiza el cronograma de cada fase junto a la duración en semanas de las mismas. Tabla 24.

Tabla 24. Cronograma de las fases

Fase	Semana 1	Semana 2	Semana 3	Semana 4	Semana 5	Semana 6	Semana 7	Semana 8+
Planificación	X	X						
Ejecución		X	X	X	X	X		
Monitoreo						X	X	Continuo
Capacitación						X	X	

Fuente: elaboración propia

Métricas de éxito

- Reducción del número de vulnerabilidades críticas identificadas en auditorías.
- Implementación exitosa de al menos el 90% de los controles priorizados.
- Incremento en el cumplimiento de políticas de seguridad.
- Respuesta a incidentes dentro del tiempo establecido (según SLA).

Riesgos y mitigación

En la tabla 25 se observa los riesgos que puede haber en la propuesta de implementación así como su impacto, probabilidad de ocurrencia y el plan para mitigar dicho riesgo.

Tabla 25. Riesgos y Mitigación

Riesgo	Impacto	Probabilidad	Plan de Mitigación
Resistencia al cambio	Alto	Media	Capacitar al personal, explicar beneficios de las medidas.
Sobrecarga de trabajo para TI	Alto	Alta	Contratar personal adicional o servicios externos.
Falta de presupuesto	Alto	Baja	Priorizar controles críticos.
Fallos técnicos en las herramientas	Medio	Media	Realizar pruebas piloto antes de la implementación total.

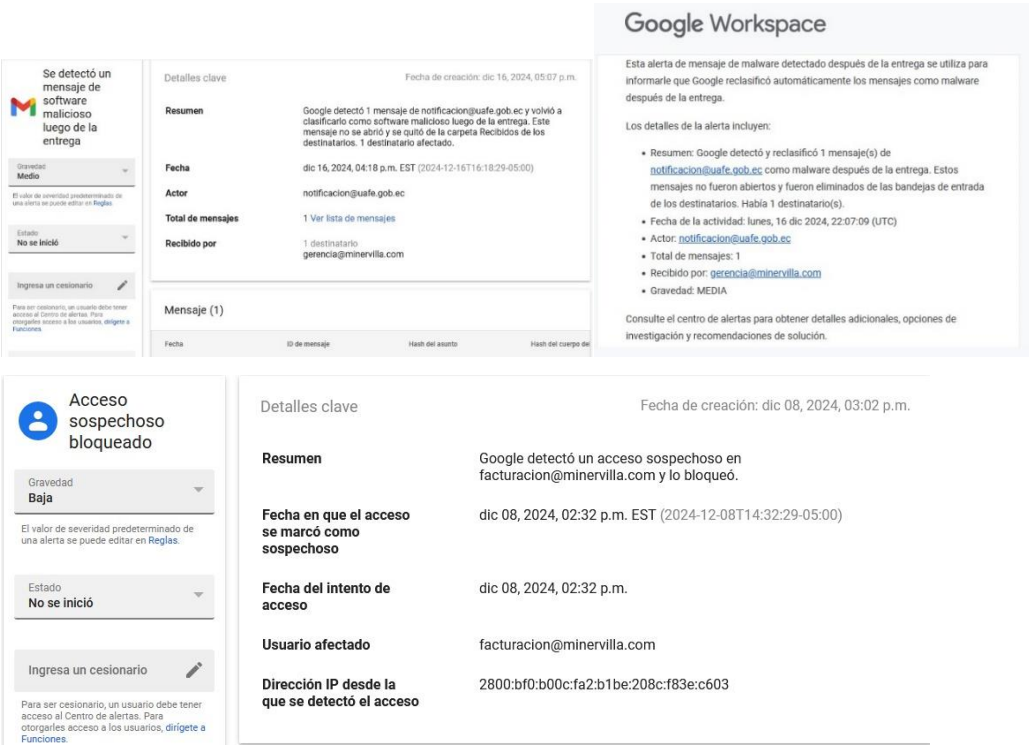
Fuente: elaboración propia

Ejecución de la propuesta

Una vez realizada la simulación de controles CIS se procede a la ejecución de la propuesta presentada para ello.

Se inicia con la implementación de herramientas de detección y eliminación de amenazas, una de ellas son las *Google Workspace* que es un conjunto de herramientas que permiten el control y la administración de los aplicativos con los que se administra MINERVILLA, como se observa en la figura 63.

Figura 63. Detección y eliminación de amenazas



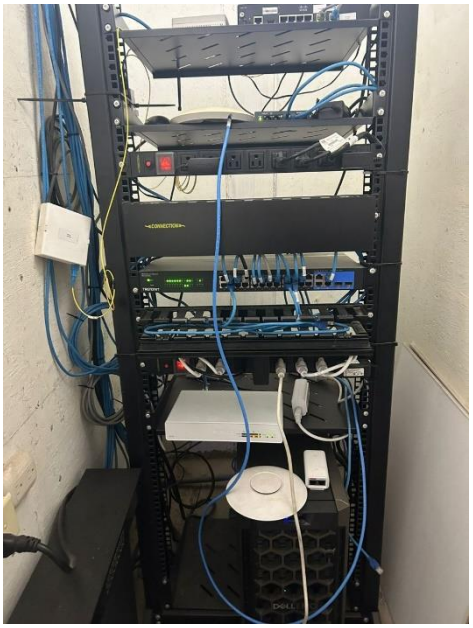
Fuente: elaboración propia

Se prosigue con la configuración y monitorización de red, para ello se procede a revisar la red actual en todos sus aspectos desde los enlaces de fibra hasta el rack principal a fin de poder detectar fallos físicos. Figura 64 y 65.

Figura 64. Revisión de los enlaces de fibra

Fuente: elaboración propia

Figura 65. Revisión de la red actual/Rack principal



Fuente: elaboración propia

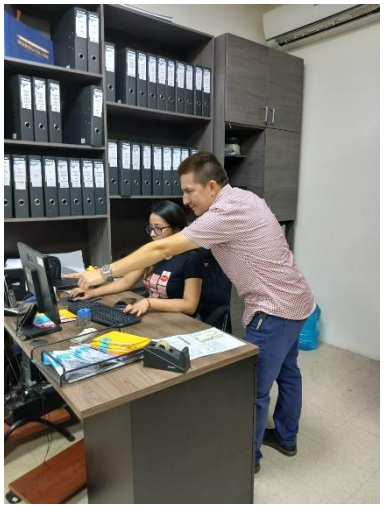
Posterior se divide las VLANS y revisarlas, luego se configura el switch de CORE y la configuración de políticas de acceso y segmentación de red.

Figura 66. Revisión de VLANS y configuración del *Switch de Core*

Fuente: elaboración propia

Finalmente se realiza la capacitación del personal

Figura 67. Capacitación del personal



Fuente: elaboración propia

CONCLUSIONES

- Se argumentaron teóricamente los aspectos sobre ciberseguridad; la protección de datos y la seguridad digital en la red institucional de Minervilla perteneciente al Grupo Chevez a través del uso de herramientas especializadas, lo que permitió identificar las vulnerabilidades potenciales que pueden llegar a comprometer la confidencialidad, disponibilidad e integridad de la información que se encuentra en la red.

- La mayoría de los ataques se pueden bloquear o negar por medio del firewall mediante la monitorización de la herramienta Sophos, donde es de gran importancia definir las entidades que tendrán acceso en la organización siendo propensas a ataques de tipo *man in the middle.*

- Al ser una organización que maneja información o sistemas sensibles se debe tener precaución, porque son propensos a los ataques por correos electrónicos conocidos como *phishing*.

- Es importancia brindar una capacitación sobre políticas de seguridad para el personal permitiendo evitar incidentes relacionados a la seguridad digital como medida de prevención.

- Con los controles aplicados en la simulación se evalúa el riesgo de la red pudiendo determinar que ante las vulnerabilidades generadas el nivel de riesgo cambio a bajo y medio; lo cual hace que se pueda tener una mejor política de seguridad implementada en la red.

- La implementación de controles CIS en empresas que están iniciando la gestión de riesgos tecnológicos en materia de ciberseguridad de la red, se convierten en el punto clave debido a que permiten la ejecución de controles específicos a las necesidades institucionales con un crecimiento progresivo que se puede definir por etapas.

RECOMENDACIONES

- La implementación de herramientas y pruebas de penetración se debe realizar en primera instancia en un entorno simulado, a fin de evitar la caída de servicios y problemas que pueden dar las mismas al momento de su ejecución.

- Se recomienda iimplementar un sistema automatizado para mantener un inventario actualizado de hardware y software, como herramientas de gestión de activos Lansweeper o GLPI.

- Establecer políticas para instalar únicamente software aprobado y verificar actualizaciones automáticas. Utilizar herramientas como SCCM o WSUS para gestionar el software.

- Definir configuraciones estándar seguras para los servidores institucionales, estaciones de trabajo y dispositivos de red, siguiendo guías como las del CIS *Benchmark.*

- Implementar la autentificación multifactor para todas las cuentas críticas y las que tengan acceso remoto.

- Segmentar la red y aplicar políticas de acceso en los firewalls para limitar la comunicación entre segmentos y tener mejor organización.

- Con el paso del tiempo los temas de ciberseguridad se actualizan constantemente y a la vez aparecen nuevos tipos de ataques, por lo que se recomienda estar actualizados con los conocimientos y herramientas adecuadas y especializadas para la detección de riesgos y así estar preparados para prevenir futuros ataques.

- Se recomienda a la Empresa Minervilla implementar todos los 20 controles CIS de tal manera que puedan completar la prevención y mitigación de los

riesgos cibernéticos en toda su estructura de red hasta abarcar todas las empresas del Grupo Chevez.

BIBLIOGRAFÍA

AWS. (2024). Implementación de controles de seguridad en AWS. *AWS Guía prescriptiva*, 6-22. Obtenido de https://docs.aws.amazon.com/es_es/prescriptive-guidance/latest/aws-security-controls/aws-security-controls.pdf#preventative-controls

Baca, G. (2017). *Introducción a la seguridad informática*. Patria.

Briceño, E. V. (2021). *SEGURIDAD DE LA INFORMACIÓN* (Primera ed.). Editorial Área de Innovación y Desarrollo,S.L.

Center for Internet Security. (2021). *Controles CIS*. http://www.cisecurity.org/controls/

CIBERSEGURIDAD . (2024). *Guía completa sobre controles de seguridad CIS*. Obtenido de https://ciberseguridad.com/herramientas/controles-seguridad-cis/

CISCO. (2023). *Ciberataques: ¿cuáles son las ciberamenazas comunes?*

Cyberzaintza. (2024). *Controles de Seguridad CIS*. Obtenido de https://www.ciberseguridad.eus/ciberpedia/marcos-de-referencia/controles-de-seguridad-cis

Figueroa-Suárez, J. A., Rodríguez-Andrade, R. F., Bone-Obando, C. C., & Saltos-Gómez, J. A. (2018). La seguridad informática y la seguridad de la información. *Polo Del Conocimiento*, *2*(12), 145. https://doi.org/10.23857/pc.v2i12.420

Fuertes, W. M. (2022). *Blue futuristic networking technology vector*. ESPE. https://acortar.link/YQIayF

Gobierno Electrónico. (2020). *Guía para la gestión de riesgos de seguridad de la información*. www.gobiernoelectronico.gob.ec

Granados, I. M. (2016). Iniciativas ciudadanas de control y vigilancia política 1. *PráxisSociológica*, *21*, 141–172. www.praxissociologica.es

Guijarro, E. G. (2023). Seguridad en la Infraestructura de Redes: Desafíos y Estrategias de Protección. *VICTEC*, *4*(7), 183–192. https://server.istvicenteleon.edu.ec/victec/index.php/revistapp.183-192

Hernández-Sampieri, R., & Mendoza, C. P. (2018). *Metodología de la Investigación* (Séptima).

Hewlett Packard Enterprise. (2023). *¿Qué es la seguridad informática?* | *Glosario*.

Honores, L. (2021). *Diseño e implementación de un sistema de seguridad mediante controles CIS para redes de acceso, caso instituto nacional de evaluación educativa (INEVAL).* Ecuador. Obtenido de http://dspace.espoch.edu.ec/bitstream/123456789/14702/1/20T01447.pdf

ISO/IEC. (2022). Information security, cybersecurity and privacy protection — Information security management systems — Requirements. *International Standard*(3).

Incibe. (2023). *Amenaza vs Vulnerabilidad, ¿sabes en qué se diferencian?* | *Empresas* | *INCIBE*.

(INCIBE), M. A. (28 de Diciembre de 2017). *INCIBE Instituto Nacional de Ciberseguridad*. Obtenido de https://www.incibe.es/empresas/blog/2017-el-ano-las-empresas-se-concienciaron-ciberseguridad

Juan José Ripoll Samper, M. R. (2015). Seguridad informática en el siglo xx : una perspectiva jurídica tecnológica enfocada hacia las organizaciones nacionales y mundiales. *SemanticScholar*, 16.

Leiva, E. A. (2015). Estrategias Nacionales de Ciberseguridad: Estudio Comparativo Basado en Enfoque Top-Down desde una Visión Global a una Visión Local. *Revista Latinoamericana de Ingeniería de Software*, *3*(4), 161–176. https://doi.org/https://doi.org/10.18294/relais.2015.161-176

Liberatori, M. C. (2018). *Redes de Datos y sus Protocolos*. eudem.

Mahn, A., Marron, J., Quinn, S., & Topper, D. (2022). Primeros pasos de NIST Marco de ciberseguridad: Guía de inicio rápido. *NIST*. https://doi.org/10.6028/NIST.SP.1271es

Marchand-Niño, W.-R., & Vega Ventocilla, E. J. (2020). Modelo Balanced Scorecard para los controles críticos de seguridad informática según el Center for Internet Security (CIS). *Interfases*, 57–76. https://doi.org/10.26439/interfases2020.n013.4876

Montesino, R., Baluja, W., & Porvén, J. (2013). Gestión automatizada e integrada de controles de seguridad informática. *RIELAC*, *1*, 40–58. http://scielo.sld.cu/pdf/eac/v34n1/eac04113.pdf

National Institute of Standards and Technology. (2018). *Framework for Improving Critical Infrastructure Cybersecurity*. https://doi.org/10.6028/NIST.CSWP.04162018

Newmeyer, K. (2015). *Ciberespacio, Ciberseguridad y Ciberguerra*. https://www.academia.edu/108550158/Ciberespacio_Ciberseguridad_y_Ciberguerra

Ocaña, E. J., Ortiz, N. S., & Trujillo, X. F. (2023). Análisis de desempeño de una red WLAN implementando el estándar IEEE 802.11ax orientado a redes de acceso múltiple y aplicaciones sensibles a latencia. *RECIAMUC*, *7*(2), 170–179. https://doi.org/10.26820/reciamuc/7.(2).abril.2023.170-179

Odom, W. (2016). *Cisco CCENT/CCNA ICND1 100-105 official Cert guide*. Cisco Press.

Pineda, S., & Morales, H. (2020). Topología aplicada en redes ad hoc. *Ingenierías*, *2*(1), 18–26. http://cipres.sanmateo.edu.co/ index.php/mi

Red Hat. (2023). *Infraestructura de red con Red Hat y sus partners*.

Rodríguez Navas, P. M., Simelio, N., & Corco y Ruiz, M. (2017). Metodologías de evaluación de la transparencia: procedimientos y problemas. *Revista Latina de Comunicación Social*, *72*(8), 818–831. https://doi.org/10.4185/RLCS

Romero, M., Fugueroa, G., Vera, D., Álava, J., Parrales, G., Álava, C., Murillo, Á., & Castillo, M. (2018). *INTRODUCCIÓN A LA SEGURIDAD INFORMÁTICA Y EL ANÁLISIS DE VULNERABILIDADES* (Primera edición).

Salcedo, D. A. (Mayo de 2023). *Guía para el establecimiento de métricas e indicadores clave de rendimiento (KPI) en la gestión de proyectos de construcción durante su fase de ejecución.* Obtenido de https://upcommons.upc.edu/bitstream/handle/2117/393135/Mem%c3%b2ria_.pdf?sequence=2&isAllowed=y#page=38&zoom=100,72,94

SCHOOL, E. I. (20 de Septiembre de 2024). *ENAE INTERNATIONAL BUSINESS SCHOOL*. Obtenido de https://www.enae.es/blog/la-importancia-de-la-ciberseguridad-en-el-mundo-digital?gad_source=1&gclid=Cj0KCQiA0--6BhCBARIsADYqyL_7yIDgdUUtRw8_uWUiE-9ltl5tc2w685vwSwiN0W0mgSxEmejrAjQaAg7qEALw_wcB&_adin=11551547647

Secureframe. (2024). *Controles de Seguridad Críticos del CIS: Cómo implementar la versión 8.1* . Obtenido de https://secureframe.com/es-es/blog/cis-critical-security-controls

Secureframe. (2024). *Secureframe*. Obtenido de https://secureframe.com/es-es/blog/secureframe-named-leader-in-winter-2024-g2-reports

Solarte, F., Enríquez, E., & Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. *Revista Tecnológica ESPOL*, *28*(5), 493–507. https://rte.espol.edu.ec/index.php/tecnologica/article/view/456/321

SolarWinds. (2023). *What is Network Infrastructure?*

Sophos. (2023). *El estado delransomware 2023*. https://news.sophos.com/es-419/2023/05/10/el-estado-del-ransomware-2023/

Urbina, G. B. (2018). *Introducción a la Seguridad Informática* (Primera ed., Vol. 1). México, México: Grupo Editorial Patria.

Vasco, G. (Noviembre de 2024). *cyber zaintza*. Obtenido de https://www.ciberseguridad.eus/boletin-cibereguraldia-ciberseguridad/ciber-eguraldia-noviembre-2024

Walton, A. (2023). *Topologías de Red LAN y WAN » CCNA desde Cero*. https://ccnadesdecero.es/topologias-red-lan-y-wan/

Whitman, M. y. (2012). Un estudio de caso sobre la adopción de directrices de seguridad en la educación de pregrado en ingeniería de software. *Scientific Research, 2*(14), 1-5.