



UNIVERSIDAD CÉSAR VALLEJO

FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA PROFESIONAL INGENIERÍA DE SISTEMAS

Implementación de hardening a nivel de red para mejorar la
seguridad de la información en la Municipalidad de Carabaylo,
2021

TESIS PARA OBTENER EL TÍTULO PROFESIONAL DE:
INGENIERO DE SISTEMAS

AUTOR:

Chinchay Toribio, Ebel Aldair (orcid.org/0000-0003-4034-5567)

ASESOR:

Mg. Carranza Barrena, Wilfredo Eduardo (orcid.org/0000-0003-0845-1984)

LÍNEA DE INVESTIGACIÓN:

Auditoría de sistemas y Seguridad de la Información

LÍNEA DE RESPONSABILIDAD SOCIAL UNIVERSITARIA:

Desarrollo sostenible y adaptación al cambio climático

LIMA - PERÚ

2022

Dedicatoria:

A mis padres quienes me brindaron su apoyo incondicional en el transcurso de mi carrera universitaria para poder lograr ser un profesional de éxito.

Agradecimiento:

Agradezco a la Universidad Cesar Vallejo que me abrió las puertas y que día a día contribuye en mi formación para lograr ser un profesional de éxito.

A mis familiares, amigos, profesores y compañeros de clases, por la ayuda en enriquecer nuestro conocimiento durante la etapa universitaria.

Índice de contenidos

I.	INTRODUCCIÓN.....	1
II.	MARCO TEÓRICO.....	5
III.	METODOLOGÍA.....	12
3.1	Tipo y diseño de investigación.....	12
3.2	Variables y Operacionalización.....	13
3.3	Población, muestra y muestreo.....	14
3.4	Técnicas e instrumentos de recolección de datos.....	15
3.5	Procedimientos.....	16
3.5.1.	Recolección de datos.....	16
3.5.2.	Procesamiento de datos.....	16
3.6	Método de análisis de datos.....	17
3.7	Aspectos éticos.....	19
IV.	RESULTADOS.....	19
V.	DISCUSIÓN.....	25
VI.	CONCLUSIONES.....	27
VII.	RECOMENDACIONES.....	28
	REFERENCIAS.....	29
	ANEXOS.....	34

Índice de tablas

Tabla 1: Determinar la Población	14
Tabla 2: Determinación de la técnica e instrumento de recolección de datos ..	16
Tabla 3: Medidas descriptivas de DANA: Detección de acceso no autorizado a la red en pre test y post test	20
Tabla 4: Medidas descriptivas de DR: Disponibilidad de la red en pre test y post test	21
Tabla 5: Prueba de normalidad - Detección de acceso no autorizado a la red	22
Tabla 6: Consulta RUC	53
Tabla 7: Distribución física de las UO por pisos	65
Tabla 8: Dispositivos de red	66
Tabla 9: Redes de la MDC	73
Tabla 10: Buenas prácticas de configuración.....	75
Tabla 11: Aplicación y servicios de la MDC.....	77
Tabla 12: Aplicaciones de la MDC	79
Tabla 13: Entrevista	84
Tabla 14. Segmentación de la red.....	92

Índice de figuras

Figura 1: Diseño de Estudio	12
Figura 2: DANA: Promedio de accesos no autorizados en pre test y post test	20
Figura 3: DR: Disponibilidad de la red en pre test y post test.....	21
Figura 4: Ubicación de la Municipalidad Distrital de Carabaylo	54
Figura 5: Ficha técnica de la MDC	55
Figura 6: Organigrama	56
Figura 7: Arquitectura modular de SAFE.....	58
Figura 8: switch no administrables	67
Figura 9: Desorden de gabinetes	67
Figura 10: Arquitectura modular actual	68
Figura 11: Modulo Central - Distribución	70
Figura 12: Módulo del Edificio	71
Figura 13: Flujo de la Información	80
Figura 14: Pasos para la obtención de requerimientos	83
Figura 15: Diagrama de red - Oficinas centrales de la entidad.....	90

Resumen

El hardening o endurecimiento, son procedimientos que permiten poner en práctica estrategias como herramientas con la finalidad de mejorar la seguridad. La problemática a nivel de red que surgen día a día; como son la lentitud o inaccesibilidad a los diferentes servicios como correo electrónico, internet, sistemas de información internos, servicios de impresión, recursos compartidos entre otros, así como el acceso de distintos equipos a la red sin la autorización del jefe inmediato superior.

La investigación tuvo una aplicación de tipo aplicada, de diseño pre experimental, con enfoque cuantitativo, se presenta conceptos claves de las variables de estudio. El objetivo de esta investigación es implementar el hardening a nivel de red para mejorar la seguridad de la información en la Municipalidad de Carabayllo.

Para la aplicación del hardening a nivel de red se realiza un rediseño a la red utilizando la metodología PPDIOO junto con el modelo de seguridad para las redes SAFE de cisco y las buenas prácticas de seguridad para la configuración de equipos definidas en los benchmarks de CISecurity.

Se realizó el pre test y post test de los indicadores DANA: detección de accesos no autorizado a la red y DR: disponibilidad de la red. Al tener una muestra menor a 50 se realiza la prueba Shapiro Wilk en la prueba de normalidad, determinado que los datos no siguen una distribución normal. Para la verificación de la hipótesis se utilizó la prueba wilcoxon.

Los resultados mostraron que para el indicador DANA mejoro (disminuyó) de un promedio de 6 a 2 accesos no autorizados con la implementación de hardening a nivel de red, para el indicador DR la disponibilidad mejoro (aumentó) de un 99.55% a 99.90% de disponibilidad de la red. Concluyendo que la implementación del hardening a nivel de red mejora la seguridad de la información en la municipalidad de Carabayllo.

Palabras Clave: Hardening, Seguridad de la Información, Vlans, metodología PPDIOO, modelo de seguridad, benchmarks de CISecurity.

Abstract

Hardening or hardening are procedures that allow strategies to be put into practice as tools in order to improve security. The problems at the network level that arise every day; such as the slowness or inaccessibility of different services such as email, internet, internal information systems, printing services, shared resources, among others, as well as the access of different computers to the network without the authorization of the immediate superior.

The research had an application of applied type, of pre-experimental design, with a quantitative approach, key concepts of the study variables are presented. The objective of this research is to implement hardening at the network level to improve information security in the Municipality of Carabayllo.

For the application of hardening at the network level, a network redesign is carried out using the PPDIOO methodology together with the security model for Cisco SAFE networks and the good security practices for the configuration of equipment defined in the CISecurity benchmarks.

The pre-test and post-test of the DANA indicators were carried out: detection of unauthorized access to the network and DR: network availability. Having a sample of less than 50, the Shapiro Wilk test is performed in the normality test, determined that the data does not follow a normal distribution. To verify the hypothesis, the Wilcoxon test was used.

The results showed that for the DANA indicator it improved (decreased) from an average of 6 to 2 unauthorized accesses with the implementation of hardening at the network level, for the DR indicator the availability improved (increased) from 99.55% to 99.90% of network availability. Concluding that the implementation of hardening at the network level improves information security in the municipality of Carabayllo.

Keywords: Hardening, Information Security, Vlans, PPDIOO methodology, security model, CISecurity benchmarks.

I. INTRODUCCIÓN

La constitución política del Perú, así como las posteriores leyes orgánicas dan a las municipalidades personería jurídica de derecho cuyo fin es de remediar las necesidades del distrito local que son de carácter esencial y, a la vez cotidianas. De acuerdo al INEI Carabayllo tiene una tasa de crecimiento de 4.6 promedio anual, de acuerdo al último censo cuenta con 333405 habitantes. Este crecimiento de la población ocasiona una gran afluencia de la ciudadanía solicitando servicios administrativos. Por lo que se debe contar con una infraestructura física y tecnológica apropiada para poder brindar una atención de calidad.

Es fundamental que una arquitectura de red, cumplan con ciertas particularidades básicas mínimas como la escalabilidad, calidad de servicio, tolerancia a fallas y seguridad, esto garantiza que las plataformas de las TIC trabajen de forma dinámica.

La red corporativa en la municipalidad de Carabayllo ha crecido de manera progresiva durante estos últimos años el cual oblige a un cambio de máscara de red de 255.255.254.0 prefijo /23 a 255.255.252.0 prefijo /22, incrementando de 512 a 1024 host permitiendo el acceso de nuevos equipos, para hacer uso de los servicios de la entidad.

El crecimiento de personal y la no planificación a futuro de posible aumento de equipos tecnológicos en las oficinas, con lleva a colocar pequeños switch domésticos. El uso de estos trae como error de conectar los dos extremos de un cable de red al mismo switch o en todo caso colocarlo a un punto de red ubicada en la pared, ocasionando un bucle, y tormenta de emisiones que esto hace que se pierda información en la red, lentitud o la inaccesibilidad a las diferentes servicios tales como correo electrónico, páginas web, sistemas de información internos, servicios de impresión, recursos compartidos, comunicación de teléfonos por IP, cámaras de seguridad y otros.

En la institución por falta de equipos de cómputo están aplicando la tendencia BYOD (Bring Your Own Device) el cual la municipalidad permite a los trabajadores llevar sus dispositivos portátiles de manera que estos puedan realizar sus actividades conectándose a la red y hacer uso de los servicios que necesiten de la institución, hay usuarios en la cual sus laptops no cuentan con puerto Ethernet por lo cual traen Access Point para poder conectarse a la red, ocasiones en las cuales estos dispositivos estaban mal configurados entregando otro rango de IP por medio de DHCP, impidiendo el acceso a recursos de la entidad. Por otro lado hay usuarios que no tienen la autorización por parte de jefe inmediato y hacen uso de los recursos suponiendo una falla en la seguridad.

El estudio se justificó socialmente ya que está orientado hacia estudiantes, profesionales y/o personas relacionadas a las TIC, ya que se da nociones importantes de una implementación de hardening a nivel de red como una herramienta disponible en pro de elevar la seguridad de la información. Las áreas orgánicas disponen de información sensible, una de estas es la gerencia de administración tributaria y recaudación. (Jara Mendoza, 2018) Indica al activo SISMUN como un riesgo, este sistema permite la administración o gestión tributaria de los contribuyentes y administrados, cuya información debe ser íntegra, esta debe ser privada de acuerdo a ley N° 29733 – Ley de protección de datos personales.

Se justificó teóricamente aportando al conocimiento actual sobre la importancia de la implementación de hardening a nivel de red. (Martínez Cruz, 2015) En su artículo menciona que los routers y switch son la base fundamental en toda infraestructura de TI. A través de recomendación por estándares o buenas prácticas de gobernanza y proveedores en su implementación de hardening a nivel de red se obtendrá un resultado favorable en mejoras de la seguridad.

Se justificó de manera práctica ya que utilizo recomendaciones de estándares y buenas prácticas con el propósito directo de reducir las vulnerabilidades, que podrían afectar a las áreas orgánicas de la entidad con respecto a los pilares de la información que son la disponibilidad, confidencialidad y disponibilidad. Evitando o entorpeciendo que se concrete una intromisión en la red.

El estudio se justificó tecnológicamente, se empleó equipos de comunicación de red tales como antenas, switch y routers el cual permitió a la municipalidad de Carabayllo tener una mejor seguridad de su información, comunicación segura y flexible.

Ante las problemáticas descritas, se plantea la implementación de hardening a nivel de red, la cual permitirá mejorar la disponibilidad, confidencialidad, integridad, calidad de servicio, la tolerancia a fallas y escalabilidad.

Sobre el origen de la problemática presentada se planteó como problema general. ¿Cómo la implementación de hardening a nivel de red mejorará la seguridad de la información en la Municipalidad de Carabayllo?, posterior a ello se plantean dos problemas específicos: ¿Cómo la implementación de hardening a nivel red mejorará la detección de acceso no autorizado a la red en la seguridad de la información en la Municipalidad de Carabayllo?, segundo problema específico ¿Cómo la implementación de hardening a nivel de red mejorará la disponibilidad de la red en la seguridad de la información en la Municipalidad de Carabayllo?

Como objetivo general indicamos. Implementar el hardening a nivel de red para mejorar la seguridad de la información en la Municipalidad de Carabayllo. Los objetivos específicos son los siguientes: Implementar el hardening a nivel de red para mejorar la detección de acceso no autorizado a la red en la seguridad de la información en la Municipalidad de Carabayllo, segundo objetivo específico Implementar el hardening a nivel de red para mejorar la disponibilidad de la red en la seguridad de la información en la Municipalidad de Carabayllo.

Con la hipótesis general. La implementación de hardening a nivel de red mejora la seguridad de la información en la Municipalidad de Carabayllo. Las hipótesis específicas son: La implementación de hardening a nivel de red mejora la detección de acceso no autorizado a la red en la seguridad de la información en la Municipalidad de Carabayllo, segunda hipótesis específica la implementación

de hardening a nivel de red mejora la disponibilidad de la red en la seguridad de la información en la Municipalidad de Carabaylo.

II. MARCO TEÓRICO

En el presente estudio se ha revisado, investigado en diversas fuentes con cobertura geográfica nacional como internacional de conceptos claves en bibliotecas indexadas, artículos científicos, revistas estadísticas, libros y repositorios universitarios, suministrando a la investigación un soporte teórico que sustenta la problemática.

(Sanchez Arias, 2018), tiene como objetivo el desarrollo de una propuesta de virtualización de dispositivos para la optimización de los servicios de la red LAN en el Hospital Nacional Edgardo Rebagliati, el tipo de investigación es aplicada y descriptiva, casi experimental. Cuya población y muestra es de 135 dispositivos de conmutación, el instrumento de recolección utilizado fueron encuesta, ficha de evaluación y observación. El autor formula como conclusión que se desarrolló una propuesta de segmentación de la red por tipos de servicio datos, video, impresión, WIFI además se propuso reglas, seguridad de puertos con el fin de mitigar posibles ataques en la red.

(Rojas Mattos, 2018) Cuya investigación tuvo como objetivo mejorar la comunicación de datos en la empresa Grupo el Saber mediante un diseño e implementación de red basada en VLAN's. Investigación explicativa, pre-experimental. Con una población y muestra de 72 broadcast al día. Se recolecto la información mediante cuestionario y entrevistas. Como conclusión resaltante menciona que se aumentó la seguridad en los equipos de interconexión de red en un 83.33% esta implementación aumentó de forma representativa la comunicación de datos en la organización, reduciendo la demora de transferencia de datos en un 38.33 %.

(Farah Miraval, 2016) Propone como objetivo diseñar un modelo de implementación de redes virtuales y priorización del ancho de banda para aumentar el rendimiento de la red de área local. Investigación de tipo aplicada descriptiva, longitudinal. Cuya muestra es de 162 usuarios con acceso a la red. El instrumento de recolección utilizado es la observación y análisis. Los resultados obtenidos fue la implementación de un modelo jerárquico escalable y disponible de la red con incorporación de políticas de seguridad, aumentando a

más de 10% el rendimiento de la red, priorizando el ancho de banda de acuerdo a la segmentación de las redes.

(Yuri Tilio, 2019), propone como objetivo determinar la influencia de un modelo de gestión de servicios de red con RoutersOS Mikrotik en la disponibilidad de información de la red, investigación aplicada y explicativa, pre experimental. De 204 host como población y muestra poblacional de 20 host, el instrumento de recolección usado fueron fichas de observación y lista de cotejos. Como conclusión el autor determino que influye positivamente la disponibilidad, prevención de ataques y accesibilidad con el modelo de gestión de servicios con RouterOS Mikrotic, recomienda implementar un firewall de capa 7.

(Garcia, 2018), menciona como objetivo la propuesta de un nivel de mejora en la red de computadoras a traves de un nuevo diseño de la red del Hospital III José Cayetano Heredia. Investigación no experimental. Cuya población son los usuarios con acceso a la red local de un total de 110 personas. Instrumento utilizado son los cuestionarios y guías de observación. Como conclusión menciona que se mejoró el cableado estructurado de acuerdo a estándares internacionales, con la utilización de VLANS se mejoró el tráfico, se redujo significativamente la latencia y se incrementó la seguridad de la información en la que se transfiere y comparte por la red.

(Congora Huanay, y otros, 2018), propone como objetivo determinar la influencia de la aplicación del diseño de una red LAN en la accesibilidad de información en la infraestructura de comunicación en la Municipalidad Daniel Hernández. Investigación de tipo tecnológica de nivel experimental, pre-experimental. De una población conformada por todos los host que está conectada a la red. Como instrumentó de recolección se utilizó las fichas de observación. Indica como conclusión que influye significativamente el diseño de una red LAN en la disponibilidad de la información en un promedio final de 117.9 ms a 62.86 ms. Mejora el tiempo de respuesta de un promedio final de 81.23 ms a 33.58 ms referente a la accesibilidad.

(Alvitres Grundy, 2017) Cuya investigación tuvo como objetivo el diseño e implementación de la red de datos para solucionar problemas de comunicación,

mejorar la calidad de servicio, optimizando procesos en la Municipalidad de Cáceres del Perú. Se utilizó dos tipos de diseño de investigación descriptiva y documental con enfoque cualitativo. Con población de 60 y muestra poblacional de 8 trabajadores. Los datos se recolectaron a través de cuestionarios. Según los resultados, con respecto al nivel de satisfacción un 63 % de trabajadores no están conformes con el sistema actual, esto concuerda con la hipótesis específica donde asume que la evaluación de la red LAN permitirá control de información, seguridad y eficiencia.

A nivel internacional (Yungán Cazar, 2016), tiene como objetivo principal evaluar la aplicación del protocolo 802.1Q en la implementación de VLANS en entornos Wireless mediante la aplicación de software libre. Investigación aplicada explicativa, experimental, cuasi experimental. De población y muestra de 4 departamentos. El instrumento de recolección usado fue captura, y monitorización de conexión de red. Como conclusión el autor menciona que a través de la segmentación de red en LAN virtuales, se evidencia incremento significativo en índices tales como tiempo de PING (sin VLAN 446,35 ms y con VLAN 162,93 ms) y pérdida de paquetes (Sin VLAN 0,40 y con VLAN 0,20), debiéndose a la focalización de tráfico y reducción de dominios de colisión.

(Fache Montaña, 2016) presento como objetivo realizar un estudio de nivel de seguridad en la red informática, para la implementación de medidas basadas en hardening, que permitan mejorar la seguridad informática en el instituto COTEL. Investigación de tipo descriptivo con métodos de análisis y síntesis. Población conformada por profesores, alumnos y trabajadores del instituto COTEL. Donde concluye que se estableció el proceso de defensa en profundidad como una manera de afianzar la infraestructura de TI, se aplicó el hardening como una solución basada en políticas, software y procedimientos de seguridad.

(Portela Carvajal, y otros, 2020), cuya investigación tiene como objetivo el rediseño lógico de la red LAN actual a partir de un modelo jerárquico de red de 3 capas de cisco mejorando el rendimiento y corrigiendo problemas de seguridad. El tipo de investigación es aplicada descriptiva cuya población son todos los usuarios conectados a la red. Menciona como conclusión que se utilizaron métodos como vlan, intervlan Routing, port security, ACL y DHCP

permitiendo un mayor rendimiento, seguridad de acceso a la información, y tráfico entre redes.

(Guido, 2018) Presenta como objetivo implementar un modelo jerárquico de red para mejorar el rendimiento, seguridad perimetral y garantizar un óptimo desempeño, rendimiento en la Unidad Educativa Salesiana Domingo Comin. Investigación de nivel descriptivo de tipo proyectiva. Menciona como conclusión que después del rediseño de la red se cuenta con una disponibilidad del 99.9 %, permitiendo las VLANs un mejor flujo del tráfico, se aísla los servidores en una DMZ, el uso del protocolo RSTP permitió una mayor disponibilidad.

(Cruz, 2017), cuya investigación tuvo como objetivo definir un proceso de hardening para el aseguramiento de la IT de la organización. Con un tipo de investigación aplicada. Concluye que al no realizar una gestión de vulnerabilidades se podría haber materializado una amenaza pudiendo llevar la pérdida de la integridad, confidencialidad y disponibilidad de la información. Un atacante interno puede generar una afectación en la entidad identificadas estas vulnerabilidades en gran medida se mitigaron.

El presente estudio contiene las siguientes teorías:

La ISO (organización internacional de normas), cuenta con un modelo de referencia en el que describe el funcionamiento de los protocolos de comunicación de datos, llamado OSI (Modelo de Referencia de interconexión de sistemas abiertos) en el cual detallan las funciones para que cada paquete de datos viaje de un origen al destino. Esta investigación trabajara en los niveles (1) nivel físico, (2) nivel de enlace de datos y (3) nivel de red.

Para (Gormaz Gonzales, 2013) el cableado estructurado es la forma en la cual se conectan los equipos.

La metodología PPDIOO permite formalizar el ciclo de vida de una red en seis etapas: Preparación, Planificación, Diseño, Implementación, Operación y Optimización. Cada una de las fases cumple con su función específica y se relacionan con su antecesora

En el libro Curso de Ciberseguridad y hacking ético (Gutierrez del Moral, 2014), menciona que “Hardening, en seguridad informática es el proceso mediante el cual se busca asegurar el sistema mediante la reducción de las vulnerabilidades del mismo” Cuyo fin, es dificultar la labor del atacante o evitar que estas se concreten, minimizando las consecuencias de un incidente de seguridad.

En el libro Ciberseguridad Sin Destinatario: La Ciberseguridad no es una moda. (Zorrilla Mateo, 2020) Indica que “El hardening es una metodología bastante singular, trata de procesos de aseguramiento de un sistema mediante la reducción de vulnerabilidades (eliminación total es utópico), para lograr esta hazaña de endurecimiento se debe eliminar el software, los servicios y usuarios innecesarios del sistema”. Para simplificarlo, lo definiremos como la serie de pasos realizados con el fin de fortalecer la seguridad. Debemos quedar claro que sin importar lo que hagamos para proteger nuestros sistemas, este no será invulnerable o imposible de penetrar, pues muy cierto es, que “imposible no es un término científico”.

Según (Cisco, 2007), una VLAN (Red de área local virtual) es un procedimiento para crear redes lógicas independientes dentro de una misma red física. Es decir, facilita la agrupación lógica de dispositivos o servicios de red en base a unidades orgánicas, funciones, aplicaciones y otros sin considerar la localización física o conexión de red, permitiendo segmentar la red según la necesidad de la organización. Una red basada en VLAN ofrece: Seguridad, solo las estaciones de trabajo que pertenecen a la misma VLAN podrán comunicarse directamente (sin enrutamiento); Reducción de costos, ya que hace uso más eficaz de los puertos y ancho de banda; Mejor rendimiento, la segmentación de la red en grupos (dominio de difusión) reduce el tráfico de broadcast mejorando el rendimiento.

Para (Martínez Cruz, 2015) indica que se deberían hacer como mínimo para el proceso de hardening en los switch estos pasos. (A) ASEGURAR EL ACCESO, consiste en desactivar protocolos inseguros, usar ACL para restringir los accesos a nivel LAN y utilizar una VLAN exclusiva para la administración de estos, (B)

ASEGURAR LOS PROTOCOLOS Y SERVICIOS, se basan en eliminar las configuraciones por defecto de fábrica, activar logs de auditoria y almacenarlos en un servidor syslog así como apagar los puertos no usados (C) ASEGURAR LA TRAZABILIDAD, tener bitácora del dispositivo y tener documentada las configuraciones.

Para (ISOTools Excellence, 2017) menciona que la seguridad de la información es la disciplina a cargo de la implementación técnica para asegurar la información, desplegando tecnologías que permitan asegurar situaciones de fallas totales o parciales. Encargándose de evaluar riesgos, amenazas, buenas practicas, análisis de escenarios y esquemas normativos que exigen un aseguramiento de tecnología y procesos. Con el fin de asegurar la integridad, disponibilidad y confidencialidad del manejo de la información de activos.

Para (welivesecurity, 2015) La seguridad de la información se sostiene de estándares, normas, técnicas, metodologías, herramientas y tecnologías, enfocados a resguardar la información en distintas facetas.

(Avenia, 2017), indica que la seguridad de la información protege la información del acceso, utilización y eliminación no autorizada a través de procedimientos, recursos informáticos y recursos humanos.

Una vulnerabilidad hace referencia a una debilidad del sistema permitiendo un ataque donde se afecte la confidencialidad, integridad y disponibilidad. Entre las principales vulnerabilidades de una red encontramos: Vulnerabilidades ambientales e infraestructura, Protección física inadecuada, control de acceso inadecuado, energía eléctrica inestable, desastre natural, desastres humanos; Vulnerabilidades del personal, personal insuficiente, falta de mecanismos de monitoreo, falta de políticas, normas y procedimientos, recursos insuficientes; Vulnerabilidades del Hardware, falla del hardware y componentes, falta de mantenimiento planificada, control de acceso inadecuado, suministro eléctrico, , conexión de equipo no autorizado; Vulnerabilidades de comunicaciones, Líneas de comunicación no protegidas, administración de la red inadecuada y protección inadecuada para el acceso público; Vulnerabilidades de software, control de acceso inadecuado, contraseñas no protegidas, claves y certificados,

falta de documentación. Esta vulnerabilidad se convierte en una amenaza pudiendo ocasionar consecuencias negativas para la entidad.

La seguridad de la información se centra en 3 pilares de la seguridad: confidencialidad, integridad y disponibilidad para (Romero, 2018).

CONFIDENCIALIDAD, mediante permisos otorgado por el administrador el usuario, personal autorizado podrá acceder a la información para hacer uso de este. Para garantizar la confidencialidad se dispone de tres principios. (1) Autenticación del usuario, (2) Manejo de gestión de privilegios, (3) Cifrado de la información.

INTEGRIDAD, la información no puede estar comprometida voluntariamente mucho menos perderse, trabajar con información equivocada generaría una cadena de errores sucesivos terminando en decisiones incorrectas, tener información errada es tan perjudicial como perder la información. Para garantizar la integridad se considera (1) Descubrir posibles instrucciones mediante el monitoreo del tráfico, (2) Implementación de políticas de auditoría, (3) Hacer uso de sistemas de control de cambios.

DISPONIBILIDAD, Para acceder a la información el mecanismo de este no debe ser tedioso o imposible, la información para que resulte útil debe estar disponible para quien lo necesite, se deben tomar medidas para asegurar esto. En este propósito se implementan (1) Acuerdo de nivel de servicio, (2) Balanceo de cargas para el tráfico (3) Copias de seguridad en caso se necesite restaurar información perdida.

III. METODOLOGÍA

3.1 Tipo y diseño de investigación

El estudio es de tipo aplicada, ya que se implementará hardening a nivel de red para mejorar la seguridad de la información, permitiendo reducir las vulnerabilidades a nivel de red.

La investigación estará dada bajo el enfoque cuantitativo según (HERNÁNDEZ, 2014), sostiene que se emplea la recolección de datos para probar la hipótesis y el análisis estadístico, respondiendo como base a la medición numérica para responder normas de conducta y probar las teorías.

La investigación presente tiene como diseño de investigación pre-experimental según indica (Hernández, 2014), Diseño se aplica a una previa prueba a un grupo con tratamiento experimental, y luego se administra el tratamiento, aplicando finalmente una prueba posterior donde hay un punto intermedio de referencia para medir el grado del grupo de las variables dependientes antes de su aplicación; en la aplicación de este diseño, hay un seguimiento del grupo. Para el estudio realizado se diagrama de la siguiente manera:

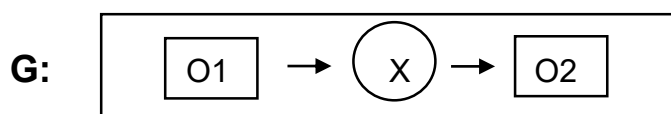


Figura 1: Diseño de Estudio

Dónde:

G: Grupo experimental

O1: Seguridad de la información antes de la implementación de hardening a nivel de red

X: Implementación de hardening a nivel de red

O2: Seguridad de la información después de la implementación de hardening a nivel de red.

3.2 Variables y Operacionalización

- **Identificación de Variables:**
 - ✓ Variable Independiente: (VI): Implementación de hardening a nivel de red.
 - ✓ Variable Dependiente: (VD): Seguridad de la información.

- **Definición Conceptual:**

- ✓ Implementación de hardening a nivel de red

Según (AVENIA, 2014) "Hardening, en seguridad informática es el proceso mediante el cual se busca asegurar el sistema mediante la reducción de las vulnerabilidades del mismo" Cuyo fin, es dificultar la labor del atacante o evitar que estas se concreten, minimizando las consecuencias de un incidente de seguridad.

- ✓ Seguridad de la Información

La seguridad de la información para (ISOTools Excellence, 2017) Es la disciplina a cargo de la implementación técnica para asegurar la información, desplegando tecnologías que permitan asegurar situaciones de fallas totales o parciales. Encargándose de evaluar amenazas, riesgos, análisis de escenarios, buenas prácticas, y esquemas normativos que exigen un aseguramiento de tecnología y procesos. Con el fin de asegurar la integridad, confidencialidad y disponibilidad del manejo de la información de activos.

- **Definición Operacional:**

- ✓ Implementación de hardening a nivel de red: Proceso en el cual se aplica buenas prácticas de configuración para reducir las vulnerabilidades así reforzar al máximo la seguridad de la información.

- ✓ La seguridad de la información: Es un conjunto de medidas, políticas y técnicas preventivas que permitan afrontar los riesgos, prevenirlos en búsqueda de soluciones para poder contenerlos o mitigarlo permitiendo custodiar la información en busca de la disponibilidad, integridad y confidencialidad de la información.

Para mayor detalle se puede apreciar en la tabla N° 6 que hace referencia a la Operacionalización de las variables.

3.3 Población, muestra y muestreo

Para la presente investigación se tendrá como población al total de incidencias reportadas por los usuarios de la Municipalidad Distrital de Carabayllo con sede palacio municipal acumuladas a la fecha (Primer trimestre del año).

Según (Arias Odon, 2012) manifiesta que “Si la población por el número de unidades que la integran, resulta accesible en su totalidad, no será necesario extraer una muestra”.

Para (Hernandez, y otros, 2010), La muestra es un grupo de personas que están siendo estudiadas, si la población conformada es menor a numero de 50 la población será la misma que la muestra.

Tabla 1: Determinar la Población

Indicador	Población	Tiempo
Detección de acceso no autorizado a la red	Total de incidencias reportadas por los usuarios de la Municipalidad Distrital de Carabayllo	Primer trimestre (de Lunes a Viernes)
Disponibilidad de la red		

Fuente: Elaboración Propia

Los **criterios de inclusión** son características indispensables que deben tener los sujetos de estudio. Como elementos de inclusión se considera cuando dos (2) o más personas no disponen de red durante un tiempo de dos (2) minutos, se considera una caída de red por mala configuración en

los equipos por parte del personal a cargo y cuando por problemas de corriente eléctrica se descomponen un router, switch y antena y/o se apagan o reinician. Es un **criterio de exclusión**, las características que aun cumpliendo los criterios de inclusión, presentan otras características que no deberá tener la muestra. Son consideradas las caídas de la red por falta de corriente eléctrica, el reinicio de switch, routers y antenas por actualización de firmware, el retiro o corte de servicios de equipos alquilados y otros no contemplados como criterio de inclusión.

El muestreo es **no probabilístico**, donde los elementos son elegidos a juicio del investigador. La muestra es **por conveniencia**, los elementos de la población que estudia a los individuos son escogidos en base a juicios preestablecidos y conocimiento del investigador (Carrasco, 2006).

3.4 Técnicas e instrumentos de recolección de datos.

La técnica usada es el fichaje para (Parraguez Simona, y otros 2017) “El fichaje nos permite registrar la información objetiva. Su aplicación requiere de fichas donde se recolectara y organizara la información de acuerdo al carácter de la investigación”.

El instrumento a ser usado es la ficha de registro, formulario por el cual se apuntan los registros de los datos observados durante el experimento (Carrasco, 2006).

Ficha de registro N°01: Detección de acceso no autorizado a la red (Anexo N° 03, Anexo N° 04, Anexo N° 05 y Anexo N° 06)

Ficha de registro N°05: Disponibilidad de la red (Anexo N° 07, Anexo N° 08, Anexo N° 09 y Anexo N° 10)

Tabla 2: Determinación de la técnica e instrumento de recolección de datos

Indicador	Técnica	Instrumento	Fuente	Informante
Detección de acceso no autorizado a la red	Fichaje	Ficha de registro de Datos	Detección de acceso no autorizado a la red	Subgerencia de Tecnología de la Información y Estadística
Disponibilidad de la red			Disponibilidad de la red	

Fuente: Elaboración Propia

3.5 Procedimientos

3.5.1. Recolección de datos

El procedimiento de recolección de datos es mediante el instrumento seleccionado (Ver Anexos N°03 al N°10), el cual es la ficha de registro ya que por medio de este instrumento se tendrá una mejor facilidad de adquisición de datos, estos datos son recolectados dentro de un periodo de 20 días del primer trimestre del año, cuyo informante de la información es la Subgerencia de Tecnología de la Información y Estadística, tomando en consideración los criterios de exclusión e inclusión, para la cual se establece lo siguiente:

- Como primer paso, se tendrá la creación del instrumento con los respectivos indicadores, con el fin de lograr obtener la información detallada del porcentaje de equipos con acceso no autorizado y del porcentaje de disponibilidad.
- Segundo paso, se implementara el instrumento para la recolección de información detallada en los indicadores.

3.5.2. Procesamiento de datos

En esta segunda parte del procesamiento se hace uso del software SPSS versión 26 para el procesamiento de los datos registrados de las fichas de registros (Ver Anexos N°03 al N°10) perteneciente a los

indicadores detección de acceso no autorizado y disponibilidad de red. Mediante estos resultados se sabrá dar solución al problema que radica en la entidad.

3.6 Método de análisis de datos

El análisis de datos es cuantitativo, los datos obtenidos de los instrumentos fueron procesados y evaluados mediante la estadística, y en base a ello, se comprobaron las hipótesis del estudio.

La prueba de normalidad determina si las muestras siguen una distribución normal o no, donde se tendrá en cuenta:

Si:

Sig. < 0.05 adopta la distribución no normal.

Sig. >= 0.05 adopta la distribución normal.

Donde:

Sig.: p- Valor o nivel crítico del contraste

Si el tamaño de una muestra es ($n \geq 51$) la prueba estadística apropiada es KOLMOGOROV SMIRNOV. Cuando la muestra es ($n < 50$) la prueba es SHAPIRO WILK. Para el estudio presente proyecto se hará uso del método de Shapiro Wilk para comprobar la normalidad de las variables, ya que se tiene una muestra menor a 50.

Definición de las variables

DANA_a: Detección de accesos no autorizado a la red

DAR_d: Disponibilidad a nivel de red

Hipótesis Estadística:

Indicador 1:

DANA_a: Detección de accesos no autorizado a la red antes de la implementación del hardening a nivel de red.

DANA_d: Detección de accesos no autorizados a la red después de la implementación del hardening a nivel de red.

Hipótesis de Investigación 1

Hipótesis alterna Ha: La implementación de hardening a nivel de red mejora la detección de acceso no autorizado en la Municipalidad de Carabayllo.

$$HA: DANA_a > DANA_d$$

Hipótesis nula H0: La implementación de hardening a nivel de red no mejora la detección de acceso no autorizado en la Municipalidad de Carabayllo.

$$H0: DANA_a \leq DANA_d$$

Indicador 2:

DAR_a: Disponibilidad a nivel de red antes de la implementación del hardening a nivel de red.

DAR_d: Disponibilidad a nivel de red después de la implementación del hardening a nivel de red.

Hipótesis de Investigación 2

Hipótesis alterna Ha: La implementación de hardening a nivel de red mejora la disponibilidad de la red en la Municipalidad de Carabayllo.

$$HA: DAR_a > DAR_d$$

Hipótesis nula H0: La implementación de hardening a nivel de red no mejorar la disponibilidad de la red en la Municipalidad de Carabayllo

$$H0: DAR_a \leq DAR_d$$

3.7 Aspectos éticos

En este proyecto de investigación se hace referencia de los aspectos éticos que se cumplirán, en relación a lo establecido por la universidad, entidad donde se realiza el estudio y de la autoría de esta investigación.

- El respeto a la propiedad intelectual de los investigadores, autores con respecto a la información recolectada para la investigación.
- El uso de la ISO 690 como directriz para la elaboración de referencias bibliográficas.
- Respetar el reglamento interno dado por la subgerencia de recursos humanos, así como las reglas, directivas o procedimientos establecidos por la Subgerencia de Tecnología de la Información y Estadística de la Municipalidad de Carabayllo.
- Se acordó respetar el presupuesto, no tener gastos innecesarios o no especificados para la implementación de hardening a nivel de red con la entidad.
- Se respetara el principio de la moral, integridad, honestidad y justicia.
- Se acordó el principio de responsabilidad en cuanto a los avances entregables, consejos y otros actos relacionados con la implementación del hardening a nivel de red.

Por último el investigador respetara los resultados, la confiabilidad de los datos brindados por la SGTIE de la Municipalidad Carabayllo.

IV. RESULTADOS

4.1. Análisis Descriptivos

En esta investigación se logró implementar un hardening a nivel de red para poder mejorar la detección de acceso no autorizado a la red y la disponibilidad de la misma para mejorar la seguridad de la información en la municipalidad de Carabayllo; a estos indicadores se aplicó un pre test, se implementó el hardening a nivel de red y se hizo un post test de cada indicador para evaluar la variación de las cantidades y disponibilidad de los indicadores. A continuación se presentan los resultados:

Indicador 1: DANA: Detección de acceso no autorizado a la red

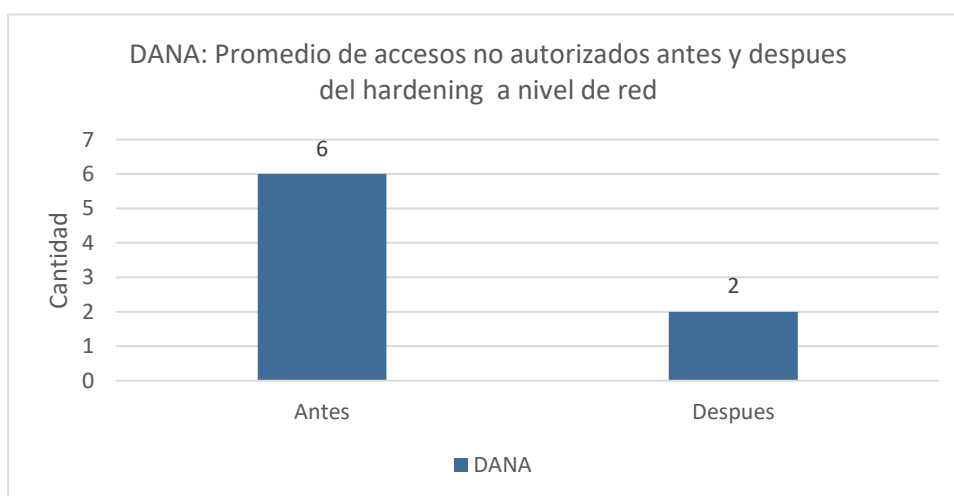
Los resultados de las medidas descriptivas de DANA se muestran en la siguiente tabla:

Tabla 3: Medidas descriptivas de DANA: Detección de acceso no autorizado a la red en pre test y post test

	N	Mínimo	Máximo	Media	Desv. Desviación	Varianza
DANA_antes	10	4	8	5,50	1,179	1,389
DANA_despues	10	1	3	2,20	,632	,400
N válido (por lista)	10					

El indicador DANA: detección de acceso no autorizado a la red, evidencio un promedio de 6 acceso no autorizados para el pretest y 2 accesos no autorizados para el post test lo cual denota una variación del indicador en el antes y después de la implementación del hardening a nivel de red.

Figura 2: DANA: Promedio de accesos no autorizados en pre test y post test



El promedio de accesos no autorizados se redujo de 6 accesos a 2 con la implementación del hardening a nivel de red.

Indicador 2: DR: Disponibilidad de la red

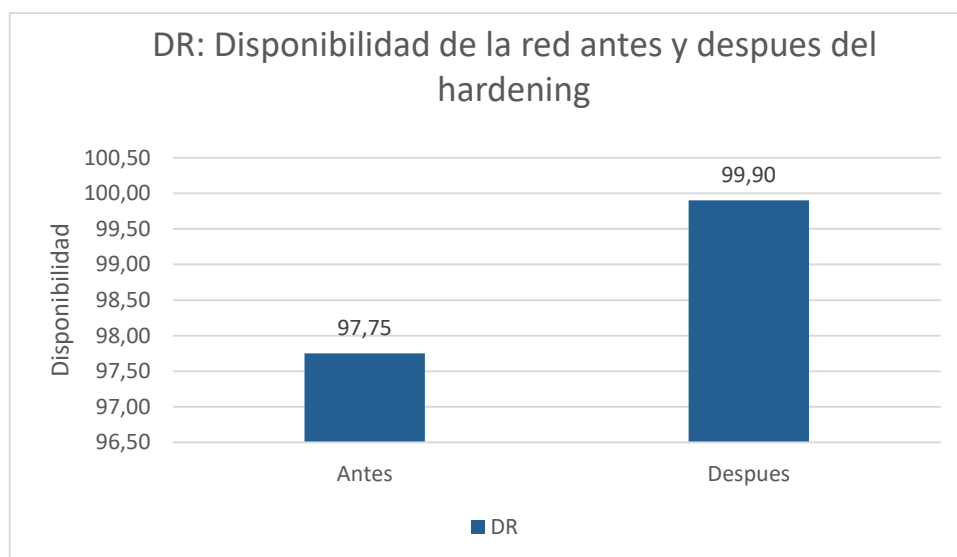
Los resultados de las medidas descriptivas de DR se muestran en la siguiente tabla:

Tabla 4: Medidas descriptivas de DR: Disponibilidad de la red en pre test y post test

Estadísticos descriptivos						
	N	Mínimo	Máximo	Media	Desv. Desviación	Varianza
DRa	10	83.33	100.00	97.7470	5.12392	26,255
DRd	10	98.96	100.00	99.8960	.32888	,108
N válido (por lista)	10					

El indicador DR: disponibilidad de la red, evidencio un promedio de 97.75 de disponibilidad para el pretest y 99.90 de disponibilidad para el post test lo cual denota una variación del indicador en el antes y después de la implementación del hardening a nivel de red. En el pre test el valor mínimo es de 83.33 y en el post test 98.96 de disponibilidad evidenciando la diferencia en el pre con el post test. Corroborándose en la siguiente figura

Figura 3: DR: Disponibilidad de la red en pre test y post test



La disponibilidad de la red aumento de 99.55 a 99.90 con la implementación del hardening a nivel de red.

4.2. Análisis Inferencial

Se realizó la prueba de normalidad para determinar si los datos siguen o no una distribución normal. Siendo la muestra menor a 50 se usó el método Shapiro Wilk, tal como lo indica Hernández y Baptista (2006, p.376) donde se toma en consideración: Si p-valor (nivel de significancia) es menor a 0.05 se considera una distribución no normal y se usara la prueba wilcoxon. Para la presente investigación la prueba de normalidad para los indicadores detección de acceso no autorizado y disponibilidad de red, se utiliza la prueba de Shapiro Wilk ya que nuestra muestra es menor a 50 incidencias.

Indicador: Detección de acceso no autorizado a la red

Con la finalidad de elegir la prueba de hipótesis, los datos recolectados fueron procesados para poder comprobar su comportamiento, determinando si es una distribución normal o no normal.

Tabla 5: Prueba de normalidad - Detección de acceso no autorizado a la red

	Kolmogorov-Smirnov ^a			Shapiro-Wilk		
	Estadístico	gl	Sig.	Estadístico	gl	Sig.
DANA_antes	,236	10	,123	,887	10	,157
DANA_despues	,324	10	,004	,794	10	,012

a. Corrección de significación de Lilliefors

De acuerdo a la tabla de procesos, los resultados indican que el valor Sig de DANA detección de acceso no autorizado en el Pre-test fue de 0.157 (mayor que 0.05), afirmando que es una “distribución normal”. En el Post-test se observa un valor Sig. de 0.12, lo cual, al estar relacionado y al ser menor que 0.05 definen que estos datos se distribuyen de una manera “no normal”.

Indicador: DR disponibilidad de la red

Con la finalidad de elegir la prueba de hipótesis, los datos recolectados fueron procesados para poder comprobar su comportamiento, determinando si es una distribución normal o no normal.

Pruebas de normalidad	
Kolmogorov-Smirnov ^a	Shapiro-Wilk

	Estadístico	gl	Sig.	Estadístico	gl	Sig.
DRa	,413	10	,000	,489	10	,000
DRd	,524	10	,000	,366	10	,000

a. Corrección de significación de Lilliefors

Los resultados mostrados en la tabla anterior indican que el valor Sig. del DR disponibilidad de la red en el pre test fue de 0.00 (menor a 0.05) evidenciando que el DR sigue una distribución no normal. El post test indica un valor Sig. de 0.00 (menor a 0.05) evidenciando una distribución no normal.

4.3. Prueba de Hipótesis

Objetivo específico 01: Controlar el acceso no autorizado a la red del personal, restringiéndolo por áreas. En la Municipalidad de Carabayllo. Asimismo evitando el acceso de intrusos.

Hipótesis Específica 1: La implementación de hardening a nivel de red mejora la confidencialidad en la seguridad de la información en la Municipalidad de Carabayllo

Indicador 1:

DANA_a: Detección de accesos no autorizados antes de la implementación del hardening a nivel de red.

DANA_d: Detección de accesos no autorizados después de la implementación del hardening a nivel de red.

Hipótesis de Investigación 1

Hipótesis alterna Ha: La implementación de hardening a nivel de red mejora la detección de acceso no autorizado en la Municipalidad de Carabayllo.

HA: DANA_a>DANA_d

Hipótesis nula H0: La implementación de hardening a nivel de red no mejora la detección de acceso no autorizado en la Municipalidad de Carabayllo.

H0: DANA_a ≤ DANAd

Estadísticos de prueba^a

	DANA _{despues} - DANA _{antes}
Z	-2,871 ^b
Sig. asintótica(bilateral)	,004

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos positivos.

De acuerdo con los resultados, se rechaza la hipótesis nula y se acepta la hipótesis alterna a un 95 % de confianza. Se concluye que la implementación de hardening a nivel de red mejora la detección de acceso no autorizado en la Municipalidad de Carabayllo.

Objetivo específico 02: Garantizar la accesibilidad a los diferentes servicios de la red sin problemas de lentitud o pérdida de información en la Municipalidad de Carabayllo.

Hipótesis Específica 2: La implementación de hardening a nivel de red mejora la disponibilidad en la seguridad de la información en la Municipalidad de Carabayllo.

Indicador 2:

DR_a: Disponibilidad a nivel de red antes de la implementación del hardening a nivel de red.

DR_d: Disponibilidad a nivel de red después de la implementación del hardening a nivel de red.

Hipótesis de Investigación 2

Hipótesis alterna Ha: La implementación de hardening a nivel de red mejora la disponibilidad de la red en la Municipalidad de Carabayllo.

$$H_A: DR_a > DR_d$$

Hipótesis nula H0: La implementación de hardening a nivel de red no mejorar la disponibilidad de la red en la Municipalidad de Carabayllo

$$H_0: DR_a \leq DR_d$$

Estadísticos de prueba^a

	DRd - DRa
Z	-2,023 ^b
Sig. asintótica(bilateral)	,043

a. Prueba de rangos con signo de Wilcoxon

b. Se basa en rangos negativos.

De acuerdo con los resultados, se rechaza la hipótesis nula y se acepta la hipótesis alterna a un 95 % de confianza. Se concluye que la implementación de hardening a nivel de red mejora la disponibilidad de la red en la Municipalidad de Carabayllo.

V. DISCUSIÓN

En esta investigación se obtuvo que la DANA detección de acceso no autorizado a la red mejoro (disminuyo) a un promedio de 6 accesos en el pre test a 2 accesos no autorizados en el post test con la implementación de hardening a nivel de red y, la DR disponibilidad de la red mejoro (disminuyo) la disponibilidad de 99.75 en el pre test a 99.90 en el post test con la implementación de hardening a nivel de red.

De la misma forma, Sanchez Arias en el 2018, en su estudio titulado “DESARROLLAR LA PROPUESTA DE VIRTUALIZACIÓN DE DISPOSITIVOS DE CONMUTACIÓN PARA OPTIMIZAR LOS SERVICIOS DE LA RED LAN EN EL HOSPITAL NACIONAL EDGARDO REBAGLIATI MARTENS - ESSALUD”, llego a la conclusión, desarrollo la propuesta de los niveles de seguridad de la red LAN a través de reglas, regulaciones y políticas por puerto, vlans y protocolos a fin de mitigar las vulnerabilidades a posibles ataques en la red. Obtuvo como resultado para el indicador seguridad de la red, el diseñó un (1) ACL para sus seis (6) subredes, para el segundo indicador disponibilidad de red se obtuvo un resultado 12 horas y 48 minutos y con el nuevo diseño se redujo a 1 hora y 30 minutos. Por ende la propuesta de virtualización de dispositivos de conmutación optimiza los servicios de la red LAN en el hospital nacional Edgardo rebagliati martens. Con respecto a nuestro indicador se realizó la creación de vlans y se realizaron las regulaciones de políticas de puerto disminuyendo al acceso no autorizado, se mejoró la disponibilidad de la red, aplicando políticas de puerto, reduciendo la tormenta de broadcast. Además se utilizó la metodología SAFE que consiste en modular la red de manera que si una es vulnerada las demás no se ven afectadas.

Farah Miraval en el 2016, en su estudio “MODELO DE IMPLEMENTACIÓN DE REDES VIRTUALES VLAN Y PRIORIZACIÓN DEL ANCHO DE BANDA PARA LA RED DE ÁREA LOCAL DEL PROYECTO ESPECIAL LAGO TITICACA – SEDE CENTRAL PUNO - 2016”.

Obtuvo como resultado para la dimensión rendimiento de la red, mejoro a más del 10 % debido a la incorrecta configuración de equipos, para el indicador latencia se redujo de 329.15 ms a 3.30 ms, para el indicador segmentos de red, vlans de 1 a 21 vlans. Con este modelo se evidencia una mejora significativa en la priorización del ancho de banda para la red de área local del proyecto especial lago Titicaca –sede central. Con respecto a nuestra investigación antes de la implementación no se contaba con VLANS, políticas de puerto, ACL aplicándolos y evidenciando una mejora en los indicadores detección de accesos no autorizados y disponibilidad de la red, aplicando benchmark de CISecurity, guías de buenas prácticas que nos facilitan configuraciones de seguridad en los equipos.

Para Rojas José en el 2018, en su estudio titulado “DISEÑO Y SIMULACIÓN DE UNA RED BASADA EN VLAN’S PARA MEJORAR LA COMUNICACIÓN DE DATOS EN LA EMPRESA GRUPO EL SABER S.A.C”. Obtuvo como resultado para el indicador nivel de seguridad de los dispositivos de comunicación un 0.57 con el diseño que ya existía y de 3.43 posterior al nuevo diseño aumentando el nivel de seguridad de los dispositivos de comunicación en un 83.38 %, para el indicador tiempo promedio en la tormenta de broadcast generados en la red de datos a través de las VLAN’s se concluye que un 72.43 de tiempo promedio de broadcast generados en la red de datos en el pre test y un promedio de tiempo de 2 después de la implementación reduciendo el tiempo promedio en la tormenta de broadcast generados en la red de datos a través de las VLAN’s en un 70.43 con un porcentaje de 97.24 %. La implementación de un diseño y simulación de una red basada en VLAN’s mejoró significativamente la comunicación de datos en la empresa Grupo El Saber S.A.C.

VI. CONCLUSIONES

Se determinó que la implementación de hardening a nivel de red mejoro la seguridad de la información en la municipalidad de Carabayllo, cumpliendo con los objetivos de la presente investigación.

Se determinó que la implementación de hardening a nivel de red disminuyo a un promedio de dos (2) la DANA detección de accesos no autorizados en un periodo de diez (10) días mejorando la seguridad de la información en la municipalidad de Carabayllo.

Se determinó que la implementación de hardening a nivel de red mejoro a un promedio de 99.90% la DR disponibilidad de la red en un periodo de diez (10) días mejorando la seguridad de la información en la municipalidad de Carabayllo.

VII. RECOMENDACIONES

Se recomienda implementar el hardening a nivel de red en toda la entidad, dicho proyecto solo abarca la sede principal de la municipalidad de Carabayllo, suponiendo riesgo de seguridad en las distintas sedes.

Se recomienda seguir la continuación del estudio abarcando el hardening en las siguientes capas del modelo OSI las cuales son, capa de transporte, capa de sesión, capa de presentación y capa de aplicación. Mencionadas capas no fueron abarcadas para este trabajo.

Para el diseño de una red de cualquier tamaño se recomienda seguir una metodología de seguridad en la cual se apliquen guías o buenas prácticas de configuración de los equipos de manera que se mejorara la seguridad de la información.

REFERENCIAS

ALVITRES Grundy, Manuel. Diseño e implementación de una red informática de datos para la Municipalidad Distrital de Cáceres del Perú – Jimbe; 2015. Chimbote: Universidad Católica los Ángeles de Chimbote, 2017.

AGUIRRE Perla y MIGUEL Sergio. Diseño de vlan para la red LAN de la empresa ISS. Mexico D.F: Instituto Politécnico Nacional, Escuela Superior de Ingeniería Mecánica y Eléctrica Unidad Culhuacan, 2010

ARIAS Odón Fidias, 2012. El proyecto de investigación: Introducción a la metodología científica. 6^{ta} ed. Caracas: Editorial Episteme. ISBN 980-07-8525-9

BAENA Paz, Guillermo, 2017. *Metodología de la investigación*. 3^a ed. México: Grupo Editorial Patria ®. ISBN 9786077447481.

CAIZA Ana. Diseño de un proceso de hardening de servidores para una Institución Financiera del Sector Público. Quito: Universidad Internacional SEK, Facultades de Arquitectura e Ingenierías, 2019.

CHICAIZA Garcia, Diego. Estudio de seguridad perimetral informáticas y propuestas de un plan de implementación para la agencia nacional de tránsito. Tesis (Maestría en redes de comunicaciones). Quito: Pontificia Universidad Católica del Ecuador, Facultad de Ingeniería, 2014.

Cisco Press, 2001. High Availability: Network Fundamentals. 1 ed. USA: Cisco Systems. ISBN 1587130173.

CRUZ Oscar. Diseño e implementación de un proceso de hardening. Bogota: Fundación Universitaria los Libertadores, Facultad de Ingeniería y Ciencias Básicas, 2017.

CONGORA Americo y ILIZARBE Ruth. Aplicación del diseño de una red para mejorar la disponibilidad de información de la infraestructura de comunicación en la Municipalidad Distrital Daniel Hernández. Huancavelica: Universidad Nacional de Huancavelica, Facultad de Ingeniería Electrónica, 2018.

DURÁN Raul. Diseño de la Infraestructura física y lógica para una red de área local y extensa (LAN Y WAN) de una PYME. Leganés: Universidad Carlos III de Madrid, Departamento de Informática, 2015.

FACHE Montaña, Jaison. Estudio sobre la aplicación de hardening para mejorar la seguridad informática en el centro técnico laboral de tunja-contel. Tesis (Especialización en Seguridad Informática). Tunja – Colombia: Universidad Nacional Abierta y a Distancia, escuela de ciencias básicas tecnológica e ingeniería, 2016.

FARAH Miraval, Jorge. Modelo de implementación de redes virtuales vlan y priorización del ancho de banda para la red de área local del proyecto especial Lago Titicaca – sede central puno – 2016. Tesis (Título de ingeniero desistemas). Puno: Universidad Nacional del Altiplano, Facultad de Ingeniería Mecánica Eléctrica, Electrónica y Sistemas, 2016.

GUIJARRO Alfonso, YEPEZ Jessica, PERALTA Tania, ORTIZ Mirella. Defensa en profundidad aplicado a un entorno empresarial [en línea]. Vol 39, N° 42, 08 de Junio del 2018 [Fecha de consulta: 30 de Mayo].

GARCIA Frank. Proyecto de rediseño de la red de computadoras del Hospital III José Cayetano Heredia utilizando VLANS. Piura: Universidad Nacional de Piura, Facultad de Ingeniería Industrial, 2018. Quito:

GUIDO Baez. Rediseño de la infraestructura de red para la unidad educativa salesiana “Domingo Comin” aplicando una topología jerárquica redundante con políticas de seguridad perimetral en la red LAN. GUAYAQUIL: Universidad Politécnica Salesiana, 2018.

HUERTAS Yuli y TAPIAS Hector. Diseño e implementación de una metodología de hardening para los servidores, estaciones de trabajo y directorio activo del ministerio de hacienda y crédito público. Tesis (Especialista en Seguridad Informática). Bogotá: Universidad Piloto de Colombia, Facultad de Ingeniería.

JIMÉNEZ Abraham. Una herramienta de gestión de redes virtuales. Mexico D.F: Universidad Autónoma Metropolitana Unidad Azcapotzalco, 2005

JARA Mendoza, Omar. Sistema de gestión de seguridad de la información para mejorar el proceso de gestión del riesgo en un gobierno local, 2018. Tesis (Maestro en ingeniería de sistemas). Perú: Universidad Cesar Vallejo, 2018.

LOPEZ Roldan, Pedro y FACHELLO Sandra, 2015. Metodología de la investigación social cuantitativa. 1 ed. Barcelona: Dipòsit Digital de Documents, Universitat Autònoma de Barcelona.

LÓPEZ Santoyo, Roberto. Propuesta de implementación de auditoria de seguridad informática. Madrid: Universidad Autónoma de Madrid: Escuela politécnica superior, 2015.

MANTEROLA, Carlos, Confiabilidad, presicion o reproducibilidad de las mediciones. Metodo de valoración, utilidad y aplicaciones en la practica clínica, Temuco-Chile. Rev. Chile infectol,(6): 680-688,2018 ISSN: 2017-0022

MARTÍNEZ Cruz, Jency. Endurecimiento (hardening) en dispositivos de red: Routers y switches. Tesis (Especialización en Seguridad Informática). Colombia: Universidad Piloto de Colombia, 2015.

PARAGUEZ Simona y otros, 2017. El estudio y la investigación documental: estrategias metodológicas y herramientas TIC. 1 ed. Chiclayo: Deposito legal en la biblioteca nacional del Perú. ISBN 9786120026038.

RAMÍREZ Leonidas. Rediseño de la Infraestructura de red en una empresa de seguridad privada. Guayaquil: Universidad de Guayaquil, Facultad de Ciencias Matemáticas y Físicas, 2018.

ROJAS Mattos, José. Diseño y Simulación de una red basada en VLAN's para mejorar la comunicación de datos en la empresa Grupo El Saber S.A.C. Tesis (Título de ingeniero de sistemas). Trujillo: Universidad Cesar Vallejo, Facultad de Ingeniería, 2018.

RAMOS Julio, DEL AGUILA Víctor, BAZALAR Ana, 2020. ESTADÍSTICA BÁSICA PARA LOS NEGOCIOS. 1 ed. Lima: Universidad de Lima. ISBN 9789972455230.

SABINO, Carlos. Él proceso de la Investigación (3 era ed.), Argentina, 1996.

SANCHEZ Arias, Raúl. Desarrollar la propuesta de virtualización de dispositivos de conmutación para optimizar los servicios de la red lan en el Hospital Nacional Edgardo Rebagliati Martins – EsSalud. Tesis (Título de ingeniero de sistemas). Lima: Universidad Señor de Sipán, Facultad de Ingeniería, Arquitectura y Urbanismo, 2018.

TIGRE Cortes, Jonathan. Desarrollar el diseño de redes virtuales locales (VLAN) para aislar el tráfico de broadcast. Quito: Universidad Tecnológica Israel, 2012.

VALDERRAMA, Santiago. y LEON, Lucy. Técnicas e datos en la investigación científica.2009,instrumentos para la obtención de datos en la investigación científica ,2009.

VIVEROS Saravia, Johanna. Defensa en profundidad para proteger la información de la red corporativa. [Fecha de consulta: 31 de Mayo].

VIDAL José. Diseño una propuesta de mejoramiento en la Infraestructura de red de datos en la ESPAM MFL con calidad de servicio. Tesis (Maestría en redes de comunicación). Quito: Pontificia Universidad Católica del Ecuador, 2016

YUNGÁN Cazar, Juan. Evaluación del protocolo 802.1q en la implementación de vlans en entornos Wireless mediante la aplicación de software libre. Tesis (Magister en Interconectividad de redes). Riobamba – Ecuador: Escuela Superior Politécnica de Chimborazo, Instituto de Posgrado y Educación Continua, 2016.

YURI Tilio, Davila. Modelo de gestión de servicios de red con RouterOS Mikrotik en la disponibilidad de información de la red de datos de la escuela profesional de ingeniería de sistemas de la universidad nacional de Huancavelica. Tesis (Título de ingeniero de sistemas). Huancavelica: Universidad Nacional de Huancavelica, Facultad de ingeniería electrónica – sistemas, 2019.

Gutierrez del Moral, Leonardo . 2014. *Curso de Ciberseguridad y Hacking Ético*. s.l. : Punto Rojo Libros S.L, 2014. 9788416068531.

ISOTools Excellence. 2017. *¿Seguridad informática o seguridad de la Información?* s.l. : ISOTools Excellence, 2017.

Portela Carvajal, John Sebastian, Rojas Henriquez, Jesús David y Muñoz Araque, Robert Steven. 2020. *Rediseño logico de una red LAN a partir de la Implementación de VLAN, INTER-VLAN ROUTING, DHCP, ACL, Y PortSecurity en un modelo jerarquico de red de tres capas cisco*. Bogotá, Colombia : s.n., 2020.

Zorrilla Mateo, Ramón Eduardo. 2020. *Ciberseguridad sin Destinatario: La Ciberseguridad no es una moda*. 2020. 9945094408; 9789945094404.

ANEXOS

Anexo 1: Tabla de Operacionalización de variables

VARIABLE	DEFINICIÓN CONCEPTUAL	DEFINICIÓN OPERACIONAL	DIMENSIONES	INDICADORES	INSTRUMENTO	ESCALA DE MEDICIÓN
SEGURIDAD DE LA INFORMACIÓN	<p>PARA ISOTOOLS EXCELLENCE (2017), ES LA "DISCIPLINA QUE SE ENCARGA DE LA IMPLEMENTACIÓN TÉCNICA PARA ASEGURAR LA INFORMACIÓN, DESPLEGANDO TECNOLOGÍAS QUE PERMITAN ASEGURAR SITUACIONES DE FALLAS TOTALES O PARCIALES. CON EL FIN DE ASEGURAR LA INTEGRIDAD, DISPONIBILIDAD Y CONFIDENCIALIDAD DEL MANEJO DE LA INFORMACIÓN DE ACTIVOS.</p>	<p>ES UN CONJUNTO DE MEDIDAS, POLÍTICAS Y TÉCNICAS PREVENTIVAS QUE PERMITAN AFRONTAR LOS RIESGOS, PREVENIRLOS EN BÚSQUEDA DE SOLUCIONES PARA PODER CONTENERLOS O MITIGARLO PERMITIENDO CUSTODIAR LA INFORMACIÓN EN BUSCA DE LA DISPONIBILIDAD, INTEGRIDAD Y CONFIDENCIALIDAD DE LA INFORMACIÓN.</p>	CONFIDENCIALIDAD DE LA RED	DETECCIÓN DE ACCESO NO AUTORIZADO A LA RED	FICHA DE REGISTRO DE DATOS	RAZÓN / CONTINUA
			DISPONIBILIDAD DE LA RED	DISPONIBILIDAD DE LA RED		

Anexo 2: Tabla de categorización

Problema	Objetivo	Categoría	Subcategoría	Código
P.G: La no planificación de un posible aumento de equipos tecnológicos ha generado una saturación de los puntos de red, instalando equipos de interconexión de red domésticos que por error involuntarios viene generando bucles y tormenta de emisiones saturando la red, el personal trae sus propios equipos haciendo uso de los recursos de la red cuando no cuentan con autorización de sus jefes evidenciando la vulnerabilidad en la red de la municipalidad de Carabayllo	O.G: Gestionar de forma correcta la seguridad de la información a nivel de red en la Municipalidad de Carabayllo; para lo cual se rediseñara la red dotándola de mayores niveles de seguridad.	Sector Publico	Municipalidad Distrital de Carabayllo	20 GOBIERNO REGIONAL, LOCAL Código de unidad ejecutora Carabayllo 301255
P.G 01: El personal de la entidad hace uso indebido de los recursos de red (servicio de internet, servicios de impresión y otros) sin autorización de los jefes inmediatos en la Municipalidad de Carabayllo.	O.E 01: Controlar el acceso no autorizado a la red del personal, restringiéndolo por áreas. En la Municipalidad de Carabayllo. asimismo evitando el acceso de intrusos			
P.G 02: Uso indebido de dispositivos de interconexión de redes ocasionando pérdida de paquete de datos, inaccesibilidad y lentitud de los diferentes servicio de redes que brinda la Municipalidad de Carabayllo.	O.E 02: Garantizar la accesibilidad a los diferentes servicios de la red sin problemas de lentitud o pérdida de información en la Municipalidad de Carabayllo.			

Fuente: Elaboración Propia

Anexo 3: Ficha de Registro de datos del indicador Acceso no autorizado a la red, correspondiente al mes de enero

FICHA DE REGISTRO DE DATOS			
Institución	Universidad Cesar Vallejo	Tipo de Prueba	PRE TEST
Investigador(es)	Ebel Aldair Chinchay Toribio		
Dimensión	Confidencialidad de la Red		
Fecha de Inicio	03/01/2022	Fecha Final	28/01/2022
Formula		Medida	Cantidad
$ANAR = \sum NANA$ ANAR= Acceso no autorizados a la red NANA=Numero de accesos no autorizado		Variable Indicador	Detección de acceso no autorizado a la red
N°	Fecha	Accesos no autorizados a la red	
01	03/01/2022	8	
02	04/01/2022	5	
03	05/01/2022	4	
04	06/01/2022	6	
05	07/01/2022	7	
06	10/01/2022	6	
07	11/01/2022	6	
08	12/01/2022	4	
09	13/01/2022	7	
10	14/01/2022	5	
11	17/01/2022	6	
12	18/01/2022	4	
13	19/01/2022	3	
14	20/01/2022	3	
15	21/01/2022	7	
16	24/01/2022	9	
17	25/01/2022	6	
18	26/01/2022	4	
19	27/01/2022	5	
20	28/01/2022	5	

Anexo 4: Ficha de Registro de datos del indicador Acceso no autorizado a la red, correspondiente al mes de febrero.

FICHA DE REGISTRO DE DATOS						
Institución	Universidad Cesar Vallejo		Tipo de Prueba		PRE TEST	
Investigador	Ebel Aldair Chinchay Toribio					
Dimensión	Disponibilidad de la red					
Fecha de Inicio	01/02/22			Fecha Final	28/02/22	
Formula	$PD = \frac{(D - TF)}{D} \times 100$ PD= Porcentaje de disponibilidad de la red. D = Disponibilidad TF = Tiempo de falias			Medida	Porcentaje	
				Indicador	Disponibilidad de la red	
N°	Fecha	Hora - Inicio	Hora - Fin	Tiempo de Falias (horas)	Disponibilidad (Horas)	Disponibilidad de la red
01	01/02/22	8:00	8:40	0.67	24	97.21
02	02/02/22	8:00	8:40	0.67	24	97.21
03	03/02/22	8:00	8:40	0.67	24	97.21
04	04/02/22	8:00	12:00	4	24	83.33
05	07/02/22	8:00	8:40	0.67	24	97.21
06	08/02/22	8:00	8:40	0.67	24	97.21
07	09/02/22	8:00	8:40	0.67	24	97.21
08	10/02/22	8:00	8:40	0.67	24	97.21
09	11/02/22	—	—	0	24	100
10	14/02/22	—	—	0	24	100
11	15/02/22	8:00	10:00	2	24	91.67
12	16/02/22	—	—	0	24	100
13	17/02/22	8:15	8:40	0.42	24	98.25
14	18/02/22	—	—	0	24	100
15	21/02/22	—	—	0	24	100
16	22/02/22	—	—	0	24	100
17	23/02/22	—	—	0	24	100
18	24/02/22	2:15	2:35	0.33	24	98.63
19	25/02/22	4:40	4:55	0.25	24	98.96
20	28/02/22	—	—	0	24	100

Anexo 5: Ficha de Registro de datos del indicador Acceso no autorizado a la red, correspondiente al mes de marzo.

FICHA DE REGISTRO DE DATOS			
Institución	Universidad Cesar Vallejo	Tipo de Prueba	PRE TEST
Investigador(es)	Ebel Aldair Chinchay Toribio		
Dimensión	Confidencialidad de la red		
Fecha de Inicio	01/03/2022	Fecha Final	28/03/2022
Formula		Medida	Cantidad
$ANAR = \sum^{SANA}$ ANAR= Acceso no autorizados a la red NANA= Numero de accesos no autorizado		Variable Indicador	Detección de acceso no autorizado a la red
Nº	Fecha	Accesos no autorizados a la red	
01	01/03/2022	5	
02	02/03/2022	6	
03	03/03/2022	7	
04	04/03/2022	5	
05	07/03/2022	5	
06	08/03/2022	6	
07	09/03/2022	6	
08	10/03/2022	5	
09	11/03/2022	4	
10	14/03/2022	7	
11	15/03/2022	6	
12	16/03/2022	4	
13	17/03/2022	8	
14	18/03/2022	6	
15	21/03/2022	4	
16	22/03/2022	6	
17	23/03/2022	5	
18	24/03/2022	5	
19	25/03/2022	5	
20	28/03/2022	6	

Anexo 6: Ficha de Registro de datos del indicador Acceso no autorizado a la red, correspondiente al mes de abril.

FICHA DE REGISTRO DE DATOS			
Institución	Universidad Cesar Vallejo	Tipo de Prueba	PRE TEST
Investigador(es)	Ebel Aldair Chinchay Toribio		
Dimensión	Confidencialidad de la Red		
Fecha de Inicio	01/04/2022	Fecha Final	28/04/2022
Formula		Medida	Cantidad
$ANAR = \sum SANA$ ANAR= Acceso no autorizados a la red NANA=Numero de accesos no autorizado		Variable Indicador	Detección de acceso no autorizado a la red
N°	Fecha	Accesos no autorizados a la red	
01	01/04/2022	6	
02	04/04/2022	7	
03	05/04/2022	6	
04	06/04/2022	5	
05	07/04/2022	5	
06	08/04/2022	6	
07	11/04/2022	6	
08	12/04/2022	5	
09	13/04/2022	5	
10	14/04/2022	-	
11	15/04/2022	-	
12	18/04/2022	6	
13	19/04/2022	5	
14	20/04/2022	6	
15	21/04/2022	6	
16	22/04/2022	7	
17	25/04/2022	6	
18	26/04/2022	8	
19	27/04/2022	5	
20	28/04/2022	5	

Anexo 7: Ficha de Registro de datos del indicador Disponibilidad de la red, correspondiente al mes de enero

FICHA DE REGISTRO DE DATOS						
Institución	Universidad Cesar Vallejo		Tipo de Prueba		PRE TEST	
Investigador	Ebel Aldair Chinchay Torbio					
Dimensión	Disponibilidad de la red					
Fecha de Inicio	03/01/22		Fecha Final		28/01/22	
Fórmula			Medida		Porcentaje	
$PD = \frac{(D - TF)}{D} \times 100$ <p>PD = Porcentaje de disponibilidad de la red. D = Disponibilidad TF = Tiempo de fallas</p>			Indicador		Disponibilidad de la red	
N°	Fecha	Hora - Inicio	Hora - Fin	Tiempo de Fallas (horas)	Disponibilidad (Horas)	Disponibilidad de la red
01	03/01/22	08:00	12:00	4	24	83.33
02	04/01/22	11:00	11:40	0.67	24	97.21
03	05/01/22	—	—	0	24	100
04	06/01/22	09:00	09:15	0.25	24	98.96
05	07/01/22	—	—	0	24	100
06	10/01/22	—	—	0	24	100
07	11/01/22	—	—	0	24	100
08	12/01/22	11:00	11:30	0.50	24	97.92
09	13/01/22	8:30	9:10	0.67	24	97.91
10	14/01/22	—	—	0	24	100
11	17/01/22	—	—	0	24	100
12	18/01/22	—	—	0	24	100
13	19/01/22	08:30	8:50	0.33	24	98.63
14	20/01/22	—	—	0	24	100
15	21/01/22	—	—	0	24	100
16	24/01/22	09:30	10:30	2	24	91.67
17	25/01/22	—	—	0	24	100
18	26/01/22	—	—	0	24	100
19	27/01/22	02:30	02:45	0.25	24	98.96
20	28/01/22	08:10	08:25	0.25	24	98.96

Anexo 8: Ficha de Registro de datos del indicador Disponibilidad de la red, correspondiente al mes de febrero

FICHA DE REGISTRO DE DATOS						
Institución	Universidad Cesar Vallejo		Tipo de Prueba		PRE TEST	
Investigador	Ebel Aldair Chinchay Torbio					
Dimensión	Disponibilidad de la red					
Fecha de Inicio	01/02/22			Fecha Final	28/02/22	
Formula				Medida	Porcentaje	
$PD = \frac{(D - TF)}{D} \times 100$ <p>PD= Porcentaje de disponibilidad de la red. D = Disponibilidad TF = Tiempo de fallas</p>				Indicador	Disponibilidad de la red	
N°	Fecha	Hora - Inicio	Hora - Fin	Tiempo de Fallos (horas)	Disponibilidad (Horas)	Disponibilidad de la red
01	01/02/22	8:00	8:40	0.67	24	97.21
02	02/02/22	8:00	8:40	0.67	24	97.21
03	03/02/22	8:00	8:40	0.67	24	97.21
04	04/02/22	8:00	12:00	4	24	83.33
05	07/02/22	8:00	8:40	0.67	24	97.21
06	08/02/22	8:00	8:40	0.67	24	97.21
07	09/02/22	8:00	8:40	0.67	24	97.21
08	10/02/22	8:00	8:40	0.67	24	97.21
09	11/02/22	—	—	0	24	100
10	14/02/22	—	—	0	24	100
11	15/02/22	8:00	10:00	2	24	91.67
12	16/02/22	—	—	0	24	100
13	17/02/22	8:15	8:40	0.42	24	98.25
14	18/02/22	—	—	0	24	100
15	21/02/22	—	—	0	24	100
16	22/02/22	—	—	0	24	100
17	23/02/22	—	—	0	24	100
18	24/02/22	2:15	2:35	0.33	24	98.63
19	25/02/22	4:40	4:55	0.25	24	98.96
20	28/02/22	—	—	0	24	100

Anexo 9: Ficha de Registro de datos del indicador Disponibilidad de la red, correspondiente al mes de marzo

FICHA DE REGISTRO DE DATOS						
Institución	Universidad Cesar Vallejo		Tipo de Prueba		Pbc TEST	
Investigador	Ebel Aldair Chinchay Toribio					
Dimensión	Disponibilidad de la red					
Fecha de Inicio	01/03/22			Fecha Final	28/03/22	
Formula				Medida		
$PD = \frac{(D - TF)}{D} \times 100$ PD= Porcentaje de disponibilidad de la red. D = Disponibilidad TF = Tiempo de falas				Indicador		
				Disponibilidad de la red		
N°	Fecha	Hora - Inicio	Hora - Fin	Tiempo de Falas (horas)	Disponibilidad (Horas)	Disponibilidad de la red
01	01/03/22	—	—	0	24	100
02	02/03/22	—	—	0	24	100
03	03/03/22	—	—	0	24	100
04	04/03/22	8:10	8:40	0.50	24	97.92
05	07/03/22	8:00	8:20	0.33	24	98.63
06	08/03/22	—	—	0	24	100
07	09/03/22	4:00	4:20	0.33	24	98.63
08	10/03/22	—	—	0	24	100
09	11/03/22	4:30	4:45	0.25	24	98.96
10	14/03/22	8:00	12:00	4	24	83.33
11	15/03/22	9:15	9:30	0.25	24	98.96
12	16/03/22	—	—	0	24	100
13	17/03/22	—	—	0	24	100
14	18/03/22	11:20	11:35	0.25	24	98.96
15	21/03/22	—	—	0	24	100
16	22/03/22	—	—	0	24	100
17	23/03/22	—	—	0	24	100
18	24/03/22	5:00	5:15	0.25	24	98.96
19	25/03/22	9:00	9:30	0.50	24	97.92
20	28/03/22	—	—	0	24	100

Anexo 10: Ficha de Registro de datos del indicador Disponibilidad de la red, correspondiente al mes de abril

FICHA DE REGISTRO DE DATOS						
Institución	Universidad Cesar Vallejo		Tipo de Prueba		Pre TEST	
Investigador	Ebel Aldair Chinchay Torbio					
Dimensión	Disponibilidad de la red					
Fecha de inicio	01/04/22			Fecha Final	28/04/22	
Formula				Medida	Disponibilidad de la red	
$PD = \frac{(D - TF)}{D} \times 100$ <p>PD= Porcentaje de disponibilidad de la red. D = Disponibilidad TF = Tiempo de fallas</p>				Indicador		
N°	Fecha	Hora - Inicio	Hora - Fin	Tiempo de Fallas (horas)	Disponibilidad (Horas)	Disponibilidad de la red
01	01/04/22	—	—	0	24	100
02	04/04/22	8:15	8:35	0.33	24	98.63
03	05/04/22	11:00	11:30	0.50	24	97.92
04	06/04/22	—	—	0	24	100
05	07/04/22	—	—	0	24	100
06	08/04/22	09:00	09:15	0.25	24	98.96
07	11/04/22	—	—	0	24	100
08	12/04/22	—	—	0	24	100
09	13/04/22	—	—	0	24	100
10	14/04/22	—	—	—	24	—
11	15/04/22	—	—	—	24	—
12	18/04/22	8:00	8:15	0.25	24	98.96
13	19/04/22	04:00	4:15	0.25	24	98.96
14	20/04/22	—	—	0	24	100
15	21/04/22	—	—	0	24	100
16	22/04/22	—	—	0	24	100
17	25/04/22	10:00	10:20	0.33	24	98.63
18	26/04/22	05:20	5:40	0.33	24	98.63
19	27/04/22	—	—	0	24	100
20	28/04/22	—	—	0	24	100

Anexo 12: CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE: Disponibilidad de la red



UNIVERSIDAD CÉSAR VALLEJO

1. CERTIFICADO DE VALIDEZ DE CONTENIDO DEL INSTRUMENTO QUE MIDE: Disponibilidad de la red

Nº	DIMENSIONES / ítems	Pertinencia ¹		Relevancia ²		Claridad ³		Sugerencias
		Si	No	Si	No	Si	No	
	DIMENSIÓN 2: Disponibilidad a nivel de red							
1	INDICADORES: Disponibilidad de la red							
a	Es formulado con lenguaje apropiado.	Si		Si		Si		
b	Es adecuado el avance, la ciencia y tecnología.	Si		Si		Si		
c	Existe una organización lógica.	Si		Si		Si		
d	Adecuado para valorar los aspectos del sistema metodológico y científico.	Si		Si		Si		
e	Está basado en aspectos teóricos y científicos.	Si		Si		Si		
f	En los datos respecto al indicador.	Si		Si		Si		
g	Responde al propósito de investigación.	Si		Si		Si		
h	El instrumento es adecuado al tipo de investigación.	Si		Si		Si		

Observaciones (precisar si hay suficiencia): _____

Opinión de aplicabilidad: **Aplicable** **Aplicable después de corregir** **No aplicable**

Apellidos y nombres del juez validador: Ebel Ndaw Chunday Torino DNI: 74010662

Especialidad del validador: _____

¹**Pertinencia:** El ítem corresponde al concepto teórico formulado.
²**Relevancia:** El ítem es apropiado para representar al componente o dimensión específica del constructo.
³**Claridad:** Se entiende sin dificultad alguna el enunciado del ítem, es conciso, exacto y directo.

Nota: Suficiencia, se dice suficiencia cuando los ítems planteados son suficientes para medir la dimensión.

17 de 12 del 2021

Firma del Experto Informante.



TABLA DE EVALUACIÓN

Apellidos y Nombres del Experto: Ebel Aldair Chinchay Toriblo
 Título y/o Grado Académico: Estudiante

Doctor () Magister () Ingeniero () Licenciado () Otro Estudiante

TESIS: "Implementación de hardening a nivel de red para mejorar la seguridad de la información en la municipalidad de Carabaylo, 2021"

Autores: Chinchay Toriblo Ebel Aldair.

MUY MAL (1) MALO (2) REGULAR (3) BUENO (4) EXCELENTE (5)

Mediante la tabla de evaluación de expertos usted tiene la facultad de evaluar la metodología de desarrollo de software involucrado mediante una serie de preguntas con puntuaciones especificadas al final de la tabla. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de las preguntas.

ÍTEM	PREGUNTAS	METODOLOGÍA			
		Top-Down Network Desing	PPDIOO	James MacCabe	Cormac Long
1	Capacidad de adaptarse a cualquier ámbito de trabajo	3	5	2	1
2	Facilidad para el despliegue de la red	2	4	2	2
3	Enfoque empresarial	4	5	1	2
4	Disponibilidad y optimización de servicios de red	3	4	2	2
5	La implementación en base a un análisis de requerimiento	5	4	3	2
PUNTUACIÓN		17	22	10	9
SUGERENCIAS					
FIRMA DEL EXPERTO					



TABLA DE VALIDACIÓN DEL INSTRUMENTO: Detección de acceso no autorizado a la red

I. DATOS GENERALES

Apellidos y Nombres del Experto: Chinchay Toribio Ebel Aldair
 Título y/o Grado Académico:

Doctor () Magister () Ingeniero () Licenciado () Otro () Estudiante

Universidad que labora:

Fecha:

17/12/2021

TESIS : Implementación de hardening a nivel de red para mejorar la seguridad de la información en la municipalidad de Carabaylo, 2021

Autor(es): Chinchay Toribio, Ebel Aldair

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

INDICADOR	CRITERIO	VALORACIÓN				
		0-20%	21-50%	51-70%	71-80%	81-100%
CLARIDAD	Es formulado con lenguaje apropiado.				80%	
OBJETIVIDAD	Esta expresado en conducta observable.				80%	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.				80%	
ORGANIZACIÓN	Existe una organización lógica.				80%	
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.				80%	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				80%	
CONSISTENCIA	Está basado en aspectos teóricos y científicos.				80%	
COHERENCIA	En los datos respecto al indicador.				80%	
METODOLOGÍA	Responde al propósito de investigación.				80%	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.				80%	
TOTAL PROMEDIO					80%	

III. PROMEDIO DE VALIDACIÓN

IV. OPCIÓN DE APLICABILIDAD

- El instrumento puede ser aplicado, tal como está elaborado
 El instrumento debe ser mejorado antes de ser aplicado

FIRMA DEL EXPERTO

Chinchay Toribio



TABLA DE VALIDACIÓN DEL INSTRUMENTO: Disponibilidad de la red

I. DATOS GENERALES

Apellidos y Nombres del Experto: Chinchay Toribio Ebel Aldair
 Título y/o Grado Académico:

Doctor () Magister () Ingeniero () Licenciado () Otro () Estudiante

Universidad que labora:

Fecha: 17/12/2021

TESIS : Implementación de hardening a nivel de red para mejorar la seguridad de la información en la municipalidad de Carabaylo, 2021

Autor(es): Chinchay Toribio, Ebel Aldair

Deficiente (0-20%) Regular (21-50%) Bueno (51-70%) Muy Bueno (71-80%) Excelente (81-100%)

Mediante la evaluación de expertos usted tiene la facultad de calificar la tabla de validación del instrumento involucrado mediante una serie de indicadores con puntuaciones especificadas en la tabla, con la valoración de 0% - 100%. Asimismo, se exhorta a las sugerencias de cambio de ítems que crea pertinente, con la finalidad de mejorar la coherencia de los indicadores para su valoración.

II. ASPECTOS DE VALIDACIÓN

INDICADOR	CRITERIO	VALORACIÓN				
		0-20%	21-50%	51-70%	71-80%	81-100%
CLARIDAD	Es formulado con lenguaje apropiado.				80%	
OBJETIVIDAD	Esta expresado en conducta observable.				80%	
ACTUALIDAD	Es adecuado el avance, la ciencia y tecnología.				80%	
ORGANIZACIÓN	Existe una organización lógica.				80%	
SUFICIENCIA	Comprende los aspectos de cantidad y calidad.				80%	
INTENCIONALIDAD	Adecuado para valorar los aspectos del sistema metodológico y científico.				80%	
CONSISTENCIA	Está basado en aspectos teóricos y científicos.				80%	
COHERENCIA	En los datos respecto al indicador.				80%	
METODOLOGÍA	Responde al propósito de investigación.				80%	
PERTENENCIA	El instrumento es adecuado al tipo de investigación.				80%	
TOTAL					80%	

III. PROMEDIO DE VALIDACIÓN

[Empty box for average validation]

IV. OPCIÓN DE APLICABILIDAD

- El instrumento puede ser aplicado, tal como está elaborado
 El instrumento debe ser mejorado antes de ser aplicado

FIRMA DEL EXPERTO

INTRODUCCIÓN

1.1. Sector Público

El sector público. Es el conjunto de organismos administrativos mediante los cuales el Estado cumple o hace cumplir la política o voluntad expresada en las leyes fundamentales del país, incluye a los órganos administrativos de los poderes legislativo, ejecutivo y judicial, y organismos públicos autónomos.

1.2. Descripción general de la entidad

La Municipalidad Distrital del Carabaylo, por su naturaleza es un Gobierno Local que emana de la voluntad popular. Tiene personería jurídica de derecho público con autonomía política, económica y administrativa en los asuntos de su competencia, ejerce funciones y atribuciones que le señalan la Constitución y la Ley Orgánica de Municipalidades N° 27972.

Conforme a la Ley de Bases de la Descentralización, ejerce con carácter exclusivo o compartido sus competencias. Cumple función Promotora, Normativa y Reguladora, así como de Ejecución, Fiscalización y Control, de acuerdo a lo estipulado en el Capítulo I, Título V de la Ley Orgánica de Municipalidades N° 27972.

1.3. Breve descripción de la empresa

En la Tabla N° 8 se muestra la consulta RUC de la Municipalidad Distrital de Carabaylo

Tabla 6: Consulta RUC

Número de RUC	20131368314 - MUNICIPALIDAD DISTRITAL DE CARABAYLLO
Tipo Contribuyente	GOBIERNO REGIONAL, LOCAL
Nombre Comercial	-
Fecha de Inscripción	04/05/1993

Fecha Inicio de Actividades	04/05/1993
Estado Contribuyente	ACTIVO
Condición del Contribuyente	HABIDO
Dirección del Domicilio Fiscal	Av. TÚPAC AMARU NRO 1733 (P.J. RAUL PORRAS BARRENECHEA) Lima – LIMA - CARABAYLLO
Sistema de Emisión de Comprobante:	MANUAL / MECANIZADO
Actividad de Comercio Exterior:	SIN ACTIVIDAD
Sistema de Contabilidad:	MANUAL
Actividad(es) Económica(s)	Principal – 8411 - ACTIVIDADES DE LA ADMINISTRACIÓN PÚBLICA EN GENERAL.
Comprobante de Pago c/ aut. de impresión (F. 806 u 816):	FACTURA
Sistema de Emisión Electrónica:	-
Afiliado al PLE desde:	-
Padrones:	NINGUNO

Fuente: Sunat

La Municipalidad Distrital de Carabaylo se ubica en la Av. Túpac Amaru N° 1733 (P.J. Raúl Porras Barrenechea), Carabaylo –Lima. Para facilitar su ubicación se muestra en la figura 1 un croquis referencial.

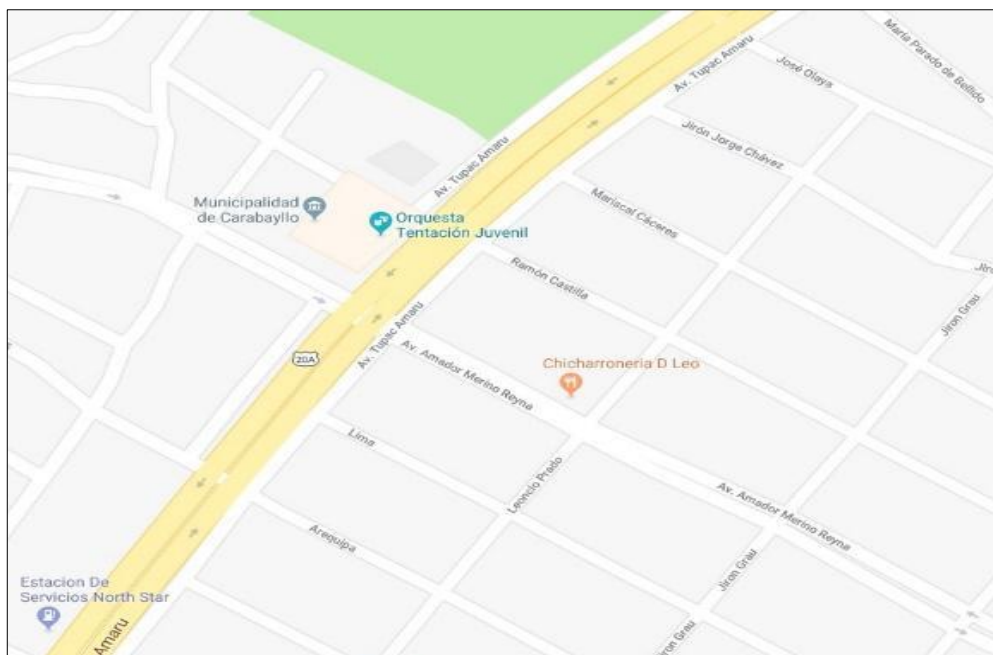


Figura 4: Ubicación de la Municipalidad Distrital de Carabaylo

Ficha técnica del distrito	
Ubicación	Noreste de la provincia de Lima, en el valle del río Chillón.
Límites	Noroeste: Distrito de Ancón Noreste: Distrito de Santa Rosa de Quives; provincia de Canta. Este: Distrito de San Antonio de Chaclla; provincia de Huarochirí y con el distrito de San Juan de Lurigancho. Sureste: Distrito de Comas y Puente Piedra.
Coordinaciones	Latitud Sur: 11°, 10',09" y 11°,54', 22" Oeste: 76°, 48', 11" y 77°, 05', 29"
Altura	Desde los 200 m s.n.m. hasta los 530 m s.n.m.
Clima	Clima árido y semicálido, con una temperatura promedio de 18° C; en la época de invierno hay presencia de nieblas bajas que cubren el valle.
Población según el INEI (2011)	257,325 Habitantes

Figura 5: Ficha técnica de la MDC

La MDC cuenta con siete (7) sedes y el Palacio Municipal, lugar en el cual se encuentra concentrado la mayor cantidad de personal administrativo, Operativo y Ejecutivo de la entidad. Las sedes se interconectan por medio de radio enlaces, por el cual pasa tráfico de datos voz y video.

Organización de la empresa

En la figura N°4 se presenta el organigrama de la Municipalidad Distrital de Carabayllo

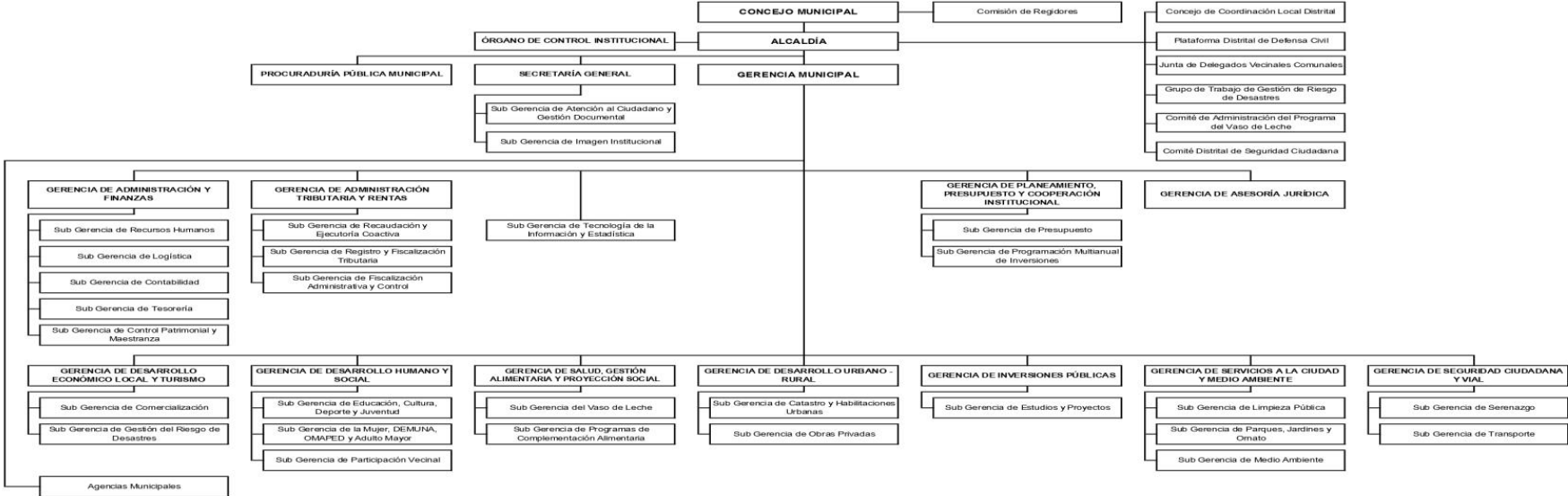


Figura 6: Organigrama

1.4. Metodología de desarrollo del hardening

La metodología PPDIOO permite formalizar el ciclo de vida de una red en seis etapas: Preparación, Planificación, Diseño, Implementación, Operación y Optimización. Cada una de las fases cumple con su función específica y se relacionan con su antecesora. El alcance de esta implementación abarca las 4 primeras fases: Preparación, Planificación, Diseño e Implementación.

PREPARACIÓN: Esta fase nos permite definir las características técnicas de la red de la MDC. Estas características comprenden a los usuarios, aplicaciones, servicios, equipos y los medios de transmisión. Información obtenida a través de entrevista al personal de la SGTIE, los resultados de la aplicación de esta fase se encuentran descritos en la sección 1.2.

PLANIFICACIÓN: Esta fase involucra el análisis de la red actual y la definición de los requerimientos de la entidad. El análisis se realizara en base al modelo SAFE y los benchmarks de CISecurity. El modelo SAFE se utilizara para el análisis de la arquitectura de red y los benchmarks se aplicaran para la evaluación de los elementos activos y terminales. Los requerimientos serán obtenidos como producto de análisis de la situación actual. El diseño de esta fase se describe en el capítulo 2.

DISEÑO: Esta fase involucra el diseño de la red de datos de la MDC, el diseño se desarrolla en base al análisis realizado y los requerimientos obtenidos en la fase anterior. El desarrollo de esta fase se desarrolla en el capítulo 3.

IMPLEMENTACIÓN: En esta fase se involucra todas las fases anteriores, aquí se pone en marcha el diseño de la red.

1.5. Herramientas

Para el desarrollo de la tesis se utilizan dos herramientas: el modelo de seguridad para redes de empresa SAFE de cisco y los benchmarks de CISecurity. Herramientas que nos permitirán realizar el análisis y diseño de la red MDC. El modelo SAFE se utilizara para el análisis y diseño de la arquitectura de red. Los benchmarks de CISecurity se utilizaran para evaluar la configuración de seguridad de los elementos activos y terminales de red, y definir la configuración que deberían presentar los dispositivos en este nuevo diseño e implementación.

1.6. Modelo de seguridad para redes de empresas SAFE

El modelo de seguridad SAFE define una arquitectura modular que integra toda la red de una organización, incluyendo campus, centro de datos, WAN, las sucursales y el personal que realiza el trabajo fuera de la institución. SAFE divide la red en áreas funcionales conocidas como módulos. Para cada módulo analiza su funcionalidad, arquitectura física y lógica, las amenazas de seguridad y los medios para combatirlas. La arquitectura modular permite que el fallo de un sistema de seguridad de un módulo no ponga en peligro a los demás módulos de red.

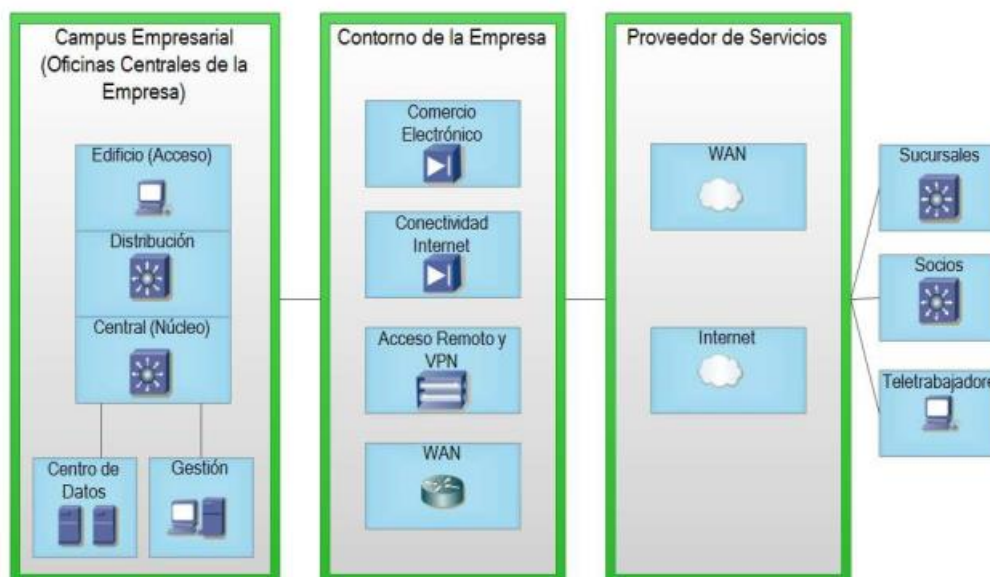


Figura 7: Arquitectura modular de SAFE

1.7. Benchmark de CISecurity

Conjunto de buenas prácticas de seguridad que definen la configuración que deberían presentar los dispositivos, los benchmark especifican los procedimientos para implementar estas buenas prácticas, y los procedimientos de auditoría que verifican si esas se están implementando correctamente.

I. FASE PREPARACIÓN

1.2 Caracterización de la organización

Esta descripción de la red de datos de la MDC se hace con el objetivo de conocer su estructura tecnológica.

1.2.1 Introducción a la red MDC

La red de datos de la Municipalidad Distrital de Carabayllo (al cual a partir de este punto nos referimos como “MDC”), fue implementado hace 12 años. Diseñada para brindar un soporte a los usuarios de los diferentes unidades orgánicas. A continuación se presentan las características con las que cuenta la red de la MDC.

USUARIOS

La red de la MDC presenta usuarios internos, que se encuentran laborando dentro de las diferentes sedes, unidades orgánicas. Los usuarios internos son aproximadamente 450 personas.

APLICACIONES Y SERVICIOS

Las aplicaciones y servicios que ofrece la red de la MDC son utilizados por usuarios internos. Las aplicaciones son de tipo escritorio y web las cuales se encuentran alojados en el centro de datos. Las principales aplicaciones son: SISMUN, SIAF, SIGA WEB, SIGA MEF, SISGEDO, entre otros. Los servicios de mayor uso son correo institucional, internet.

EQUIPOS Y DISPOSITIVOS DE RED

Para ofrecer los servicios y aplicaciones en la red de la MDC se tienen desplegadas los siguientes equipos y dispositivos de red.

- 450 computadoras
- 70 impresoras de red
- 12 servidores
- 10 cámaras de video vigilancia
- Un IPS
- 16 switch

MEDIOS DE TRANSMISIÓN

La red de la MDC cuenta con un medio de transmisión guiado. En los medios de comunicación guiados se utiliza dos tipos de cable: Fibra óptica y cable UTP categoría 6 y 5e. El cableado de la fibra óptica es utilizado verticalmente o backbone. El cableado horizontal se extiende a través de toda el área de trabajo

de cada piso hacia el centro de telecomunicación ubicado en el mismo piso; el cableado vertical se extiende desde el cuarto de comunicación de cada piso hasta el cuarto principal (DATACENTER) de interconexión ubicado en el cuarto piso.

Los terminales se conectan a los switches ubicados en los centros de comunicación mediante cable UTP categoría 6 y 5e. Los switches ubicados en los centros de comunicación se conectan al switch core ubicado en el datacenter mediante fibra óptica.

1.3 Definición del problema

El diseño de la red de la MDC no garantiza la seguridad y disponibilidad, debido a un conjunto de problemas organizacionales y tecnológicos que se presentan a continuación.

1.3.1 Problemas organizacionales

Los problemas en la entidad surgen a causa de que el diseño actual no ha seguido un conjunto de buenas prácticas en su implementación. El personal técnico y administrativo de la municipalidad tampoco ha definido políticas que limiten el mal uso de los recursos informáticos. Los problemas organizacionales son:

No aplican configuración al modelo del diseño de la red.

Para el diseño de la red en la MDC se siguió el modelo jerárquico de Cisco el cual consta de tres capas, desde que la red fue implementada se realizaron una serie de cambios el cual no ha ido siguiendo ninguna buena práctica. En las capas de distribución y acceso no se realizaron ningún tipo de configuración que pueda mejorar la seguridad y el rendimiento de la red, mientras que en la capa de núcleo se realizaron configuraciones mínimas. Teniendo un ataque de tipo ransomware (Ataque stop ransomware variante djvu.pulsar1) sucedido un 14 de marzo del 2019 a través de un correo malicioso.

Ausencia de políticas de seguridad.

En la entidad no se han establecido directivas, políticas o lineamientos que definan el uso de los recursos y servicios informáticos de la organización. La ausencia de estas ha llevado a un mal uso de los recursos y servicios, afectando la seguridad y funcionalidad de la red.

No se realizaron mantenimiento al etiquetado de los equipos

En su implementación no se entregó ninguna documentación del diseño de la red. Con el pasar de los años se ha venido retirando por distintas razones el etiquetado de la red para la identificación que se realizó en su momento de implementación generando problemas para su identificación para la resolución de problemas y/o configuración.

Caídas constantes de la corriente

En la municipalidad de Carabayllo se presentan constantes caídas de la corriente afectando a los equipos tecnológicos, estas caídas ocasionado daños en los equipos.

1.3.2 Problemas tecnológicos

Estos problemas se presentan porque no se implementó un requerimiento importante la configuración de los equipos, a su vez el incremento del personal, la necesidad de más puntos de red y el casi nulo presupuesto al área de TI obliga a comprar equipos caseros y realizar un cableado malo. Los problemas tecnológicos son:

Configuración por defecto de los equipos

No se realizó ninguna configuración a los equipos de red. Parámetros no han sido modificados en la configuración de los equipos permanecen con los valores por defecto, de fábrica.

Agrupación de las diferentes áreas en una sola red

Todas las unidades orgánicas se encuentran en una sola red, saturando la red con la difusión de broadcast, tener una sola red implica un problema de seguridad ya que los usuarios podrían acceder a información de las diferentes áreas, comprometiendo la seguridad de la información.

Equipos de comunicación no administrables y/o caseros.

Ante el incremento de personal por ende el aumento de equipos tecnológicos conectados a la red, es que se ha venido colocando equipos de comunicación provisionales no administrables caseros generando lentitud, caídas y/o inaccesibilidad de la red.

1.4 Metodologías y herramientas

Para el rediseño de la red se definió utilizar la metodología PPDIOO junto con el modelo de seguridad para las redes de las empresas SAFE de Cisco y las buenas prácticas de seguridad para la configuración de equipos definidas en los benchmarks de CISecurity y otros.

II. ANÁLISIS DE LA RED DE LA MDC (PLANIFICACIÓN)

2. Situación actual

Para realizar un correcto rediseño de red que cumpla con los requerimientos de la MDC es necesario levantar el estado actual de los equipos, personal y servicios de los cuales se disponen y así poder determinar el impacto que va a tener en los mismos en el rediseño.

Para el desarrollo de esta fase se han realizado entrevistas con el Subgerente de Tecnología de la Información y Estadística, identificando una serie de parámetros que son de suma importancia para el rediseño de la red aplicando hardening a nivel de red.

2.1 Distribución física de las unidades orgánicas

La MDC en la sede principal “PALACIO MUNICIPAL”, dispone de 5 pisos y un sótano, en los cuales se encuentran distribuidos de la siguiente manera:

Tabla 7: Distribución física de las UO por pisos

N°	Piso	Áreas
01	Sótano	Subgerencia de Atención al Ciudadano y Gestión Documental (Archivo)
02	Primer Piso	Plataforma, Subgerencia de Tesorería, Subgerencia de la Oficina de Programación Multianual de Inversiones, Subgerencia de Atención al Ciudadano y Gestión Documental (Mesa de Partes y Oficina Administrativa) y el Área de Seguridad Interna.
03	Segundo Piso	Subgerencia de Recursos Humanos, Subgerencia de Transportes, Gerencia de Desarrollo Económico Local y Turismo, Subgerencia de Comercialización, Subgerencia de Gestión del Riesgo, Subgerencia de Recaudación y Ejecución Coactiva, Subgerencia de Registro y Fiscalización Tributaria y la Gerencia de Administración y Recaudación Tributaria.
04	Tercer Piso	Subgerencia de Logística, Subgerencia de Control Patrimonial y Maestranza, Subgerencia de Presupuesto, Gerencia de Planeamiento y

		Cooperación Institucional, Subgerencia de Contabilidad, Gerencia de Administración y Finanzas, Subgerencia de Obras Privadas, Subgerencia de Estudios y Proyectos y la Gerencia de Inversiones Públicas.
05	Cuarto Piso	Alcaldía, Gerencia Municipal, Gerencia de Asesoría Jurídica, Gerencia de Secretaria General, Subgerencia de Imagen Institucional, Subgerencia de Tecnología de la Información y Estadística.
06	Quinto Piso	Gerencia de Desarrollo Urbano y Rural, Subgerencia de Catastro, Gerencia de Procuraduría Pública Municipal, Oficina de Control Institucional, Subgerencia de Participación Vecinal.

2.2. Dispositivos de red

Para verificar el estado de cada dispositivo se red es necesario tomar en cuenta el número de usuarios concurrentes que acceden a la red. Los dispositivos de red no cuentan con UPS y ante los constantes bajones de corriente se apagan.

Tabla 8: Dispositivos de red

N°	Marca	Total de Puertos / Puertos Disponibles	Ubicación	Función
01	HP 5130(JG937A)	48/48	Gabinete de Comunicación - Sótano	Acceso
02	HP 5130(JG932A)	24/23	Gabinete de Comunicación - primer piso (Tesorería)	Acceso
03	HP 5130(JG932A)	24/17	Gabinete de Comunicación - primer piso (Plataforma)	Acceso
04	HP 5130(JG937A)	48/48	Centro de Comunicación - segundo piso	Acceso
05	HP 5130(JG937A)	48/48	Centro de Comunicación - segundo piso	Acceso
06	HP 5130(JG932A)	24/24	Centro de Comunicación - segundo piso	Acceso
07	HP 5130(JG937A)	48/48	Centro de Comunicación - tercer piso	Acceso
08	HP 5130(JG937A)	48/48	Centro de Comunicación - tercer piso	Acceso
09	HP 5130(JG932A)	24/5	Centro de Comunicación - tercer piso	Acceso

10	HP 5130(JG937A)	48/48	DATA CENTER – cuarto piso		Acceso
11	HP A7506(JD239B)	48/34 8/4	DATA CENTER – cuarto piso		Distribución
12	FIREWALL		24/21	DATA CENTER – cuarto piso	Núcleo
13	HP 5130(JG932A)		24/12	Informática – cuarto piso	Acceso
14	HP A7506(JD239B)		48/48	Informática – cuarto piso	Acceso
15	HP 5130(JG932A)		48/48	Centro de Comunicación – quinto piso	Acceso
16	HP 5130(JG932A)	24/10	Centro de Comunicación – quinto piso	Acceso	

2.3. Cableado estructurado

Los puntos de red actualmente colocados en el Palacio Municipal se encuentran en buen estado, ante el incremento de los usuarios y/o equipos de tecnológicos (computadoras, teléfonos, laptops y otros), se cuenta con pequeños switch domésticos, los cables están por el suelo, junto con cables de corriente. El 80 % del etiquetado de la infraestructura se perdió con el pasar del año, desorden en los gabinetes de red.



Figura 8: switch no administrables

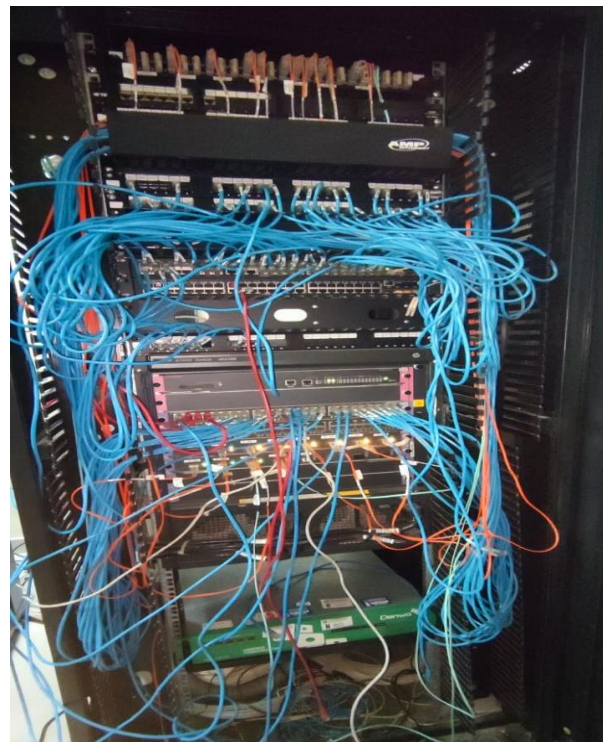


Figura 9: Desorden de gabinetes

2.4. Red física

La arquitectura modular SAFE nos permite analizar la funcionalidad de la red tomando en consideración conceptos como: modularidad, redundancia y amenazas de seguridad que se deben mitigar. Por lo que el diseño actual será mapeado en módulos que permitan analizar la funcionalidad de cada uno.

2.4.1 Arquitectura de red

La red actual de la MDC presenta una arquitectura jerárquica conformada por capas de núcleo, distribución y de acceso. La conexión hacia redes externas y la seguridad de la red está dada por la capa núcleo. La capa de distribución permite la conexión de los usuarios ubicados en la capa de acceso con los servicios ubicados en el datacenter y la conexión hacia redes externas mediante el perímetro (núcleo).

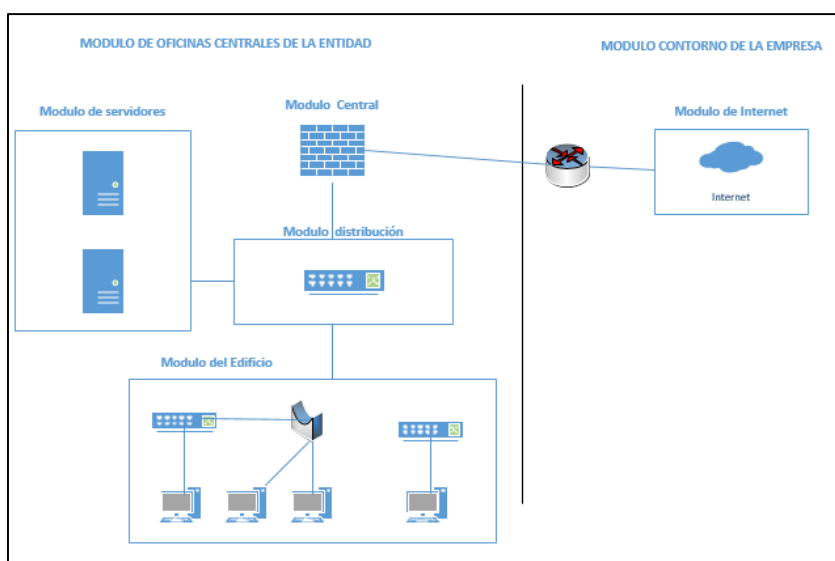


Figura 10: Arquitectura modular actual

2.4.1.1.1 OFICINA CENTRALES DE LA EMPRESA

Las oficinas centrales de la empresa proveen acceso a la red a usuarios y dispositivos. Los módulos a analizar dentro de las oficinas centrales de la entidad en la red de la MDC son: modulo central, distribución, modulo del edificio y módulo de servidores.

2.4.1.1.1.1 MODULO CENTRAL

El modulo central conecta a todos los módulos de la arquitectura SAFE. Este módulo enruta y conmuta el tráfico desde un módulo hacia otro. Las amenazas que debe combatir este módulo según SAFE son los denominados rastreadores de paquetes, que son mitigados con la infraestructura conmutada.

SAFE describe a la arquitectura conmutada como un método para contrarrestar el uso de rastreadores de paquetes. Por ejemplo si una organización tiene instalada Ethernet conmutado los atacantes solo pueden obtener acceso al tráfico que fluye en el puerto específico al que se conectan. La municipalidad de Carabayllo tiene una infraestructura conmutada, minimizando las amenazas de rastreadores de paquetes en todos los módulos de la arquitectura.

El modulo central actualmente está constituido por un único router - firewall que enruta y conmuta los paquetes provenientes del módulo de distribución y de internet. Al ser el único router este constituye en un punto único de falla, una falla podría causar la falta de disponibilidad los servicios de internet. En el tercer punto, se analizaran si es factible agregar un dispositivo redundante para eliminar este único punto de falla o mantener solo el dispositivo actual. La conexión con el módulo de distribución se realiza mediante enlaces de cable UTP categoría 6 de 1 Gbps.

2.4.1.1.1.2 MODULO DISTRIBUCIÓN

Este módulo permite la comunicación entre el modulo central y el modulo del edificio. Las amenazas que combate este módulo según SAFE son: accesos no autorizados y rastreadores de paquetes. Estas amenazas son mitigadas mediante filtrado de paquetes y la implementación de una infraestructura conmutada. Actualmente este módulo no tiene implementado filtrado de paquetes, pero si se cuenta con una infraestructura conmutada

Este módulo se encuentra constituido por un switch core que se encarga de transportar los datos al módulo central. Al ser el único

switch este constituye en un punto único de falla, este podría causar la falta de disponibilidad de toda la red. En base a los requerimientos se analizara si es factible agregar un dispositivo redundante para eliminar este punto de falla o mantener el dispositivo actual. La conexión con los switch del módulo de edificio se realiza mediante enlaces de fibra óptica de 10 Gbps. La conexión con el módulo de servidores y el módulo de internet se realiza mediante enlaces de cable UTP categoría 6 de 1 Gbps.

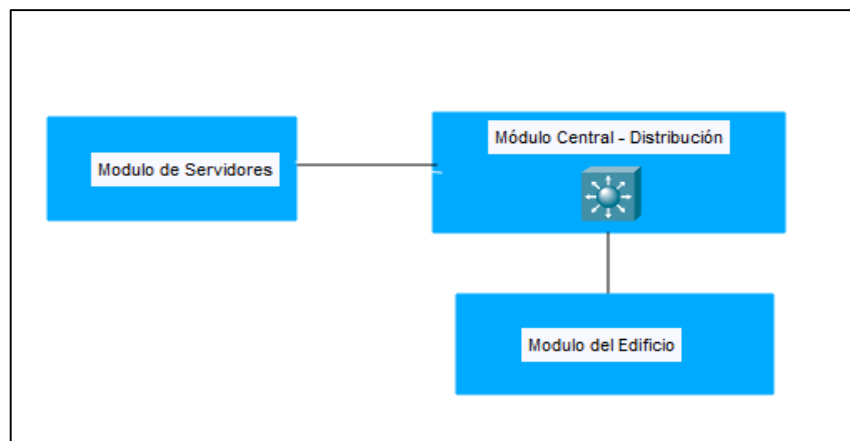


Figura 11: Modulo Central - Distribución

2.4.1.1.1.3 MODULO DEL EDIFICIO

Este módulo del edificio provee acceso a los servicios de red a los usuarios finales, aquí se encuentran dispositivos como: computadoras, impresoras, teléfonos IP, marcadores digitales, Acces Point. Las amenazas que combate este módulo según SAFE son: rastreadores de paquetes, virus y troyanos. Estas amenazas son mitigadas con la implementación de VLANS y la instalación de un antivirus.

La figura 11 representa el modulo del edificio actualmente instalado en la red de la MDC, compuesto por 16 switches y 18 repetidores. Los dispositivos desplegados son: computadoras de escritorio, laptop, teléfonos IP, Access point, impresoras IP y marcadores digitales.

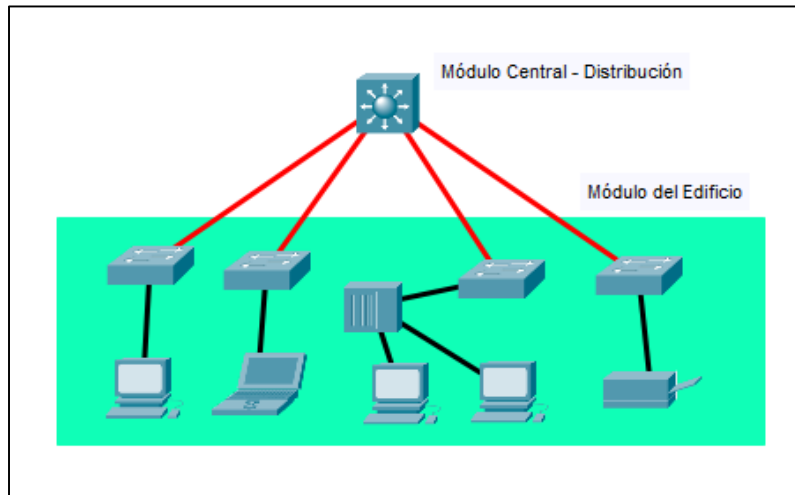


Figura 12: Módulo del Edificio

La conexión con el switch (core) al módulo distribución se realiza mediante fibra óptica de 10 Gbps. La conexión hacia los terminales se realiza mediante enlaces UTP de categoría 6 de 1 Gbps.

Los usuarios que se conectan al módulo del edificio se encuentran en una sola red del primero al quinto piso. El antivirus utilizado en la MDC es GDATA la actualización de esta es de manera automática.

2.4.1.1.4 MODULO DE SERVIDORES

En el módulo de servidores contiene a los servidores y dispositivos de almacenamiento que brindan las aplicaciones y servicios a los usuarios internos. Este módulo no es accesible de manera directa desde el internet para el público en general de acceso libre a la red interna. Las amenazas a combatir según SAFE son: accesos no autorizados, ataques a la capa de aplicación, abusos de confianza y redirección de puertos. Estas amenazas son mitigadas con la instalación de sistemas de detección de intrusos basados en host y controles de acceso, instalación de parches de seguridad, utilizados de vlans.

2.4.1.1.2. CONTORNO DE LA EMPRESA

El contorno de la empresa es una parte de la arquitectura que permite conectividad desde la red interna hacia el internet y proporciona accesos a los servicios públicos a los usuarios de la entidad.

2.4.1.1.2.1 MODULO DE INTERNET

Este módulo provee acceso a internet a los usuarios de la entidad, la implementación del módulo de internet incluye elementos tales como: Perímetro de red, acceso corporativo y DMZ.

El perímetro de red contiene al router que realiza el enrutamiento del tráfico entre la red de la entidad y redes externas. Actualmente se dispone de un único proveedor.

El acceso corporativo y la DMZ proporcionan el acceso a internet a los usuarios, a la vez permite el acceso a servicios externos. Se implementa con un router- firewall que protege los recursos de la entidad de amenazas externas y limitan el acceso de usuarios externos. Las amenazas que deben mitigar este módulo según SAFE son: accesos no autorizados, reconocimiento de red, ataques a la capa de aplicación, virus y troyanos, ataques a contraseñas, rastreadores de paquetes, redirección de puertos, abuso de confianza, y ataques de denegación de servicio. Estas amenazas son mitigadas con la implementación de un firewall, sistemas de detección de intrusos, instalación de parches de seguridad, instalación de antivirus y utilización de vlans.

El módulo de internet actualmente, constituido por un firewall y un router. La conexión hacia redes externas se realiza mediante el proveedor de servicios. El personal de la MDC no interviene en la administración y configuración del firewall y router.

El firewall controla el tráfico proveniente del router que está conectado directamente al proveedor de servicios, el firewall limita las amenazas de acceso no autorizado y denegación de servicio mediante políticas. El firewall representa un punto único de falla, viéndose afectado el acceso a internet

La DMZ estará conformada por un switch de acceso y por los servidores de correo y pagina web. Los servidores se conectaran al switch de acceso y este switch se conectara al firewall. Las conexiones entre los equipos de la red interna y la DMZ están permitidas, mientras que las conexiones externas podrán acceder solamente hasta la DMZ.

Después de realizar el análisis de la situación actual de la red física se puede concluir que el diseño actual presenta características que no cumplen con respecto a los principios de SAFE

- Redundancia de equipos en el módulo central
- Redundancia de equipos en el módulo de distribución
- Redundancia de equipos en el módulo de internet

Estas características serán consideradas en la propuesta de nuevo diseño de la red de datos de la MDC

2.5. Red lógica

Se entiende por red lógica en la manera en la que los dispositivos se organizan y comunican entre sí. El análisis de la red lógica considera los protocolos de la capa de red y transporte correspondiente al direccionamiento, enrutamiento y configuración.

2.5.1. Direccionamiento

La red de la MDC está dividida en 2 redes que han sido desplegadas a base del servicio que ofrecen. Las redes son:

Tabla 9: Redes de la MDC

Descripción	Rango de Direcciones
Equipos de Red	172.16.4.0/22
DMZ	192.168.3.0/22

2.5.2 Enrutamiento

El proceso de enrutamiento es el encargado de determinar la ruta o camino de los paquetes entre su origen y destino. El enrutamiento está a cargo el proveedor de servicios.

2.5.3 Configuración

La configuración IP es mixta, se utiliza DHCP y asignaciones estáticas, solo los equipos de cómputo tienen asignaciones DHCP mientras que impresoras, servidores, cámaras, marcadores digitales y teléfonos son asignados IP estáticamente.

2.3. Seguridad

En la sección 2.1.1. Se describió el análisis de la arquitectura de red, en la que se revisaron recomendación de seguridad SAFE para cada módulo. Las recomendaciones consideran el despliegue e instalación de equipos y software de seguridad. En esta sección se describe la configuración que deben tener los dispositivos, como elementos activos terminales en base a las buenas prácticas dadas en los benchmarks de CISecurity.

2.3.1. Elementos activos

Los elementos activos identificados en la red MDC son switch y routers. El análisis considera únicamente a los switch ya que la administración y configuración del router está a cargo del proveedor de servicios, razón por la que no fue permitido el acceso a estos dispositivos y revisar su configuración, no obstante se dará recomendaciones de configuración. El benchmark utilizado para el análisis se denomina "Center for Internet Security Benchmark for Cisco IOS". En este benchmark se encuentran un conjunto de buenas prácticas y recomendaciones para la configuración de switches, routers y firewalls.

El benchmark está enfocado a equipos cisco, por lo que se ha tomado como referencia y se ha aplicado los puntos compatibles con los equipos HP. La tabla 10 presenta el resultado de aplicar benchmark en los elementos activos de la red MDC. Para los puntos presentados se especifica si la configuración actual cumple o no la recomendación, y una observación referente a cada punto. Al final de la tabla se resume los puntos que no se están cumpliendo y se describe una justificación de los beneficios de implementar cada una de las recomendaciones

Tabla 10: Buenas prácticas de configuración

Benchmark para la configuración de la seguridad	Cumplimiento	Observaciones
Plano de Gestión		
Reglas de acceso		
¿Se requiere usuarios locales y contraseñas encriptadas?	NO	No existe clave para su acceso
¿Se requieren SSH para el acceso remoto?	NO	No se tiene habilitado SSH
¿Se ha definido un tiempo de espera para cerrar las sesiones iniciadas?	NO	No existe ningún tiempo de espera para el cierre de sesión automático
¿Se ha habilitado ACLs (Lista de control de acceso) para al administración remota del dispositivo?	NO	Se puede iniciar sesión con el dispositivo desde cualquier terminal
Normas sobre los mensajes de advertencia (banners)		
¿Se visualiza un mensaje de advertencia (banner) al inicio de sesión?	NO	No se definió ningún banner en ninguno de los equipos
Normas para simple Network Management Protocol (SNMP)		

¿Se encuentra habilitado el protocolo SNMP?	NO	No esta habilitado
Plan de control		
¿Se ha deshabilitado Hypertext Transfer protocol (HTTP) para la administración vía web?	NO	La administración mediante HTTP esta deshabilitada
Reglas de registro		
¿El registro de eventos (logs) está habilitado?	NO	No esta habilitado los logs
¿Se han designado uno o más servidores de logs, para centralizar el registro de eventos?	NO	No se cuenta con servidores para el almacenamiento de logs

En base a los resultados del análisis mostrado en la tabla anterior y de acuerdo a las recomendaciones del benchmark, se han llegado a las siguientes recomendaciones:

Requerir usuarios locales y contraseñas encriptadas. Por defecto la configuración de los dispositivos no requiere una autenticación fuerte, esto podría ser aprovechado por un atacante para comprometer un equipo. Se recomienda tener un usuario local y utilizar contraseñas encriptadas para mejorar la autenticación.

Mostrar un mensaje de advertencia al inicio de sesión (Banner). Este mensaje permite informar que el acceso está prohibido y que el acceso no

autorizado podría ocasionar acciones legales, solo usuario autorizado pueden acceder.

Deshabilitar el servidor HTTP. El servidor HTTP permite la gestión remota del dispositivo. Cuando sea posible se debe deshabilitar HTTP y reemplazar por HTTPS.

Habilitar un servidor de logs. Los dispositivos como switches o routers tienen una capacidad de almacenamiento mínima, un servidor de log permite almacenar la información en el disco duro del servidor y no en el equipo (switch o router) logrando así un almacenamiento a un largo plazo y de manera centralizada.

2.4. Aplicaciones y servicios

Las aplicaciones y servicios que está utilizando actualmente la Municipalidad Distrital de Carabayllo

Tabla 11: Aplicación y servicios de la MDC

Aplicación o Servicio	Descripción
Servicio DNS	El Sistema de Nombres de Dominio o DNS es un sistema de nomenclatura jerárquico que se ocupa de la administración del espacio de nombres de dominio (Domain Name Space). Su labor primordial consiste en resolver las peticiones de asignación de nombres
Servicio de Directorio Activo	Se trata de una estructura de base de datos distribuida y jerárquica que comparte información de infraestructura para localizar, proteger, administrar y organizar los recursos del equipo y de la red, como archivos, usuarios, grupos, periféricos y dispositivos de red.
Servicio de DHCP	El servicio DHCP (Dynamic Host Configuration Protocol) permite que un servidor especifique parámetros de red de manera automática a las máquinas que lo solicitan cuando se conectan a la red. De esta manera se facilita la configuración en red de los

	ordenadores y su posterior mantenimiento.
Servicio de Impresión y documentos	Permite compartir impresoras y escáneres en una red, configurar servidores de impresión y servidores de digitalización, así como centralizar las tareas de administración de escáneres e impresoras de red
Servicio de archivos y almacenamiento	Un file server o servidor de archivos es una instancia de servidor central de una red de ordenadores que permite a los clientes conectados acceder a sus propios recursos de almacenamiento. El término abarca tanto el hardware como el software que se necesita para implementar dicho servidor. Si los usuarios obtienen los correspondientes permisos, pueden abrir las carpetas y archivos guardados en el servidor, así como consultarlos, modificarlos, eliminarlos o subir sus propios documentos.
Servicio de FTP	El servicio FTP (File Transfer Protocol) es un servicio utilizado para el envío y obtención de archivos entre dos equipos remotos. Los casos más usuales son transferencias entre el equipo local de un cliente y el servidor del proveedor, aunque también se pueden establecer conexiones FTP entre dos servidores.
Página web Institucional	Página web publica que contiene información sobre su estructura, actividad y otros. Bajo el dominio http://www.municarabayllo.gob.pe/
Servicio de Correo Electrónico Institucional	El servidor de correos es una herramienta institucional de comunicación e intercambio de información oficial entre los trabajadores e instituciones públicas y/o privadas con fines institucionales. Bajo el dominio https://mail.municarabayllo.gob.pe/#1
Servidor Antivirus	Servidor diseñado con arquitectura de alto rendimiento, en el cual se instala herramientas de seguridad para administración remota, con el objetivo de monitorear amenazas de malware, validar licencias de producto, distribuir

	actualizaciones de firmas y realizar configuraciones personalizadas en diversos computadores, conectados básicamente a la red local.
Sistemas de Información Internos	Sistemas Informáticos internos que ayudan en la parte administrativa de la organización. Contando con: SIGGEDO SISMUN SIGA Web y otros.
Servicio de Internet	Servicio en el cual nos permite establecer una comunicación directa e intercambiar información con personas de todo el mundo.

La tabla 12 muestra las aplicaciones identificadas en la red que son utilizadas por los usuarios de la MDC, junto con su dirección IP.

Tabla 12: Aplicaciones de la MDC

Aplicación	Dirección IP	Puerto
SISMUN	172.16.4.31	-
SIGGEDO	172.16.5.63	8081
SIGAWEB	172.16.4.98	8094
SIGA-MEF	172.16.5.98	-
SISVLECHE	172.16.5.63	8055
SIAF	172.16.4.134	-
SISMUNWEB	172.16.4.31	8088
SISRRHH	172.16.5.63	8270
SIGAM	172.16.4.3	-
SIGMUN	172.16.4.31	8261
SISCOMED	172.16.5.63	8250
COA	172.16.5.63	8081
SISVISITAS	172.16.5.63	8081
SISLLAMADO-TK	172.16.5.63	8081
CORREOWEB-MDC	192.168.3.14	80

En la figura 6 representa el flujo de la información de los usuarios de los pisos de las distintas áreas ubicado en palacio municipal. Las peticiones inician desde el computador del usuario localizado en el módulo del edificio, pasando al módulo de distribución y finalmente llegan a la aplicación alojada en el módulo de servidores.

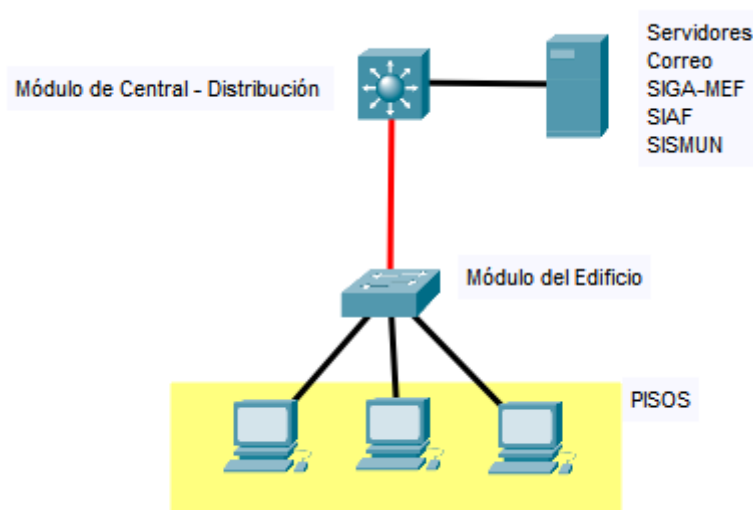


Figura 13: Flujo de la Información

En la propuesta del nuevo diseño de red, se considerara las ACLs que se deberían implementar en módulo central – distribución para limitar el tráfico entre las comunidades de usuarios y las aplicaciones.

2.5. Vulnerabilidades a nivel de red

Una vulnerabilidad es un fallo en un sistema que pone en riesgo la seguridad de la información pudiendo permitir que un atacante pueda comprometer la disponibilidad, confidencialidad e integridad de la información, por lo que es importante identificarlos y eliminarlos lo ante posibles. Por ende las vulnerabilidades son características propias de los sistemas.

2.5.1 Vulnerabilidades de medio ambiente e infraestructura en la MDC:

Vulnerabilidades que se ven amenazadas frente a la exposición del medio ambiente.

- Protección física inadecuada (edificio, gabinetes, centros de comunicación)
- Control de acceso inadecuado
- Energía eléctrica inestable
- Equipos de enfriamiento inadecuados
- Desastre natural
- Desastres humanos
- Falta de mantenimiento de la infraestructura
- Falta de un plan y/o prevención contra incendios o detección

2.5.2 Vulnerabilidades del personal en la MDC: Vulnerabilidades enfocadas al trabajo y los roles del personal

- Personal insuficiente
- Falta de mecanismos de monitoreo
- Falta de políticas, normas y procedimientos
- Falta de delegación, participación y sucesión
- Recursos insuficientes e inadecuados

2.5.3 Vulnerabilidades de Hardware en la MDC: Vulnerabilidades que pueden presentar los componentes de hardware expuestos a diversas amenazas.

- Falla del hardware y componentes
- Almacenamiento inadecuado
- Falta de mantención planificada
- Control de acceso inadecuado,
- Suministro eléctrico
- Control de configuración inadecuado
- Conexión de equipo no autorizado

2.5.4 Vulnerabilidades de comunicaciones en la MDC: Vulnerabilidades relacionadas con la posible interceptación de la información por personas no autorizadas y con fallas a la disponibilidad del servicio.

- Líneas de comunicación no protegidas
- Uniones de cables deficientes

- Administración de la red inadecuada
- Protección inadecuada para el acceso público
- Puntos de acceso no protegido

2.5.5 Vulnerabilidades de software: Vulnerabilidades enfocadas en el uso del hardware (switch)

- Control de acceso inadecuado
- Uso impropio no controlado
- Contraseñas no protegidas, claves, certificados
- Administración deficientes de clave
- Falta de documentación
- Administración de configuración inadecuado

3.0. Requerimientos

En esta sección se describe el análisis de los requerimientos para la red de datos de la MDC. La metodología PPDIOO que se sigue para el desarrollo de este proyecto, recomienda que se consideren cinco pasos para la obtención de los requerimientos, tal como se presentan en la figura 13 .La información recolectada de los cinco pasos permitirá la definición de los requerimientos para la propuesta de nuevo diseño.

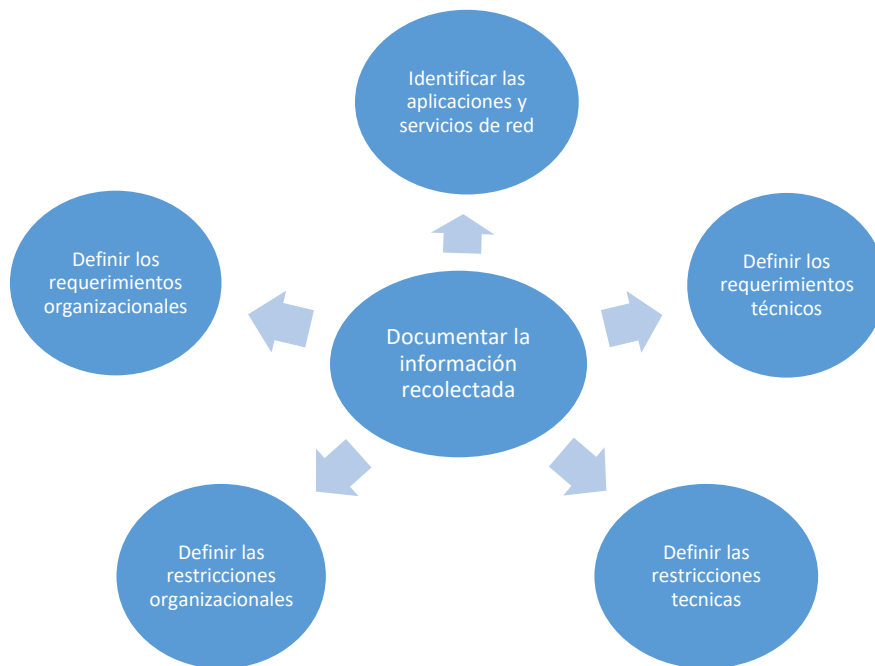


Figura 14: Pasos para la obtención de requerimientos

La información se obtiene mediante entrevistas realizadas al personal de la Subgerencia de Tecnología de la Información y Estadística (SGTIE). Para obtener y documentar la información del personal de TI se ha realizado un cuestionario a utilizar en las entrevistas con el personal de TI.

3.1. Entrevista

El diseño de la entrevista tiene como finalidad obtener y documentar la información necesaria para definir los requerimientos de la red de la MDC. La información obtenida será analizada y se obtendrán los requerimientos.

En la tabla 13 se presenta el cuestionario realizado para obtener información de las aplicaciones y servicios de red.

Tabla 13: Entrevista

¿Qué aplicaciones y servicios se consideran más importantes para la entidad?

OBJETIVO: Identificar el grupo de aplicaciones y servicios considerados de mayor importancia

¿Qué sistema maneja información sensible que pueda considerarse de mayor importancia y riesgo?

OBJETIVO: Identificar el tipo de información que se maneja en las aplicaciones, para determinar su importancia en la seguridad de la misma.

¿Qué porcentaje de disponibilidad deberían presentar las aplicaciones y servicios, tanto para usuarios internos como externos?

OBJETIVO: Identificar la disponibilidad que se requiere que tengan los servicios ofrecidos por la red, para determinar su importancia en el nuevo diseño.

¿Qué retos u objetivos enfrenta la MDC?

OBJETIVO: Identificar los objetivos organizacionales, para determinar las características que la red debe implementar para dar soporte a esos objetivos.

¿Cuáles son las limitaciones para la implementación de un nuevo diseño de red en la organización?

OBJETIVO: Identificar las limitaciones organizacionales que existen, para que el diseño de red se limite de acuerdo a estas consideraciones.

¿Qué limitaciones se han identificado en el diseño actual en base a los requerimientos iniciales solicitados?

OBJETIVO: Identificar cuáles son los requerimientos iniciales, que no se han cumplido o que se han cumplido parcialmente, para analizarlos y tenerlos en cuenta en el rediseño.

¿Cuáles son las prioridades tecnológicas?

OBJETIVO: Identificar las prioridades tecnológicas, para determinar su importancia dentro de la propuesta de rediseño de la red.

¿Qué problemas de infraestructura existen o podrían existir?

OBJETIVO: Identificar cuáles son los posibles problemas de infraestructura que existen o podrían existir en la organización de manera que se propondría una solución en el rediseño.

¿Qué problemas tecnológicos deberían corregirse de manera inmediata?

OBJETIVO: Identificar cuáles son los problemas tecnológicos más críticos que existen actualmente de manera que se presenta una solución dentro del rediseño de la red

3.1.1. Análisis de la entrevista

Realizada la entrevista se han documentado y analizado, obteniendo la siguiente información:

- Las aplicaciones de mayor importancia son: SISMUN, SIAF, SIGEDO, SIGA – MEF, SIGA WEB, SIGAM, SISMUN WEB, SIGMUN ENTRE OTROS.

- El SISMUN ya que es un sistema que abarca el tema de rentas y tesorería hay información sensible de los contribuyentes que puede ser usado para el tráfico de terrenos.
- La propuesta de un nuevo diseño debe mantener la capacidad de soportar todos los servicios y/o aplicaciones con las que cuenta la entidad. Se desea mejorar la seguridad de la información ya que se tuvo un ataque de tipo ransomware (ATAQUE STOP RANSOMWARE VARIANTE DJVU .PULSAR1), el 14 de marzo del 2019 en la cual se infectó distintos archivos paralizando así el trabajo por al menos 3 semanas paralizando el trabajo en las distintas áreas, adicional a eso se desea contar con una red con una disponibilidad de al menos un 98% en donde las caídas solo se han por equipos malogrados.
- El factor económico evita el contratar a una empresa especializada para auditar la seguridad de la información, estos factores impiden la compra de equipos de cómputo y comunicación u otros para su renovación.
- En cuanto a las limitaciones técnicas el cableado estructurado que está presente en la sedes de la entidad están en muy mal estado, cables que pasan por la misma canaleta con el cable de corriente, el recubrimiento de protección roto (mal estado), cableado parchado para poder llegar a un punto (deterioro), múltiples cascada con switch baratos, categoría de cable 5 de aluminio. Por lo que se debe proponer alternativas para que el diseño propuesto funcione de manera correcta, es decir, se debe considerar un nuevo cableado estructurado utilizando un cable de categoría 6 o mayor.

La propuesta del nuevo diseño descrito en el siguiente capítulo considera cada uno de los puntos anteriores.

III. DISEÑO DE LA RED CON EL MODELO

En este capítulo se describe el diseño físico y lógico de la red de la MDC. El diseño físico muestra la arquitectura de la red, en las capas física y enlace de datos del modelo OSI y se base en la arquitectura modular SAFE de cisco. El diseño lógico muestra el direccionamiento, enrutamiento y mecanismos de configuración de los equipos a nivel de la capa de red del modelo OSI.

3.1. Red física

En esta sección se presenta el rediseño de los módulos que presentaron inconvenientes y necesitan modificarse para satisfacer los requerimientos descritos en la sección anterior.

El diseño actual presenta cuatro características (que fueron señalados al final del análisis de la red física en la sección 2.1.) que no se cumplen con respecto a los principios de la arquitectura modular SAFE. Estas son:

- Redundancia de equipos en el módulo central
- Redundancia de equipos en el módulo de distribución
- Redundancia de equipos en el módulo de internet

Estas tres características podrían causar el incumplimiento de las cuales detallo:

Redundancia de equipos en el módulo central: Este módulo tiene un solo router – firewall que representa un punto único de falla. La falla de este dispositivo comprometería la comunicación entre el módulo de distribución e internet, viéndose afectado el servicio de internet. Agregar un segundo router – firewall ayudaría a mantener la disponibilidad de la red, implicando un costo económico en la adquisición del equipos o servicio de alquiler. En la próxima sección se analizara la factibilidad de agregar o no un segundo router – firewall.

Redundancia de equipos en el módulo de distribución: Este módulo presenta solo un switch core representando un punto único de falla. La falla de este equipo comprometería la comunicación con el modulo central, servidores y de acceso comprometiéndolo el acceso a los servidores, los usuarios no tendrían acceso a ninguno de ello. Se recomienda la adquisición de otro equipo de manera que no se afectaría la disponibilidad de la red. En la próxima sección se analizara la factibilidad de agregar o no un segundo switch core

Redundancia de equipos en el módulo de internet: La conexión hacia redes externas esta soportada por un solo proveedor de servicios de internet, si este presente algún fallo los usuarios internos no podrían acceder a internet y los externos no tendrían acceso a los servicios públicos (DMZ). Se ve en la necesidad de analizar la factibilidad de contratar un servicio de internet de proveedor distinto.

Cada una de estas características es analizada y considerada en la propuesta del diseño físico de las oficinas centrales de la empresa y del contorno de la empresa.

3.1.1. Oficinas centrales de la empresa

El módulo de la oficina central de la empresa abarca los módulos de central, de distribución, del edificio y de servidores. El módulo de gestión es agregado a las oficinas centrales de la municipalidad, debido a que la administración centralizada es uno de los requerimientos y es una recomendación de la arquitectura modular SAFE, facilitando la administración de los dispositivos localizados en todos los módulos de la arquitectura.

3.1.1.1 Modulo central

SAFE recomienda que se instalen routers redundantes a nivel de modulo central, eliminando el único punto de falla. Esta solución implica un costo económico que sería presupuestado y aprobado por la gerencia. Cabe indicar que la disponibilidad podría ser afectada por desastre naturales, errores humanos o problemas con el software.

3.1.1.2 Módulo de distribución

El módulo de distribución está conectado al módulo central, no se ha establecido redundancia entre los dispositivos. En la propuesta del nuevo diseño se considera redundancia ya que el este módulo va conectado de manera directa al firewall.

3.1.1.3. Módulo de servidores

El módulo de servidores está conectado al switch core, no se ha establecido redundancia entre los dispositivos. En la propuesta del nuevo diseño no se considera redundancia ya que el este módulo va conectado de manera directa al switch core.

3.1.1.4. Módulo de gestión

Este módulo tiene como objetivo facilitar la gestión segura de los dispositivos y equipos de la arquitectura de la red. Para la implementación de este módulo se considera dos propuesta. La primera es la separación física del módulo de gestión y la segunda mantener una separación virtual mediante la VLAN "Administrativa".

La primera opción permitirá la organización física en un switch dedicado, que permitirá la conexión de los equipos designados a la gestión de los dispositivos y equipos de red. De manera que los equipos estarán dentro de la VLAN "Administrativa" y conectados físicamente al mismo switch.

La segunda opción permitirá la organización virtual mediante VLAN "Administrativa", con esta opción el módulo administración se encontrara físicamente dentro del módulo de servidores y modulo del edificio, pero configurados dentro de la vlan administrativa. Esta propuesta es considerada para el nuevo diseño. Se recomienda implementar en este módulo, servidores de gestión snmp, servidor de autenticación, autorización y contabilización (AAA), servidor NTP, servidor de logs.

Entre los reportes que se deberían almacenar y registrar tenemos: reportes de autenticación y autorización, reportes de cambios en los sistemas, reportes de actividad de red y reportes de fallas y errores críticos.

La agregación de estos servidores ayudara a realizar una gestión centralizada de la red, brindando una mayor seguridad.

En la figura 11 se presenta el diagrama de red de la arquitectura física de las oficinas centrales de la empresa con la agregación del módulo de Gestión. Compuesta por 4 módulos, con arquitectura jerárquica de dos capas. La capa núcleo representado por el modulo central – distribución, al que se conectan el módulo de servidores, gestión y contorno de la empresa. Finalmente se encuentra la capa de acceso representada por el modulo del edificio.

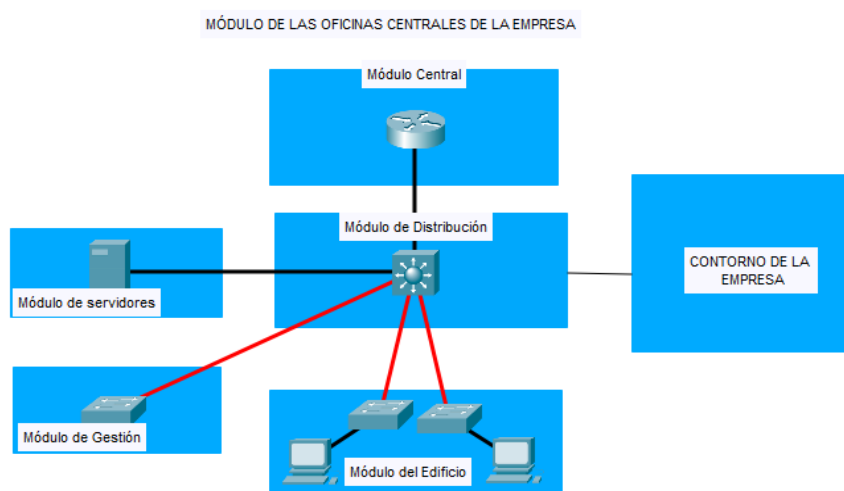


Figura 15: Diagrama de red - Oficinas centrales de la entidad

3.1.2. Contorno de la empresa

El Contorno de la Empresa en la red actual comprende el módulo de Internet, que contiene la infraestructura para la conexión con el Internet. El diseño actual no ha definido una VPN que permita el acceso y la administración de los dispositivos de la organización remotamente. En base a los principios de la arquitectura modular de SAFE y a los requerimientos de la organización, en el nuevo diseño se considera la agregación de la VPN al módulo de Internet.

El módulo de Internet estará conformado por la DMZ, VPN y la agregación de un segundo proveedor de servicio de internet.

3.1.2.1. Módulo de internet

El modulo internet presenta una característica que no cumple con respecto a la arquitectura modular SAFE, que es implementar equipos redundantes para mejorar la disponibilidad. En base a los requerimientos obtenidos, en la propuesta de nuevo diseño se considera la agregación de un segundo ISP, cabe indicar que la alta gerencia no aprobó esta solicitud por la cual no se podrá incorporar un segundo proveedor.

3.2. Red lógica

El diseño de la red lógica describe el direccionamiento, enrutamiento, y los mecanismos de configuración de los equipos. El direccionamiento IP detalla las subredes asignadas a cada VLAN agregada en la propuesta del nuevo diseño de red. El enrutamiento determina los protocolos escogidos para el envío de paquetes. Los mecanismos de configuración presentan el direccionamiento estático o mediante DHCP, con el que se deberán configurar los equipos de cada VLAN. También se presenta las configuraciones de seguridad que deberían tener los equipos en base a las buenas prácticas dadas en los Benchmarks de CISecurity y a los principios de la arquitectura modular de SAFE.

3.2.1. Direccionamiento

El análisis de la situación actual de la red lógica realizado en la sección 2.2. Presentó que existen un total de 2 redes. En esta sección se realiza la propuesta del nuevo diseño de la red en base al análisis realizado, del análisis se determinó que al tener todos los equipos de cómputo, servidores, impresoras en una sola red supone un fallo de seguridad abriendo la posibilidad de que se exploten amenazas como accesos no autorizados que podría comprometer la confidencialidad de la información, colisión de broadcast, uso desmedido del ancho de banda afectando la disponibilidad.

Para evitar estos problemas de seguridad y disponibilidad la propuesta de nuevo diseño recomienda implementar direccionamiento de VLANS, la tabla 6 muestra la nueva distribución por VLANS con su dirección IP de red

Tabla 14. Segmentación de la red

VLAN ID	VLAN NAME	IP DE RED	PRIMER HOST	ULTIMO HOST	BROADCAST	MASCARA	SUBFIJO
103	VIGILANCIA	172.18.5.104	172.18.5.105	172.18.5.110	172.18.5.111	255.255.255.248	/29
105	ATENCION AL CIUDADANO	172.18.3.160	172.18.3.161	172.18.3.174	172.18.3.175	255.255.255.240	/28
107	TESORERIA	172.18.1.96	172.18.1.97	172.18.1.126	172.18.1.127	255.255.255.224	/27
109	PLATAFORMA	172.18.1.64	172.18.1.65	172.18.1.94	172.18.1.95	255.255.255.224	/27
201	RRHH	172.18.3.208	172.18.3.209	172.18.3.222	172.18.3.223	255.255.255.240	/28
207	RIESGO	172.18.1.128	172.18.1.129	172.18.1.158	172.18.1.159	255.255.255.224	/27
209	COMERCIO	172.18.3.176	172.18.3.177	172.18.3.190	172.18.3.191	255.255.255.240	/28
211	RECAUDACION	172.18.1.160	172.18.1.161	172.18.1.190	172.18.1.191	255.255.255.224	/27
213	GER ADMIN TRIBUTARIA	172.18.5.112	172.18.5.113	172.18.5.118	172.18.5.119	255.255.255.248	/29
215	REGISTRO Y FISCALIZACION	172.18.3.224	172.18.3.225	172.18.3.238	172.18.3.239	255.255.255.240	/28
301	LOGISTICA	172.18.4.32	172.18.4.33	172.18.4.46	172.18.4.47	255.255.255.240	/28
305	PRESUPUESTO	172.18.5.128	172.18.5.129	172.18.5.134	172.18.5.135	255.255.255.248	/29
307	PLANEAMIENTO	172.18.5.120	172.18.5.121	172.18.5.126	172.18.5.127	255.255.255.248	/29
309	CONTABILIDAD	172.18.4.64	172.18.4.65	172.18.4.78	172.18.4.79	255.255.255.240	/28
311	FINANZAS	172.18.4.0	172.18.4.1	172.18.4.14	172.18.4.15	255.255.255.240	/28
317	INVERSIONES PUBLICAS	172.18.4.16	172.18.4.167	172.18.4.30	172.18.4.31	255.255.255.240	/28
401	ALCALDIA	172.18.5.136	172.18.5.137	172.18.5.142	172.18.5.143	255.255.255.248	/29
403	JURIDICA	172.18.5.144	172.18.5.145	172.18.5.150	172.18.5.151	255.255.255.248	/29
405	SEC GENERAL	172.18.4.128	172.18.4.129	172.18.4.142	172.18.4.143	255.255.255.240	/28
407	IMAGEN	172.18.4.112	172.18.4.113	172.18.4.126	172.18.4.127	255.255.255.240	/28
409	TIE	172.18.1.224	172.18.1.225	172.18.1.254	172.18.1.255	255.255.255.224	/27
411	GER MUNICIPAL	172.18.4.96	172.18.4.97	172.18.4.110	172.18.4.111	255.255.255.240	/28
501	OCI	172.18.4.144	172.18.4.145	172.18.4.158	172.18.4.159	255.255.255.240	/28
505	CATASTRO	172.18.2.0	172.18.2.1	172.18.2.30	172.18.2.31	255.255.255.224	/27
507	PROCURADURIA	172.18.4.160	172.18.4.161	172.18.4.174	172.18.4.175	255.255.255.240	/28
511	CATASTRO-RENTAS	172.18.2.32	172.18.2.33	172.18.2.62	172.18.2.63	255.255.255.224	/27
715	IMPRESORAS	172.18.0.0	172.18.0.1	172.18.0.126	172.18.0.127	255.255.255.128	/25
737	SERVIDORES	172.18.3.96	172.18.3.97	172.18.3.126	172.18.3.127	255.255.255.224	/27
739	ADMIN-SW	172.18.3.128	172.18.3.129	172.18.3.158	172.18.3.159	255.255.255.224	/27

El cambio realizado implementa las vlans organizadas de acuerdo a las unidades orgánicas, con el fin de evitar accesos no autorizados que comprometan la confidencialidad de la información o afecte la disponibilidad de la misma.

3.2.2. Enrutamiento

Para el enrutamiento la municipalidad de Carabayllo contrata un servicio de seguridad perimetral dejando la administración totalmente a ellos, cabe precisar que aquí se dará a conocer recomendaciones de seguridad que se debería

implementar en el equipo, ya que en capítulos anteriores se presenta como amenaza el acceso no autorizados que podrían comprometer la confidencialidad de la información. Las configuraciones que deberían implementarse para limitar el acceso son:

- Se realizó la conexión intervlan de todas las vlan mencionadas en la tabla N° 14
- Se solicitó mediante correo la creación de vlans de las unidades orgánicas así como su respectiva conectividad a la vlan 737 servidores.
- Se permitió el acceso de la red interna (VLANS CREADAS) hacia EL servidor web con ip 192.168.3.13, habilitando los módulos de antivirus e IPS.
- Se habilitó el tráfico de afuera hacia los puertos IMAP, IMAPS, POP3, PO3S, SMTP, SMTPS para que los usuarios externos puedan acceder al correo, habilitando el filtro de antivirus.

3.3.3. Modulo del edificio

En el nuevo diseño se implementara las vlans de acuerdo a las unidades orgánicas estas ya han pasado por un proceso de subneteo, la cual se idéntico la cantidad de usuarios por área para la realización de este procedimiento. El tráfico generado por las VLANS se enviara por los puertos troncales, estas permitirán el acceso a determinadas VLAN de acuerdo a la unidad orgánica y el piso en el que se encuentren.

- Creación de vlans por unidades orgánicas
- Seguridad de puertos
- Limitaciones de banda ancha por puertos

3.3.4. Módulo de internet

En el nuevo diseño se propuso un nuevo proveedor de servicios de internet, siendo negada por la alta dirección justificando que no se contaba con presupuesto.

3.3.4.1. DMZ

Un atacante busca comprometer un servidor o un computador para obtener acceso a la red y desde esta realizar nuevos ataques. Si un

equipo es comprometido los atacantes tienen acceso libre a cualquier otro dispositivo del segmento de la red. Para reducir el riesgo se han establecido políticas de seguridad que restringen el tráfico.

V IMPLEMENTACIÓN

5.1. Configuración del nuevo diseño

La propuesta del nuevo diseño de red considera la asignación de direcciones IP mediante asignación estática.

Los puntos que aquí se consideran son un resumen del análisis con los benchmarks de CISecurity y las recomendaciones de implementación de cada módulo dadas por SAFE.

5.2. Configuración de los Elementos Activos.

Utilizar SSH para la administración remota del dispositivo. SSH permite que la información viaje encriptada, limitando a terceros obtener datos como nombres de usuarios y contraseñas.

Establecer un tiempo de espera para el bloqueo automático de sesiones de usuario, para evitar que terceros puedan acceder a secciones iniciadas por usuarios legítimos.

Habilitar ACLs para el acceso a los dispositivos. Las ACLs limitarán el acceso al dispositivo por parte de usuarios no autorizados. Estas deberían permitir el acceso a los dispositivos de red únicamente al personal del departamento de TI encargado de la administración. También limitarán las amenazas de abuso de confianza

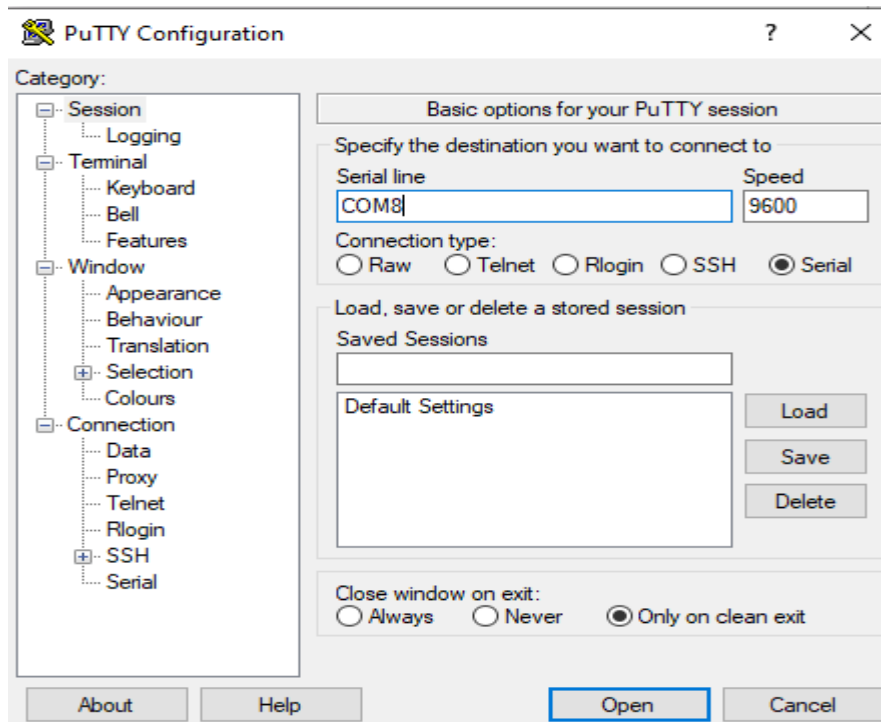
Visualizar un mensaje de advertencia al inicio de sesión en cualquier dispositivo, para advertir a un posible atacante de las consecuencias legales de acceder a un dispositivo sin estar autorizado. Encriptar el envío de contraseñas a través de la red, para limitar que terceros puedan hacerse de estas mediante amenazas como rastreadores de paquetes

Deshabilitar, cuando sea posible, el protocolo HTTP para la administración del dispositivo mediante un navegador, en lugar de este protocolo utilizar HTTPS. HTTP es un protocolo inseguro y está sujeto

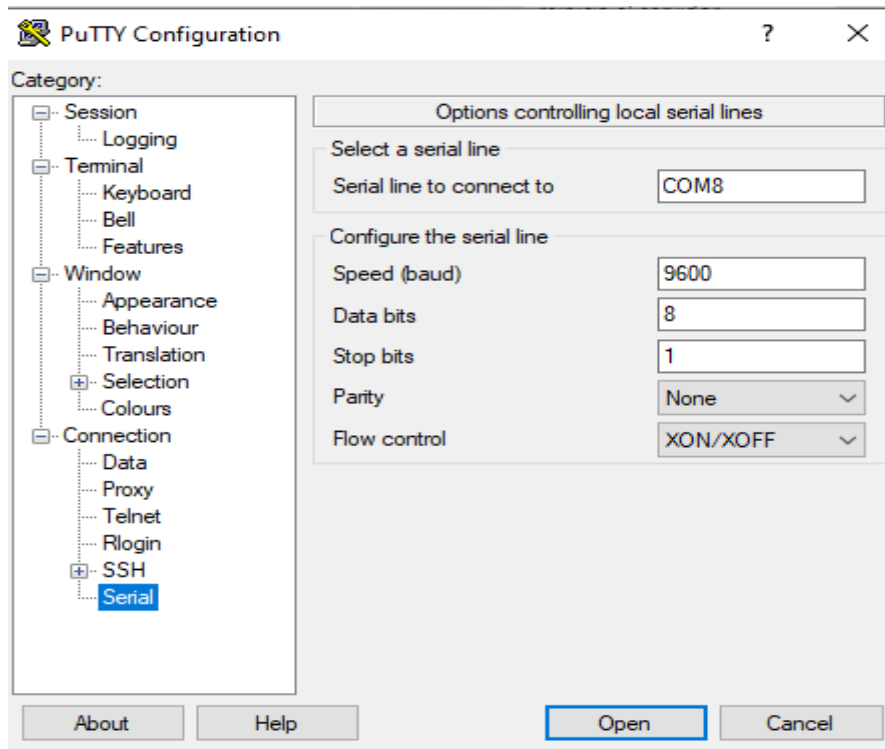
a ataques que pueden permitir que un atacante obtenga información confidencial como nombres de usuarios y contraseñas.

5.3. Implementación de la configuración

Para la realización de la configuración de los equipos se utilizó cable consola y se utilizó el software PUTTY. Para acceder a los switch a través de PUTTY se realizó la siguiente configuración



Con la siguiente configuración de serial



A continuación se empieza a realizar la configuración, al ingresar entraremos al entorno usuario para poder realizar las configuraciones utilizamos el comando **system-view** de manera que podamos ingresar al modo sistema. Cambiamos el nombre de equipo y una breve descripción. Para salir de los modos de configuración usamos el comando **quit**

```

*****
Copyright (c) 2010-2014 Hewlett-Packard Development Company, L.P.
Without the owner's prior written consent,
no decompiling or reverse-engineering shall be allowed.
*****

HPJG932A>sys
HPJG932A>system-view
system View: return to User View with Ctrl+Z.
HPJG932A]sys
HPJG932A]sysname SW-4-SGTIE-01

```

Cabe indicar que las configuraciones de los switch son almacenadas en **current-config**, este almacenamiento es volátil, en caso de una pérdida de energía eléctrica se perderá. Para ello es necesario guardarlo en la configuración de arranque **startup-config** que se almacena en la memoria no volátil para guardar la información se utiliza el comando **save safely force**.

Se procede a realizar la configuración de un aviso o mensaje al intentar acceder al equipo. Configurando un mensaje legal que aparecerá antes de introducir la contraseña en el sistema. A continuación se ejecuta el comando:

```
[SW-4-SGTIE-01]header legal +SOLO PERSONAL AUTROIZADO+
[SW-4-SGTIE-01]
```

Para una mayor seguridad, se realiza la configuración de política de contraseñas. Activamos el control de claves

```
[SW-4-SGTIE-01]password-control enable
[SW-4-SGTIE-01]pas
```

Fijamos una longitud mínima de caracteres

```
[SW-4-SGTIE-01]password-control length ?
  INTEGER<4-32>  Minimum password length, in characters
  enable        Enable the password control function
[SW-4-SGTIE-01]password-control login-attempt 3 exceed lock
[SW-4-SGTIE-01]pas
```

Se fija el número de reintentos en 3, bloqueando el usuario en caso de fallo adicional

Se fija un periodo de vida a cada clave a 30 días

```
[SW-4-SGTIE-01]password-control aging
[SW-4-SGTIE-01]password-control aging 30
[SW-4-SGTIE-01]pas
```

Se fija un periodo mínimo de actualización de 1 hora

```
[SW-4-SGTIE-01]password-control update-interval 1
[SW-4-SGTIE-01]pas
```

Se fija la configuración para que el usuario solo pueda entrar hasta 3 veces en 7 días antes de que la clave expire.

```
[SW-4-SGTIE-01]password-control expired-user-login delay 7 times 3
[SW-4-SGTIE-01]pas
```

Se fija la configuración para rechazar las contraseñas donde se incluya el usuario o su reverso.

```
[SW-4-SGTIE-01]password-control complexity user-name check  
[SW-4-SGTIE-01]pas
```

Se fija la configuración para limitar el uso de un carácter repetido 3 veces.

```
[SW-4-SGTIE-01]password-control complexity same-character check  
[SW-4-SGTIE-01]
```

Es necesario precisar que todos los switch de le entidad cuentan con la configuración de las políticas de clave.

Se procede con la configuración de usuarios locales en los equipos HP

En la configuración de fábrica los equipos HP no vienen configurado con clave el acceso a la consola, accediendo cualquier persona que tenga acceso físico. Es necesario y de vital importancia restringir este acceso, motivo por el cual se procede a crear usuario con sus respectivas claves cumpliendo las políticas de contraseña.

Se realiza la creación del usuario ebel.chinchay con la clave igor.2022, con permisos de ssh y terminal, con un acceso total.

```
[SW-4-SGTIE-01]local-user ebel.chinchay  
[SW-4-SGTIE-01-luser-manage-ebel.chinchay]password simple igor.2022  
Cannot change password until the update-wait time expires.  
[SW-4-SGTIE-01-luser-manage-ebel.chinchay]authorization-attribute user-role level-15  
[SW-4-SGTIE-01-luser-manage-ebel.chinchay]service-type ?  
  ftp      FTP service  
  http     HTTP service type  
  https    HTTPS service type  
  pad      X.25 PAD service  
  ssh      Secure Shell service  
  telnet   Telnet service  
  terminal  Terminal access service  
  
[SW-4-SGTIE-01-luser-manage-ebel.chinchay]service-type https  
[SW-4-SGTIE-01-luser-manage-ebel.chinchay]service-type ssh  
[SW-4-SGTIE-01-luser-manage-ebel.chinchay]service-type terminal  
[SW-4-SGTIE-01-luser-manage-ebel.chinchay]dta  
[SW-4-SGTIE-01-luser-manage-ebel.chinchay]sta  
[SW-4-SGTIE-01-luser-manage-ebel.chinchay]state act  
[SW-4-SGTIE-01-luser-manage-ebel.chinchay]state active  
[SW-4-SGTIE-01-luser-manage-ebel.chinchay]
```

Para verificar el estado del usuario, usamos el comando **display local-user**

```
[SW-4-SGTIE-01]display local-user
Total 3 local users matched.

Device management user aldair.chinchay:
State: Active
Service type: SSH/Terminal/HTTP
User group: system
Bind attributes:
Authorization attributes:
Work directory: flash:
User role list: level-15, network-operator
Device management user aldair:
State: Active
Service type: SSH/Telnet/Terminal/HTTP/HTTPS
User group: system
Bind attributes:
Authorization attributes:
Work directory: flash:
User role list: level-15, network-operator
Device management user ebel.chinchay:
State: Active
Service type: SSH/Terminal/HTTPS
User group: system
Bind attributes:
Authorization attributes:
Work directory: flash:
User role list: level-15, network-operator
[SW-4-SGTIE-01]
[SW-4-SGTIE-01]
```

Para eliminar un usuario usamos el comando **undo**

```
[ ] local-user ebel.chinchay
```

Para bloquear sin su eliminación

```
[SW-4-SGTIE-01]local-user juan
[SW-4-SGTIE-01]local-user juan
[SW-4-SGTIE-01-luser-manage-juan]st
[SW-4-SGTIE-01-luser-manage-juan]state ?
  active Active state in which local user is allowed to request network
  services
  block Block state in which local user is not allowed to request network
  services

[SW-4-SGTIE-01-luser-manage-juan]state b1
[SW-4-SGTIE-01-luser-manage-juan]state block
```

Para proteger el acceso por consola se debe configurar el puerto de consola, para solicitar clave al momento del ingreso, configurándolo:

```
[SW-4-SGTIE-01]user-interface 0
[SW-4-SGTIE-01-line0]authentication-mode password
[SW-4-SGTIE-01-line0]set authentication password simple igor.2022
[SW-4-SGTIE-01-line0]idle-timeout 2
[SW-4-SGTIE-01-line0]
```

El indicador 0 puede cambiar. Cuando el equipo dispone de más de un puerto por consola, se limite el acceso por inactividad a dos minutos. Para la verificación de la configuración se utilizara el comando **display user-interface aux 0**

Los equipos HP tienen o disponen de cuatro (4) modos de acceso http, https, telnet y ssh. Para este hardening solo se activará el modo ssh, desactivando los demás modos de acceso. Utilizando el comando:

```
[ ] undo ip http enable
[ ] undo ip https enable
[ ] undo telnet server enable
```

Procedemos a configurar nuestro único modo de acceso SSH, para esta configuración se necesitamos generar la clave RSA, activar el SSH en las líneas remotas y habilitar el servicio SSH. El comando **ssh server enable** habilita el servicio, por defecto se habilita ssh versión 2.

```
[SW-4-SGTIE-01]ssh server enable
[SW-4-SGTIE-01]public-key local create rsa
The local key pair already exists.
Confirm to replace it? [Y/N]:y
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:user-interface vty 0 5
Invalid number, the range is (512 ~ 2048).
Input the modulus length [default = 1024]:authentication-mode scheme
Invalid number, the range is (512 ~ 2048).
Input the modulus length [default = 1024]:
Generating Keys...
...+++++
...+++++
.....+++++
.....+++++
Create the key pair successfully.
[SW-4-SGTIE-01]
[SW-4-SGTIE-01]
[SW-4-SGTIE-01]
[SW-4-SGTIE-01]
[SW-4-SGTIE-01]ssh server enable
[SW-4-SGTIE-01]public-key local create rsa
The local key pair already exists.
Confirm to replace it? [Y/N]:y
The range of public key modulus is (512 ~ 2048).
If the key modulus is greater than 512, it will take a few minutes.
Press CTRL+C to abort.
Input the modulus length [default = 1024]:
Generating Keys...
.....+++++
..+++++
...+++++
..+++++
Create the key pair successfully.
[SW-4-SGTIE-01]user-interface vty 0 5
[SW-4-SGTIE-01-line-vty0-5]authentication-mode scheme
[SW-4-SGTIE-01-line-vty0-5]idle-timeout 2
[SW-4-SGTIE-01-line-vty0-5]
```

Se habilita las conexiones remotas ssh, en las líneas virtuales se configura de la 0 a la 5. Se limita la sesión a 2 minutos en caso de inactividad.

Para prevenir problemas de broadcast es necesario limitar el volumen que circulan por la red. Utilizando los siguientes comandos:

```
[SW-4-SGTIE-01]interface GigabitEthernet 1/0/48
[SW-4-SGTIE-01-GigabitEthernet1/0/48]bro
[SW-4-SGTIE-01-GigabitEthernet1/0/48]broadcast-suppression ?
  INTEGER<0-100>  Suppression threshold in percentage
  kbps            Suppression threshold in kbps
  pps            Suppression threshold in pps

[SW-4-SGTIE-01-GigabitEthernet1/0/48]broadcast-suppression 20
[SW-4-SGTIE-01-GigabitEthernet1/0/48]
```

La configuración se realiza a cada interfaz de los equipos, configurando los límites en porcentaje. Para su verificación utilizamos el comando ***display interface gigabitethernet1/0/48***

```
Description: GigabitEthernet1/0/48 Interface
Bandwidth: 1000000kbps
Loopback is not set
Media type is twisted pair
Port hardware type is 1000_BASE_T
Unknown-speed mode, unknown-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
The Maximum Frame Length is 9216
Allow jumbo frame to pass
Broadcast MAX-ratio: 20%
Multicast MAX-ratio: 100%
Unicast MAX-ratio: 100%
PVID: 739
```

```
SW-4-SGTIE-01]arp source-suppression enable
SW-4-SGTIE-01]arp source-suppression limit 10
SW-4-SGTIE-01]
```

Una VLAN divide los dominios de transmisión en un entorno LAN, siempre que los host en una VLAN necesiten comunicarse con host en otra VLAN, debe rutearse el tráfico entre ellos. Esto se conoce como ruteo intervlan, esa configuración se realizara en nuestro firewall.

Para minimizar la inestabilidad de la red y también para evitar cualquier riesgo de seguridad en dispositivos que no sean de confianza se procede a eliminar los

puertos de acceso desde la vlan 1. Se proceden a crear las VLANS en los switch de todos los cuartos de comunicación de acuerdo a los pisos. Ejemplo 4 piso: creación de vlans 409, 411, 403, 401.

```
[SW-4-SGTIE-01]vlan 409
[SW-4-SGTIE-01-vlan409]name SGTIE
[SW-4-SGTIE-01-vlan409]VLAN 411
[SW-4-SGTIE-01-vlan411]NAME GER MUNICIPAL
[SW-4-SGTIE-01-vlan411]VLAN 403
[SW-4-SGTIE-01-vlan403]NAME JURIDICA
[SW-4-SGTIE-01-vlan403]VLAN 401 ALCALDIA
^
% Unrecognized command found at '^' position.
[SW-4-SGTIE-01-vlan403]VLAN 401
[SW-4-SGTIE-01-vlan401]NAME ALCALDIA
[SW-4-SGTIE-01-vlan401]VLAN 737
```

El paso siguiente de la configuración de una vlan es asignar el puerto a una vlan de acceso, realizándolo:

```
[SW-PFIZER4]interface GigabitEthernet 1/0/23
[SW-PFIZER4-GigabitEthernet1/0/23]port link-type access
[SW-PFIZER4-GigabitEthernet1/0/23]port access vlan 739
[SW-PFIZER4-GigabitEthernet1/0/23]
```

En el caso de los enlaces troncales se utiliza el comando trunk

```
[SW-4-SGTIE-01]interface Ten-GigabitEthernet 1/0/52
[SW-4-SGTIE-01-Ten-GigabitEthernet1/0/52]PORT link-type trunk
[SW-4-SGTIE-01-Ten-GigabitEthernet1/0/52]PORT TRUNK PERMIT VLAN 409 411 403 401
737
```

La seguridad de puertos es muy importante, motivo por el cual en este hardening aplicaremos port security. Este es un mecanismo de NAC (network Access Control) basado en la dirección MAC. Es una extensión del IEEE 802.1.X y la autenticación MAC. Previene el acceso no autorizado de dispositivos basándose en la verificación de la dirección MAC de origen, en el tráfico de entrada en el puerto.

Con la seguridad de puertos activada (port security), las tramas cuya dirección MAC de origen no corresponde con una de las aprendidas por el equipo son consideradas ilegales. Detectada las tramas ilegales el equipo toma la acción predefinida automáticamente.

A continuación mostramos una configuración de seguridad de puertos

```
[SW-PFIZER4]port-security enable
[SW-PFIZER4]interface GigabitEthernet 1/0/23
[SW-PFIZER4-GigabitEthernet1/0/23]port-security max-mac-count 1
[SW-PFIZER4-GigabitEthernet1/0/23]port-security port-mode autolearn
[SW-PFIZER4-GigabitEthernet1/0/23]port-security intrusion-mode dis
[SW-PFIZER4-GigabitEthernet1/0/23]port-security intrusion-mode disableport
[SW-PFIZER4-GigabitEthernet1/0/23]
```

En esta configuración habilitamos la seguridad de puertos y en el puerto gigabitethernet1/0/23 aplicamos como máximo una estación, el aprendizaje de la MAC será automático y en el caso que la MAC sea diferente al aprendido el puerto se apaga (deshabilita).

```
interface GigabitEthernet1/0/2
  port-security intrusion-mode disableport
  port-security max-mac-count 1
  port-security port-mode autolearn
  port-security mac-address security sticky f439-090c-4ba9
```

local7	notice	SW-PFIZER4 %PORTSEC/ -IfName=GigabitEthernet1/0/2+MACAddr=805e-c089-885d-VLANId=1-IfStatus=Up; Intrusion detected.
local7	err	SW-PFIZER4 %IFNET/3/P1 GigabitEthernet1/0/2 link status is down.

Como se puede apreciar al conectar otro equipo, y al ser una MAC distinta al autorizado el puerto automáticamente se apaga, tal como se muestra en la imagen obtenido de un reporte “VISUAL SYSLOG SERVER”. En la siguiente imagen se hace una consulta al puerto 1/0/2 del switch a través del comando “**display interface gigabitethernet 1/0/2**”, en el cual se demuestra que el puerto mencionado fue apagado ante la detección de un acceso no autorizado.

```
[SW-4-SGTIE-01]display interface GigabitEthernet 1/0/2
GigabitEthernet1/0/2
Current state: Port Security Disabled
Line protocol state: DOWN
IP Packet Frame Type: PKTFMT_ETHNT_2, Hardware Address: bcea-fa9a-86a1
Description: GigabitEthernet1/0/2 Interface
Bandwidth: 1000000kbps
Loopback is not set
Media type is twisted pair
Port hardware type is 1000_BASE_T
Unknown-speed mode, unknown-duplex mode
Link speed type is autonegotiation, link duplex type is autonegotiation
Flow-control is not enabled
The Maximum Frame Length is 9216
Allow jumbo frame to pass
Broadcast MAX-ratio: 100%
Multicast MAX-ratio: 100%
Unicast MAX-ratio: 100%
VVID: 1
Mdi type: automdix
Port link-type: access
Tagged Vlan: none
Untagged Vlan: 1
Port priority: 0
Last clearing of counters: Never
Peak value of input: 4751102 bytes/sec, at 2022-07-20 11:31:29
Peak value of output: 13078674 bytes/sec, at 2022-07-22 19:51:25
Last 300 seconds input: 0 packets/sec 0 bytes/sec -%
Last 300 seconds output: 0 packets/sec 0 bytes/sec -%
Input (total): 51157254 packets, 57713037709 bytes
49643709 unicasts, 1412343 broadcasts, 101200 multicasts, 0 pauses
Input (normal): 51157252 packets, - bytes
49643709 unicasts, 1412343 broadcasts, 101200 multicasts, 0 pauses
Input: 2 input errors, 0 runts, 0 giants, 0 throttles
2 CRC, 0 frame, - overruns, 0 aborts
- ignored, - parity errors
Output (total): 118866533 packets, 31885864978 bytes
32048800 unicasts, 68840486 broadcasts, 17977247 multicasts, 0 pauses
Output (normal): 118866533 packets, - bytes
32048800 unicasts, 68840486 broadcasts, 17977247 multicasts, 0 pauses
Output: 2 output errors, - underruns, - buffer failures
0 aborts, 0 deferred, 0 collisions, 0 late collisions
2 lost carrier, - no carrier
```

En la entidad se cuenta con áreas donde por falta de infraestructura de hardware se tiene que ampliar puntos de red colocando switch no administrables, por lo que se ve en obligación configurar un máximo de 4 estaciones de aprendizaje MAC automático.

```
[SW-PFIZER4]interface GigabitEthernet 1/0/20
[SW-PFIZER4-GigabitEthernet1/0/20]port-security max-mac-count 4
[SW-PFIZER4-GigabitEthernet1/0/20]port-security port-mode autolearn
[SW-PFIZER4-GigabitEthernet1/0/20]port-security intrusion-mode disableport
[SW-PFIZER4-GigabitEthernet1/0/20]
```

```
[SW-4-SGTIE-01]display port-security
Port security parameters:
  Port security           : Enabled
  AutoLearn aging time   : 0 min
  Disableport timeout    : 20 s
  MAC move                : Denied
  Authorization fail     : Online
NAS-ID profile is not configured
OUI value list          :

GigabitEthernet1/0/2 is link-down
Port mode                : secure
NeedToKnow mode         : Disabled
Intrusion protection mode : DisablePort
Security MAC address attribute
  Learning mode          : Sticky
  Aging type             : Periodical
Max secure MAC addresses : 1
Current secure MAC addresses : 1
Authorization            : Permitted
NAS-ID profile is not configured
```

Se realizó la configuración del ancho de banda de 1 Mbps aproximadamente, donde:

CIR: Es el ancho de banda mínimo que se garantiza que funcione, en condiciones normales, en cualquier momento, el ancho de banda no debe caer debajo de él.

CBS: Cantidad máxima de información que un usuario puede enviar hacia la red.

```
SW-PFIZER4]interface GigabitEthernet 1/0/23
SW-PFIZER4-GigabitEthernet1/0/23]qos lr inbound cir 768 cbs 20480
SW-PFIZER4-GigabitEthernet1/0/23]qos lr outbound cir 768 cbs 20480
SW-PFIZER4-GigabitEthernet1/0/23]
SW-PFIZER4-GigabitEthernet1/0/23]
```

Para la conexión de las vlans se solicitó mediante ticket la creación de estas en el firewall

ID	IP	Host	Group	Protocol	Port	Direction	Action	Status	Priority
91	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	IN	ACCEPT	Disabled	0
92	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	OUT	ACCEPT	Disabled	0
93	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	IN	ACCEPT	Disabled	0
94	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	OUT	ACCEPT	Disabled	0
95	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	IN	ACCEPT	Disabled	0
96	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	OUT	ACCEPT	Disabled	0
97	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	IN	ACCEPT	Disabled	0
98	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	OUT	ACCEPT	Disabled	0
99	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	IN	ACCEPT	Disabled	0
100	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	OUT	ACCEPT	Disabled	0
101	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	IN	ACCEPT	Disabled	0
102	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	OUT	ACCEPT	Disabled	0
103	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	IN	ACCEPT	Disabled	0
104	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	OUT	ACCEPT	Disabled	0
105	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	IN	ACCEPT	Disabled	0
106	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	OUT	ACCEPT	Disabled	0
107	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	IN	ACCEPT	Disabled	0
108	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	OUT	ACCEPT	Disabled	0
109	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	IN	ACCEPT	Disabled	0
110	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	OUT	ACCEPT	Disabled	0
111	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	IN	ACCEPT	Disabled	0
112	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	OUT	ACCEPT	Disabled	0
113	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	IN	ACCEPT	Disabled	0
114	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	OUT	ACCEPT	Disabled	0
115	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	IN	ACCEPT	Disabled	0
116	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	OUT	ACCEPT	Disabled	0
117	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	IN	ACCEPT	Disabled	0
118	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	OUT	ACCEPT	Disabled	0
119	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	IN	ACCEPT	Disabled	0
120	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	OUT	ACCEPT	Disabled	0
121	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	IN	ACCEPT	Disabled	0
122	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	OUT	ACCEPT	Disabled	0
123	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	IN	ACCEPT	Disabled	0
124	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	OUT	ACCEPT	Disabled	0
125	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	IN	ACCEPT	Disabled	0
126	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	OUT	ACCEPT	Disabled	0
127	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	IN	ACCEPT	Disabled	0
128	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	OUT	ACCEPT	Disabled	0
129	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	IN	ACCEPT	Disabled	0
130	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	OUT	ACCEPT	Disabled	0
131	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	IN	ACCEPT	Disabled	0
132	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	OUT	ACCEPT	Disabled	0
133	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	IN	ACCEPT	Disabled	0
134	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	OUT	ACCEPT	Disabled	0
135	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	IN	ACCEPT	Disabled	0
136	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	OUT	ACCEPT	Disabled	0
137	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	IN	ACCEPT	Disabled	0
138	10.10.10.10	10.10.10.10	10.10.10.10	ALL	ALL	OUT	ACCEPT	Disabled	0

Estimado Cliente,

Le ofrecemos las disculpas por la demora en la respuesta, detallo los puntos realizados.

- Las vians 409 y 739 cuentan con internet y hay interconectividad hacia la red 172.16.4.0/22. REALIZADO

Política pasa salida a internet:

ADMIN-SW (VLAN739)	WAN_GTD (wan1)	all	all	always	ALL	ACCEPT
TIE (VLAN409)	WAN_GTD (wan1)	all	all	always	ALL	ACCEPT

Política para comunicación entre redes:

From	To	Source	Destination	Schedule	Service	Action
LAN1 (port1)	TIE (VLAN409)	all	all	always	ALL	ACCEPT
TIE (VLAN409)	LAN1 (port1)	all	all	always	ALL	ACCEPT
ADMIN-SW (VLAN739)	LAN1 (port1)	all	all	always	ALL	ACCEPT
LAN1 (port1)	ADMIN-SW (VLAN739)	all	all	always	ALL	ACCEPT

- La vlan 737 tiene interconectividad hacia la red 172.16.4.0/22, a este segmentó de red habilitar internet. REALIZADO
- A la Vlan 409 habilitar el acceso hacia la DMZ que se encuentra las paginas <http://www.municarabayllo.gob.pe/> y <https://mail.municarabayllo.gob.pe/#4>. REALIZADO

Política para comunicación entre redes:

TIE (VLAN409)	DMZ (port10)	all	all	always	ALL	ACCEPT
DMZ (port10)	TIE (VLAN409)	all	all	always	ALL	ACCEPT

- A la Vlan 409 habilitar el acceso hacia la DMZ que se encuentra las paginas <http://www.municarabayllo.gob.pe/> y <https://mail.municarabayllo.gob.pe/#4>. REALIZADO

Política para comunicación entre redes:

TIE (VLAN409)	DMZ (port10)	all	all	always	ALL	ACCEPT
DMZ (port10)	TIE (VLAN409)	all	all	always	ALL	ACCEPT

Que las VLANs 409, 737 y el segmentó de red 172.16.4.0/22 tengan interconectividad. REALIZADO

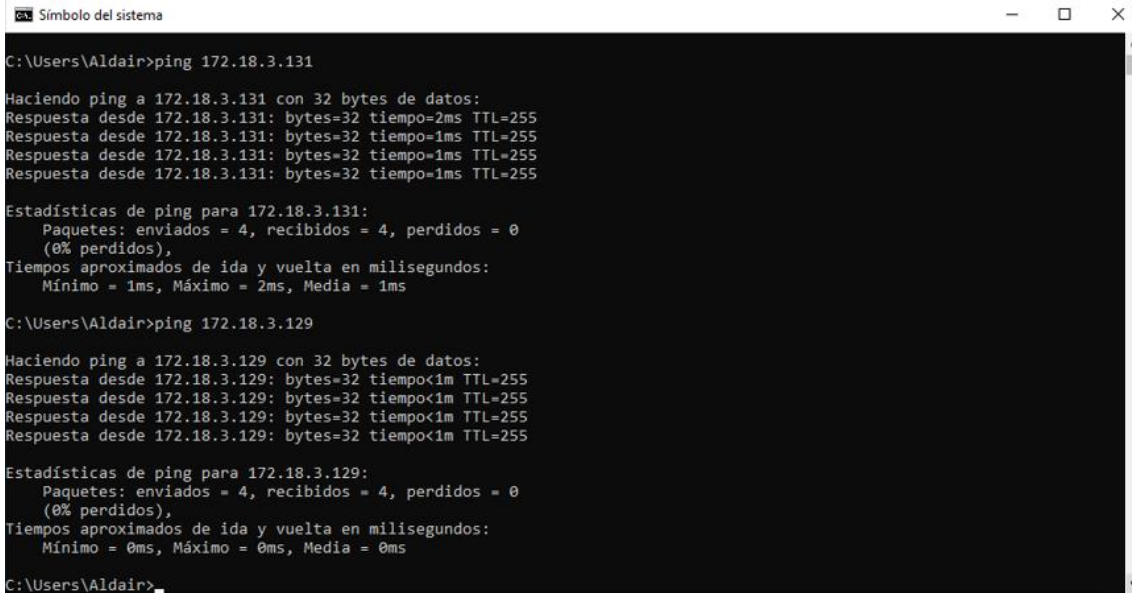
Política para comunicación entre redes:

LAN1 (port1)	TIE (VLAN409)	all	all	always	ALL	ACCEPT
TIE (VLAN409)	LAN1 (port1)	all	all	always	ALL	ACCEPT
LAN1 (port1)	SERVIDORES (VLAN737)	all	all	always	ALL	ACCEPT
SERVIDORES (VLAN737)	LAN1 (port1)	all	all	always	ALL	ACCEPT

Pruebas de conectividad

Prueba de la VLAN 739 ping

739	ADMIN-SW	172.18.3.128	172.18.3.129	172.18.3.158	172.18.3.159	255.255.255.224	/27
-----	----------	--------------	--------------	--------------	--------------	-----------------	-----



```
Símbolo del sistema
C:\Users\Aldair>ping 172.18.3.131

Haciendo ping a 172.18.3.131 con 32 bytes de datos:
Respuesta desde 172.18.3.131: bytes=32 tiempo=2ms TTL=255
Respuesta desde 172.18.3.131: bytes=32 tiempo=1ms TTL=255
Respuesta desde 172.18.3.131: bytes=32 tiempo=1ms TTL=255
Respuesta desde 172.18.3.131: bytes=32 tiempo=1ms TTL=255

Estadísticas de ping para 172.18.3.131:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 1ms, Máximo = 2ms, Media = 1ms

C:\Users\Aldair>ping 172.18.3.129

Haciendo ping a 172.18.3.129 con 32 bytes de datos:
Respuesta desde 172.18.3.129: bytes=32 tiempo<1m TTL=255
Respuesta desde 172.18.3.129: bytes=32 tiempo<1m TTL=255
Respuesta desde 172.18.3.129: bytes=32 tiempo<1m TTL=255
Respuesta desde 172.18.3.129: bytes=32 tiempo<1m TTL=255

Estadísticas de ping para 172.18.3.129:
    Paquetes: enviados = 4, recibidos = 4, perdidos = 0
              (0% perdidos),
    Tiempos aproximados de ida y vuelta en milisegundos:
        Mínimo = 0ms, Máximo = 0ms, Media = 0ms

C:\Users\Aldair>
```



UNIVERSIDAD CÉSAR VALLEJO

**FACULTAD DE INGENIERÍA Y ARQUITECTURA
ESCUELA PROFESIONAL DE INGENIERÍA DE SISTEMAS**

Declaratoria de Autenticidad del Asesor

Yo, RIVERA CRISOSTOMO RENEE, docente de la FACULTAD DE INGENIERÍA Y ARQUITECTURA de la escuela profesional de INGENIERÍA DE SISTEMAS de la UNIVERSIDAD CÉSAR VALLEJO SAC - LIMA NORTE, asesor de Tesis titulada: "Implementación de hardening a nivel de red para mejorar la seguridad de la información en la Municipalidad de Carabaylo, 2021", cuyo autor es CHINCHAY TORIBIO EBEL ALDAIR, constato que la investigación tiene un índice de similitud de %, verificable en el reporte de originalidad del programa Turnitin, el cual ha sido realizado sin filtros, ni exclusiones.

He revisado dicho reporte y concluyo que cada una de las coincidencias detectadas no constituyen plagio. A mi leal saber y entender la Tesis cumple con todas las normas para el uso de citas y referencias establecidas por la Universidad César Vallejo.

En tal sentido, asumo la responsabilidad que corresponda ante cualquier falsedad, ocultamiento u omisión tanto de los documentos como de información aportada, por lo cual me someto a lo dispuesto en las normas académicas vigentes de la Universidad César Vallejo.

LIMA, 03 de Enero del 2022

Apellidos y Nombres del Asesor:	Firma
RIVERA CRISOSTOMO RENEE DNI: 08554321 ORCID: 0000-0002-5496-7036	Firmado electrónicamente por: RERIVERAC el 04- 01-2022 00:25:07

Código documento Trilce: TRI - 0250704