OFICINA DE POSGRADOS

Tema:

PROPUESTA DE MEJORES PRÁCTICAS DE CIBERSEGURIDAD PARA LA COMUNICACIÓN EN REDES DE CLIENTES CORPORATIVOS

Proyecto de Investigación y Desarrollo previo a la obtención del título del Magíster en Ciberseguridad

Línea de Investigación:

Protección de datos y comunicaciones

Autor:

Elías Fernando Allauca Carrillo

Director:

Diego Fernando Ávila Pesántez, PhD.

Ambato – Ecuador

Septiembre 2022

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

SEDE AMBATO

HOJA DE APROBACIÓN

Tema:

PROPUESTA DE MEJORES PRÁCTICAS DE CIBERSEGURIDAD PARA LA COMUNICACIÓN EN REDES DE CLIENTES CORPORATIVOS

Línea de Investigación:

Protección de datos y comunicaciones

Autor:

Elías Fernando Allauca Carrillo

Diego Fernando Ávila Pesantez, Ing. PhD. f._____

CALIFICADOR

Liliana del Rocío Mena Hernández, Ing. MSc. f._____

CALIFICADOR

Enrique Xavier Garces Freire, Ing. MSc. f._____

CALIFICADOR

Juan Carlos Acosta Teneda, P. PhD. f._____

DIRECTOR UNIDAD ACADÉMICA

Hugo Rogelio Altamirano Villarroel, Dr. f._____

SECRETARIO GENERAL PUCESA

Pontificia Universidad Católica del Ecuador
DIRECCIÓN CENTRO DE POSGRADOS
Sede Ambato

Pontificia Universidad Católica del Ecuador
SECRETARÍA GENERAL
PROCURADURÍA

Ambato – Ecuador

Agosto 2022

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD

Yo: **ELIAS FERNANDO ALLAUCA CARRILLO,** con CC. **0604110031** autor del trabajo de graduación intitulado: **"PROPUESTA DE MEJORES PRÁCTICAS DE CIBERSEGURIDAD PARA LA COMUNICACIÓN EN REDES DE CLIENTES CORPORATIVOS"**, previa a la obtención del título profesional de MAGÍSTER EN CIBERSEGURIDAD, en la OFICINA DE POSGRADOS.

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

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

Ambato, agosto 2022

ELIAS FERNADO ALLAUCA CARRILLO

CC. 0604110031

AGRADECIMIENTO

A Dios por brindarme su fuerza y apoyo en este camino arduo para cumplir una de las metas de mi vida, el obtener un título cuarto nivel. A mi familia y en especial a mis padres y hermanos, por su apoyo incondicional en cada decisión que he tomado.

Al PhD. Diego Ávila Pesantez, quien asesoró esta tesis y constantemente me motivó para realizar un buen trabajo.

DEDICATORIA

A Dios por haberme dado fuerza y salud para lograr mis objetivos, a mis padres y hermanos por su apoyo moral e incondicional en cada paso que daba hacia la culminación de mis estudios y por la motivación constante para ser una persona de bien.

RESUMEN

El incremento del uso del servicio de internet y conectividad entre agencias mediante una red de datos ha ocasionado que la disponibilidad de los servicios se mantenga en un porcentaje alto, perder conectividad o presentar intermitencias, llevará consigo una pérdida económica de los clientes corporativos, quienes al tener bajos recursos o no aplicar de manera adecuada las políticas y técnicas de seguridad no logran proteger sus redes internas de manera adecuada frente a ciberataques. Esto ocasiona inconvenientes a los ISP (Proveedores del Servicio de Internet) que se ven obligados a tomar acciones para mitigar la afectación en sus enlaces. Por lo que, resulta importante, que se apliquen un conjunto de buenas prácticas de seguridad tanto en clientes como en el ISP para mantener la comunicación activa. Él presente proyecto tiene como objetivo proponer las mejores prácticas de ciberseguridad a nivel de infraestructura de red para los clientes corporativos de un ISP. Se utilizó la metodología cualitativa aplicada a un grupo de clientes ya establecidos que han sufrido mayor cantidad de inconvenientes con el servicio. Con un diseño experimental se confirmó que el rendimiento de los clientes de datos fijos corporativos mejora, posterior a la aplicabilidad de las recomendaciones brindadas por parte del ISP.

Palabras claves: ciberseguridad, vulnerabilidad, políticas, infraestructura de red.

ABSTRACT

The increase in the use of internet service and connectivity between agencies through a data network has caused the availability of services to be maintained at a high percentage. Loss of connectivity or intermittency can lead to economic losses for corporate clients, who, due to low resources or the failure to adequately apply security policies and techniques, are unable to protect their internal networks adequately against cyber-attacks. This causes inconvenience to Internet Service Providers (ISPs) who are forced to take action to mitigate the impact on their links. Therefore, it is important to apply a set of good practices in both clients and ISPs to maintain active communication. The objective of this project is to propose the best cybersecurity practices at the network infrastructure level for the corporate clients of an ISP. A qualitative methodology was used, applied to a group of established customers who have suffered the most problems with the service. With an experimental design it was confirmed that the performance of corporate fixed data clients improves, after the applicability of the recommendations provided by the ISP.

Keywords: cybersecurity, vulnerability, security policies, network infrastructure.

ÍNDICE GENERAL

DECLARACIÓN DE AUTENTICIDAD Y RESPONSABILIDAD iii
AGRADECIMIENTO iv
DEDICATORIA v
ABSTRACT vii
ÍNDICE GENERAL viii
ÍNDICE DE TABLAS ix
ÍNDICE DE CUADROS x
ÍNDICE DE FIGURAS xi
INTRODUCCIÓN 1
1.1. Antecedentes 5
1.2. Prácticas de seguridad 6
1.3. ISO 27000 7
1.4. Estándar ISO 27032 8
1.5. Redes corporativas 15
CAPÍTULO II. DISEÑO METODOLÓGICO 24
2.1. Metodología de Investigación 24
2.2. Metodología de desarrollo 29
CAPÍTULO III. ANÁLISIS Y VALIDACIÓN DE RESULTADOS 39
3.1. Reportes de problemas de clientes corporativos 39
3.2. Casos de cliente corporativos de un ISP 39
3.3. Validación de la propuesta de solución 60
3.4. Verificación de la hipótesis 81
CONCLUSIONES 89
RECOMENDACIONES 90
BIBLIOGRAFÍA 91
ANEXOS 97

ÍNDICE DE TABLAS

Tabla 1. ISP del Ecuador 16
Tabla 2. Latencia de los casos analizados 81
Tabla 3. Disponibilidad del servicio de los casos analizados 82
Tabla 4. Calculo valor t-student latencia 85
Tabla 5. Prueba t-student disponibilidad 87

ÍNDICE DE CUADROS

Cuadro 1. Controles norma ISO 27000 10
Cuadro 2. Registro principales reportes 27
Cuadro 3. Encuesta de reportes ISP 32
Cuadro 4. Propuestas de mejores prácticas de seguridad 35
Cuadro 5. Caso 001.- Sin servicio 40
Cuadro 6.Caso 002.- Intermitencia del servicio 41
Cuadro 7. Caso 003.- Bloqueo de Salida de correo 43
Cuadro 8. Caso 004.- Ingreso no autorizado de equipos 45
Cuadro 9. Caso 005.- Phishing 47
Cuadro 10. Caso 006.- Lista negra UCEPROTECT 49
Cuadro11. Caso 007.- Ransomware 50
Cuadro 12. Caso 008.- Denegación de servicio 52
Cuadro 13. Caso 009.- Reporte vulnerabilidad 55
Cuadro 14. Caso 010.- Ataque Phishing 58
Cuadro 15. Monitoreo Caso 001.- Sin servicio 60
Cuadro 16. Monitoreo Caso 002.- Intermitencia del servicio 63
Cuadro 17. Monitoreo Caso 003.- Bloqueo de Salida de correo 65
Cuadro 18. Monitoreo Caso 004.- Ingreso no autorizado de equipos 67
Cuadro 19. Monitoreo Caso 005.- Phishing 69
Cuadro 20. Monitoreo Caso 006.- Lista negra UCEPROTECT 71
Cuadro 21. Monitoreo Caso 007.- Ransomware 73
Cuadro 22. Monitoreo Caso 008.- Denegación de servicio 75
Cuadro 23. Monitoreo Caso 009.- Escaneo de puertos 77
Cuadro 24. Monitoreo 010.- Ataque Phishing 79

ÍNDICE DE FIGURAS

Figura 1. Series Norma ISO 27000 8
Figura 2. Guía de técnicas ISO 27000 9
Figura 3. Guía de técnicas ISO 27032 12
Figura 4. Conexión red 13
Figura 5. Estructura Internet 16
Figura 6. ASN ISP Ecuador 17
Figura 7. MPLS vs SD WAN 18
Figura 8. Servidor DHCP 21
Figura 9. Conexión red 22
Figura 10. Variables del proyecto de investigación 26
Figura 11. Logs equipo 28
Figura 12. IPs de alto impacto 28
Figura 13. Modelo de mejora continúa 29
Figura 14. Actividades etapa diagnóstico 30
Figura 15. Actividades etapa ejecución 33
Figura 16. Actividades etapa verificación 37
Figura 17. Prueba de normalidad Ryan-Joiner latencia. 83
Figura 18: Prueba de normalidad Ryan-Joiner disponibilidad 83
Figura 19. Normalidad de las variables. 84
Figura 20. Gráfica distribución latencia 85
Figura 21. Gráfica valores individuales y de caja latencia 86
Figura 22. Gráfica distribución disponibilidad 87
Figura 23. Gráfica valores individuales y de caja, disponibilidad 88

INTRODUCCIÓN

En la actualidad, mantener a los usuarios de internet protegidos de los ciberataques y otras amenazas es uno de los desafíos de seguridad para los proveedores de servicio de internet (ISP). De acuerdo con los últimos datos de ESET Security *Report* 2021, el 34% de los incidentes que sufrieron el último año las empresas latinoamericanas fue debido a los códigos maliciosos, donde los países más afectados fueron Brasil, México, Argentina, Colombia, Perú y Ecuador (Datta Business Innovation 2021).

El uso de las tecnologías en las empresas permite tener un acercamiento global con los clientes, mediante los diversos métodos de comunicación que existen en la actualidad, lo que permite expandir sus ventas y aumentar sus ingresos. Lastimosamente, esto no solo trae beneficios para las empresas, si no se implementan medidas de ciberseguridad y se gestiona el riesgo, tanto en la infraestructura tecnológica como en los procesos del giro del negocio, las empresas se enfrentarán a una gran cantidad de amenazas que, si un ciberdelincuente aprovecha las vulnerabilidades, comprometerán seriamente sus activos de información.

Es común ver que varias compañías o empresas, tanto públicas como privadas de nuestro país, han sufrido constantes ataques a su red, al ser vulnerado su sistema, pierden credibilidad de sus usuarios. Esto se evidencia con el último informe anual de seguridad de *Kaspersky* que revela que en Ecuador existe un crecimiento del 75% en cuanto a los ataques informáticos, es decir, hay alrededor de 89 ataques por minuto (latam.kaspersky., 2021). Según varios expertos nacionales en el ámbito de la seguridad, indican que, esto afecta no solo a las empresas grandes o a los bancos, como ocurría en el pasado, sino que cada vez hay más interés por la información de las pequeñas y medianas empresas (pymes), lo más usual es ver ataque por malware por medio de robo de identidad. Los inconvenientes más frecuentes que se presentan en el servicio es la caída del rango de IP en listas negras, saturación, intermitencias, ingreso de correos sospechosos, intentos de acceso a los equipos de personal no

autorizado y otros métodos que utilizan los atacantes para vulnerar su sistema de seguridad.

La falta de aplicación de técnicas o políticas de seguridad de los clientes de datos fijos corporativos en sus redes internas acarrean grandes inconvenientes a su ISP, lo que ocasiona incluso que se vean afectados otros clientes. Por lo que es fundamental trabajar en conjunto en la ejecución de un análisis de las mejores técnicas y métodos de seguridad a implementar, muchos ciberataques se propagan a través de mecanismos que aprovechan las debilidades que se encuentran en los usuarios finales, lo que convierte a los usuarios en el elemento más débil de la cadena de seguridad, para lo cual, las empresas tienen la obligación de impartir capacitaciones constantes para aprender cómo funciona la ingeniería social y conocer cuáles son las formas más comunes de ataques.

Existen varias normas o estándares de seguridad establecidas por la ISO (Organización Internacional para la Estandarización), entre las cuales se encuentra la norma ISO 27032, la misma que ofrece el uso de buenas prácticas de seguridad aplicables para el ámbito de la protección de la información. Además, brinda herramientas para gestionarla dentro de una organización, que permite contar con procesos de protección de operaciones y de las actividades que se realicen en línea, del software que se utilice, manejo de datos, servicios, capacitar al personal encargado del manejo de estas herramientas.

Esta normativa se creó con dos fines, el primero es cubrir aspectos de ciberseguridad que no se habían tocado en versiones anteriores y promover la cooperación entre agentes como CSF, *CyberSecurity Framework* y el Marco de Ciberseguridad del NITS. Además, se enfocaba en cuatro ejes, las cuales son seguridad de la información, seguridad de las redes, seguridad en Internet y la protección de infraestructuras críticas para la información (piranirisk, 2020).

La norma ISO 27032 se centra en los cuatro ejes anteriores y propone un marco seguro para compartir información y los procesos necesarios para resolver cualquier incidente de seguridad que surja. Además, brinda herramientas para la gestión dentro de su organización, habilitar procesos y actividades para proteger las operaciones que se realizan en línea, la gestión de datos, los servicios y la capacitación del personal encargado del manejo de estas herramientas.

Con este antecedente, el problema científico de la investigación en este trabajo se define: ¿Cómo influye la aplicabilidad de mejores prácticas de ciberseguridad en el rendimiento de la red de los clientes corporativos dentro de un ISP?, y la hipótesis de trabajo se establece como: La propuesta de mejores prácticas a nivel de infraestructura de red a los clientes corporativos mejora el rendimiento de red, disminuye el reporte de incidentes del servicio a su proveedor.

Por tal motivo, la presente investigación tiene como objetivo general proponer las mejores prácticas de ciberseguridad a nivel de infraestructura de red de clientes corporativos de un proveedor de servicio de internet, para el cumplimiento se plantea los siguientes objetivos específicos:

1. Describir los principales problemas de ciberseguridad de clientes corporativos en la infraestructura de un ISP, que sirva de base para la propuesta de solución.
2. Realizar un estudio comparativo de los diferentes ataques de ciberseguridad que se han producido en los clientes corporativos dentro de un ISP.
3. Definir un conjunto de recomendaciones a nivel de la red LAN (Red de Área Local) de clientes corporativos para mitigar la afectación del servicio a los clientes corporativos.

Se utilizó la metodología cualitativa aplicada a un grupo de clientes ya establecidos, que han sufrido mayor cantidad de inconvenientes con el servicio, con un diseño experimental con el que se pretende confirmar si el rendimiento de los clientes de datos

fijos corporativos mejora, posterior a la aplicabilidad de las recomendaciones brindadas por parte de su proveedor de servicio.

Para lo cual, se basa en casos de reportes de clientes y establecer un análisis de cada escenario, con el fin de determinar la causa del inconveniente y realizar las recomendaciones necesarias para que se ejecute las acciones correctivas a nivel de la red LAN de cada cliente, aplicar los métodos de seguridad a nivel de la infraestructura del ISP mediante reglas a nivel de la red y el análisis del tráfico.

Además, se necesita ejecutar una revisión bibliográfica sobre las principales recomendaciones y mecanismos que protejan contra los principales ataques basados en la red, como el escaneo de vulnerabilidades, los ataques de intrusión, escucha de red, alteración de datos y los ataques de denegación de servicio (DoS), para establecer un conjunto de recomendaciones de seguridad, las mismas que se aplique en la red interna, una organización al tener varios dispositivos que están interconectados en la red interna, es una puerta para que los atacantes vulneren el sistema de seguridad, por lo que es de gran importancia generar las mejores prácticas de seguridad para mitigar un daño en la continuidad del servicio.

CAPÍTULO I. ESTADO DEL ARTE Y LA PRÁCTICA

1.1. Antecedentes

La exposición de los activos de información al complejo entorno del ciberespacio conlleva una variedad de riesgos de ciberseguridad que ponen en peligro la disponibilidad, integridad y confidencialidad de la información organizacional, razón por lo cual, es necesario, implementar métodos y técnicas de seguridad que permitan mitigar una posible afectación del servicio, un sistema de gestión automatizado basado en buenas prácticas de ciberseguridad, como la Organización Internacional de Estandarización (ISO) 27032, permite asegurar los pilares de la seguridad de la información en una organización. En este contexto, se pretende conocer los principales ataques que sufren un ISP y las recomendaciones de ciberseguridad se recomienda a sus suscriptores para que no presenten inconvenientes en su servicio.

Existen varios estudios e investigaciones que se realizan sobre la importancia de un sistema de seguridad y aplicabilidad de la norma ISO 27032, como el realizado por Guzmán Solano, Sandra Liliana (Guzmán Solano 2019). Que es una guía para la implementación de la norma ISO 27032 en empresas de Colombia, en este trabajo contiene el análisis del estado de la Ciberseguridad en su país y la guía para que las organizaciones implementen controles bajo las mejores prácticas de seguridad determinadas en la norma ISO 27032.

Sobre la importancia de que las organizaciones mantenga la información de una manera segura, en la actualidad ya no solo abarca organizaciones que trabaje en el área de TI, sino, a todas las organizaciones en general, un artículo científico denominada *Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria* presentado por estudiantes de la Universidad de Murcia crean esta guía con el fin que se utilice como una orientación sobre buenas conductas y hábitos del personal sanitario en el tratamiento de los datos, y ayudar en la formación de estos profesionales. Esta guía

se utilizaba para evaluar y auditar el comportamiento en materia de seguridad del trabajador por parte de los responsables de seguridad informática del centro de AP (Sánchez-Henarejos et al. 2014), por lo que con la gran evolución de la tecnología, conectividad y crecimiento del teletrabajo ha generado aumento significativo de ataques informáticos, se ve importante en la actualidad generar una guía actualizada sobre las mejores prácticas de seguridad que se emplea en una organización.

1.2. Prácticas de seguridad

Las buenas prácticas de seguridad en una organización son de suma importancia en la actualidad, permite proteger de forma adecuada la información sensible de una organización, para lo cual, se emplearía, una correcta gestión de la seguridad de la información, en donde se establecería como principio básico los tres elementos importantes de la seguridad como es la confidencialidad, integridad y disponibilidad.

La confidencialidad es el proceso que asegura que la información sea accesible solo para aquellos usuarios que cuenten con autorización a tener acceso a la misma. Es el principio básico de la política de seguridad en una organización. El acceso a esta información es estrictamente controlado de acuerdo con las consideraciones legales y éticas para asegurar que solo sea para el personal autorizado.

El segundo pilar, la integridad, se refiere a la obligación de garantizar que la información sea exacta y no se modifique de manera no autorizada, por último, la disponibilidad consiste en garantizar que se proporcione información a los usuarios autorizados en el momento en que se requiere, una vez ya con la explicación con la definición de los elementos de la tríada CIA se analiza a detalle las mejores prácticas de seguridad que se implementa para la protección de información, sin embargo, la tríada CIA ha sido muy criticada en la última década, por varios especialistas en el campo de la seguridad indican que no abarca en su totalidad los requerimientos básicos de seguridad que se demandan en la actualidad, por lo que el científico Donn Parker propuso otros tres pilares que complementan a la tríada las cuales son: control,

autenticidad y utilidad con lo que se formó el denominado hexágono Parkeriano (Briceño 2021).

La mayoría de las organizaciones emplean la tríada CIA para revisar todos los mecanismos de seguridad para la continuidad del negocio y minimizar los riegos de un ataque informático, sin embargo, no se trata de solo utilizar los tres o uno de elementos, se utiliza todos de manera equilibrada y así tener un modelo de seguridad robusta a los ciberataques.

1.3. ISO 27000

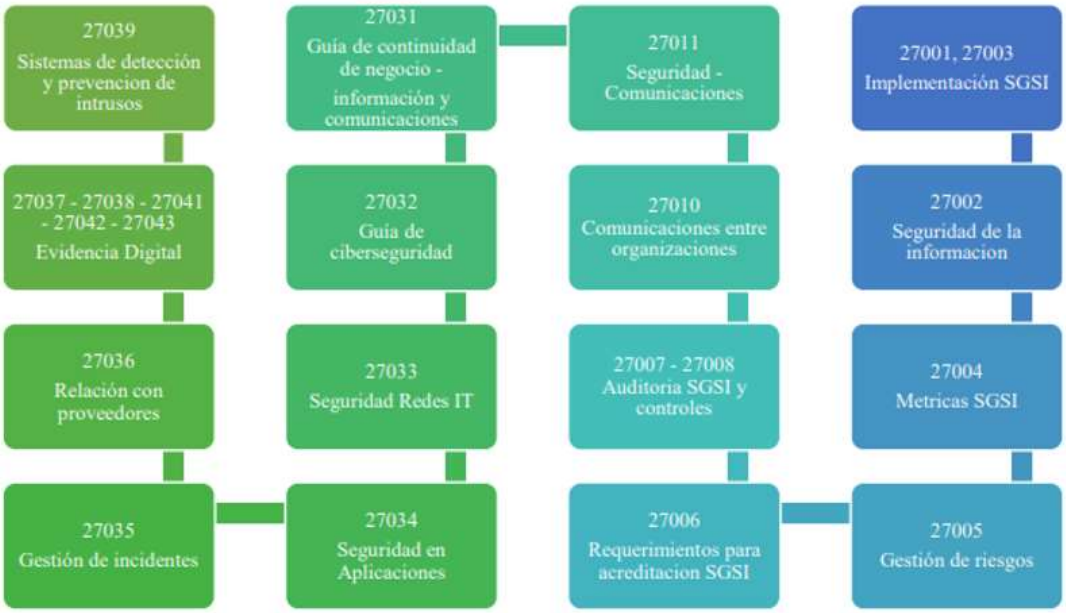
Con el desarrollo de la tecnología en las compañías han permitido automatizar la mayoría de los procesos, permite que tengan un mayor crecimiento en el mercado que se desarrollan, con lo cual, nace la importancia de una buena aplicabilidad de las mejores prácticas de seguridad, la Organización Internacional de Estandarización (ISO) recoge un extenso número de normas dentro de la familia de ISO 27000 que permite apoyar al desarrollo en tema de seguridad en las tecnologías de la información (TI).

La ISO 27000 fue publicada el 1 de mayo de 2009, revisada con una segunda edición de 01 de diciembre de 2012, una tercera edición de 14 de enero de 2014 y una cuarta en febrero de 2016. Esta norma proporciona una visión general de las normas que componen la serie 27000, indica para cada una de ellas su alcance de actuación y el propósito de su publicación. Recoge todas las definiciones para la serie de normas 27000 y aporta las bases de por qué es importante la implementación de un sistema de Gestión de Seguridad de la Información (SGSI) (ISO 27000 2021).

La primera norma con un estándar certificable es la ISO 27001, la cual, permite a las organizaciones contar con los lineamientos mínimos para garantizar la integridad, confidencialidad y disponibilidad de la información, pero adicionalmente se han creado otros estándares, los cuales apoyan la implementación del SGSI, como es la ISO

27032. En la figura 1 se observa un resumen de un listado de buenas prácticas de seguridad definidas para el aseguramiento de la información en las organizaciones desde diferentes aspectos claves (Guzmán Solano 2019).

Figura 1. Series Norma ISO 27000



Fuente: Tomado a partir de Guzmán Solano (2019).

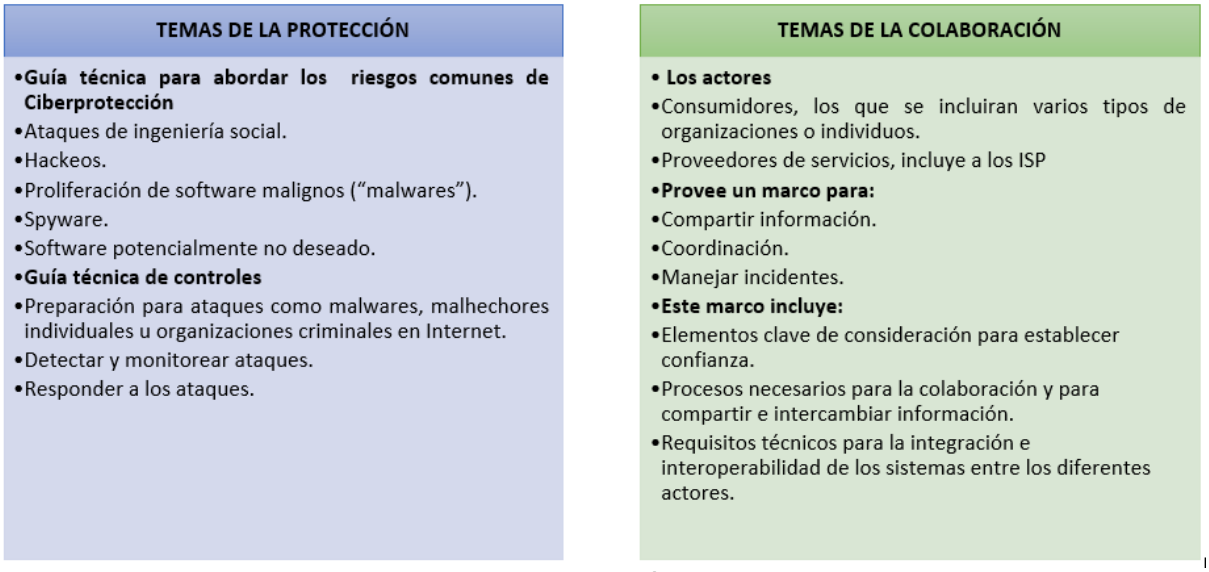
1.4. Estándar ISO 27032

El estándar ISO 27032 fue publicado en julio del año 2012, la cual, es una guía que abarca la mejora del estado de la ciberseguridad en una organización, la norma indica que hay asuntos de seguridad que no son cubiertos por las buenas prácticas actuales de protección de la información, protección de Internet, protección de red y protección de TIC, debido a que existen brechas entre estos dominios y la falta de comunicación entre las organizaciones y su ISP, como los dispositivos de red y las redes que dan servicio de acceso al ciberespacio, cada uno con sus problemas comerciales, de operaciones y regulaciones que no ha permitido abarcar en su totalidad la protección de la información.

Esta guía facilita las mejores técnicas para abordar los riegos comunes de ciberseguridad como los ataques, para lo cual, abarca dos áreas, en la figura 2 se

observa un cuadro resumen de las áreas que abarca la norma ISO 27032, en la misma se describe cada función.

Figura 2. Guía de técnicas ISO 27000



Fuente: elaboración propia

La norma ISO/IEC 27032 proporciona un marco de orientación para mejorar el estado de la Ciberseguridad, usa para ello los aspectos estratégicos y técnicos relevantes para esa actividad adicional como primera instancia la norma indica que se comprende la naturaleza de la ciberseguridad para que la utilidad del ciberespacio prevalezca, las partes interesadas en el Ciberespacio, contienen un plan activo, lo que significa ir más allá de proteger sus propios activos. Como preparar a las personas y organizaciones para los riesgos y desafíos de seguridad emergentes para una prevención y respuesta efectivas a los malos usos y explotaciones criminales.

La norma ha identificado cinco funciones clave necesarias para la protección de los activos digitales. La cual, indica que se ejecutarían las siguientes actividades:

- **Identificar:** Utilice la comprensión de la organización para minimizar el riesgo de los sistemas, activos, datos y capacidades.

- **Proteger:** Diseño salvaguardias para limitar el impacto de los eventos potenciales sobre los servicios y las infraestructuras críticas.
- **Detectar**: Ejecutar actividades para identificar la ocurrencia de un evento de ciberseguridad.
- **Responder:** Tomar las medidas apropiadas después de enterarse de un evento de seguridad.
- **Recuperar:** Planificar la capacidad de recuperación y la reparación oportuna de capacidades y servicios comprometidos.

Una vez que se identifican los riesgos a la Ciberseguridad y se bosquejan las directrices apropiadas, se seleccionaran e implementaran los controles de Ciberprotección que apoyan a los requisitos de seguridad. Esta cláusula da una visión general de los controles clave de Ciberprotección que se implementaría para apoyar las directrices especificadas en esta norma, el cuadro 1 indica el control y las descripciones generales de cada una de ellas.

Cuadro 1. Controles norma ISO 27000

CONTROL	DESCRIPCIÓN GENERAL
Controles a nivel de aplicación	• Exponer notificaciones cortas con resúmenes claros, concisos sobre el tema de políticas de seguridad. • Asegurar el manejo de sesiones para las aplicaciones Web. Esto incluye mecanismos online como cookies. • Asegurar la validación y manejo de las entradas para prevenir ataques comunes, tales como la Inyección SQL. • Asegurar el scripting de la página Web para prevenir ataques comunes como las Secuencias de órdenes en Sitios Cruzados o Cross-site Scripting. • Revisar y testear la seguridad de los códigos por medios de entidades cualificadas apropiadamente. Que el proveedor use un subdominio desde un nombre de dominio con marca registrada de la organización y posiblemente el uso de credenciales HTTPS registrado a nombre de la organización.
Protección del servidor	• Configurar los servidores, incluye los sistemas operativos subyacentes, de acuerdo con una guía de configuración de seguridad base. Reforzar los controles de acceso en los directorios y archivos de programa y sistema y habilitar el registro de auditoría de, particularmente, la seguridad y otros eventos de fallas en el sistema. Es más, se recomienda instalar

	un sistema mínimo en un servidor para reducir el vector de ataque. • Implementar un sistema para probar e implementar actualizaciones de seguridad y asegurarse de que el sistema operativo y aplicaciones del servidor se mantengan actualizados. • Revisar la configuración de seguridad y seguimiento del desempeño de seguridad del servidor. • Hacer escaneos constantes en busca de posibles vulnerabilidades y ejecutar controles *anti-software* malicioso (como *spyware* o *malware*) en el servidor. • Escanear todo el contenido alojado y subido, de manera regular, usar controles actualizados *anti-software* malicioso y realizar evaluaciones de vulnerabilidades y pruebas de seguridad de manera constante.
Controles para los usuarios finales	• El sistema operativo y el software de aplicación se actualizarían con respecto a los parches de seguridad. • Usar herramientas anti-virus y *anti-spywares*, el *software* de seguridad se actualizaría con respecto a los parches de seguridad y a las bases de datos de firmas. • Los navegadores Web y barras de herramientas de navegador comunes que incorporen capacidades como bloqueadores de pop-ups que evitan que sitios Web maliciosos muestren ventanas que contienen *spyware* o software engañoso. • Los navegadores proveerán alertas, normalmente en forma de resaltos codificados con color, para advertir a los usuarios del potencial riesgo. Las organizaciones establecerán una política para habilitar el uso de dicha herramienta. • Los proveedores de servicios fomentarán el uso de funciones de firewall y HIDS personales y/o sugerir otros productos de firewall y HIDS personales de terceros que han sido evaluados y considerados como confiables, además, de educar y ayudar a los usuarios a habilitar una seguridad de red básica a nivel de sistema de usuario final. • Las aplicaciones en las que confían los usuarios (por ejemplo, productos antispyware y antivirus) se habilitaran para que realicen actualizaciones automáticas. Esto asegura que los sistemas se actualicen con los últimos parches de seguridad.
Controles contra los ataques de ingeniería social	• Desarrollar y documentar controles de seguridad específicos para la protección contra la exposición accidental y el acceso no autorizado intencional. • Publicar procedimiento de cómo manejar las propiedades intelectuales de una compañía, los datos personales y otra información confidencial • Acuerdo de política de seguridad con el proveedor de servicios. • Que los usuarios cursen un número mínimo de horas de formación para asegurar que estén conscientes de sus roles y responsabilidades en el Ciberespacio, además, de los controles técnicos que estos implementarían como individuos al usar el Ciberespacio. • Las personas necesitan estar conscientes de los riesgos relacionados en el Ciberespacio, y las organizaciones establecerán políticas pertinentes y dar pasos proactivos para

	patrocinar programas relacionados para asegurar la conciencia y competencia de las personas. • Se considera la provisión de soluciones de autenticación sólidas, ya sea como parte de la autenticación de acceso y/o cuando se ejecuten transacciones críticas. • Usar un "Certificado de Alta Seguridad" para proporcionar una seguridad adicional a los usuarios online.
Disposición de la Ciber protección	• Controles técnicos adicionales que se aplicaran para mejorar la disposición en el área de detección de eventos, a través de una *Darknet* para Seguimiento; la investigación, a través de *Tracebacks*; y la respuesta, a través de una Operación *Sinkhole*, como parte de la Ciber protección de una organización.
Otros Controles	• Otros controles incluirán algunos relacionados con la alerta y cuarentena de dispositivos que están comprometidos en actividades sospechosas u observadas, a través de la correlación de eventos desde los elementos del ISP o empresa como los servidores DNS, el flujo de red de router, la filtración de mensajes salientes y las comunicaciones *peer-to-peer*.

Autor: Tomado de la norma ISO 27000

Además, de los controles mencionados, esta norma proporciona una guía para mejorar el estado de la ciberseguridad, resalta los aspectos importantes de esa actividad y sus dependencias en otros dominios de protección, como se muestra en la figura 3.

Figura 3. Guía de técnicas ISO 27032

Fuente: Tomado de isecauditors (2021)

1.4.1. Seguridad de la información

La seguridad de la información es un término que cada vez es más común y se escucha con mayor frecuencia, porque gran mayoría de las personas sabe que la información es un activo muy importante. Por lo tanto, se protege de manera correcta.

La seguridad de la información tiene como objetivo minimizar estos riesgos de información a un nivel aceptable. Es necesario aclarar que, si se refiere a información, es a toda la información, sin importar en qué formato aparezca, ya sea físico, digital u otro medio.

Según la norma ISO 27032 indica que la seguridad de la información se preocupa de la protección de la confidencialidad, integridad y disponibilidad de la información en general, para responder con las necesidades del usuario en cuanto a la información aplicable.

1.4.2. Seguridad de las redes

El objetivo de la Seguridad es evitar riesgos potenciales, tanto accidentales como intencionados, de ataque, robo o daño que provocaran la interrupción total o parcial de las operaciones de la empresa. El desarrollo de la conectividad, los sistemas abiertos, el uso común de redes y la explosión de Internet hacen que el acceso a la información ya no esté limitado a unos pocos, lo cual implica, al mismo tiempo, que la información se encuentre expuestos a múltiples amenazas, en el ciberespacio.

Una red realiza el enrutamiento de datos entre hosts, una red es LAN o WAN (red de área amplia), en la figura 4 se verifica la conexión, una LAN es una red que conecta hosts, se trata de una red privada desplegada por las empresas, una red WAN interconecta varias redes LAN, es una red de tipo pública desplegada por operadores de acceso y tránsito de internet (Pérez 2020).

Figura 4. Conexión red

Fuente: Tomado Pérez (2020)

La norma ISO 27032 indica que la protección de red se preocupa del diseño, implementación y operación de las redes para lograr los propósitos de seguridad de la información en las redes dentro de las organizaciones, entre organizaciones y entre las organizaciones y los usuarios.

1.4.3. Seguridad en Internet

Internet ha pasado por cuatro fases distintas en los últimos 30 años, las cuales son fases académica, comercial, transaccional y social. Los servicios que allí se brindan se han convertido en una parte esencial de nuestras vidas. Además, la explosión de la conectividad ubicua a través del uso masivo de dispositivos móviles inteligentes, especialmente *Smartphones*, y redes de datos móviles cada vez más rápidas, hace que todos estos servicios se utilicen en cualquier lugar y en cualquier momento del día o de la noche, por lo que hablar sobre "personas conectadas" en lugar de computadoras y dispositivos conectados, por lo que es importante promover el uso seguro y responsable de Internet, explicar los riesgos a los que están expuestos los usuarios y proporcionar las instrucciones necesarias para aprovechar los servicios sin comprometer nuestra seguridad y confidencialidad.

La norma ISO especifica que la protección de Internet se refiere a la protección de los servicios relacionados con Internet y los sistemas y redes relacionados con las TIC como una extensión de la protección de redes en organizaciones y hogares para lograr el objetivo de protección. La protección de Internet también asegura la confiabilidad, disponibilidad e integridad de los servicios de Internet.

1.4.4. Protección de la Infraestructura Crítica de la Información (CIIP)

CIIP es un tema complejo, pero también importante para los países. En general, los países dependen en gran medida de los servicios de infraestructura esenciales, como la electricidad, las telecomunicaciones, los sistemas financieros, el agua potable y los servicios gubernamentales.

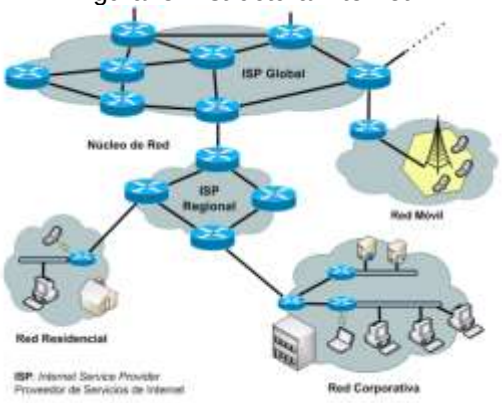
De acuerdo con la norma ISO 27032, CIIP se ocupa de la protección de los sistemas proporcionados u operados por proveedores de infraestructura crítica, como servicios de energía, telecomunicaciones y agua. CIIP garantiza que estos sistemas y redes estén protegidos contra los riesgos de protección de la información, los riesgos de protección de la red, los riesgos de protección de Internet y los riesgos de Ciberseguridad.

1.5. Redes corporativas

La red corporativa permite conectar todas las localizaciones de la empresa de una forma permanente, privada, segura y fiable a través de las diferentes tecnologías de comunicación, el producto red corporativa permite a la empresa cursar todas sus comunicaciones, ya sean datos, voz, vídeo o imágenes, de un modo rápido y seguro.

De esta forma se asegura el correcto tratamiento a los distintos tipos de tráfico, además, permite a través de un panel de control conocer en cualquier momento el estado de la red, en la figura 5 representa los distintos tipos de redes de acceso desde un punto de vista estructural, entre las cuales se destacan las redes residenciales, como su nombre lo indica es el internet en el hogar, las redes corporativas, son las redes existentes en edificios más grandes, como empresas o universidades que se interconectan entre las distintas sucursales dentro de un país y las redes móviles las mismas que se conectan a una estación base con la mayor cobertura posible.

Figura 5. Estructura Internet



Fuente: http://vishub.org/pictures/4626.jpeg

1.5.1. Proveedor de servicio de internet ISP

Los ISP comenzaron a surgir a finales de 1980 y principios de 1990, son las empresas y organizaciones que proporcionan acceso a Internet y servicios relacionados a los usuarios. Estos proveedores conectan a los clientes de otros proveedores de servicio por medio de redes. A menudo, los ISP son empresas que proporcionan servicios de telecomunicaciones, entre ellos, acceso a las comunicaciones de datos y la conexión telefónica, o incluso acceso a la televisión por cable. ISP es el término con el que se identifica a las compañías que proporcionan acceso a Internet, tanto a los hogares como a otras empresas, en la figura 6 se describe los principales ISP del país con su respectivo número de sistema autónomo (ASN) y en la tabla 1 se registra los mayores ISP con el número de IP asignadas.

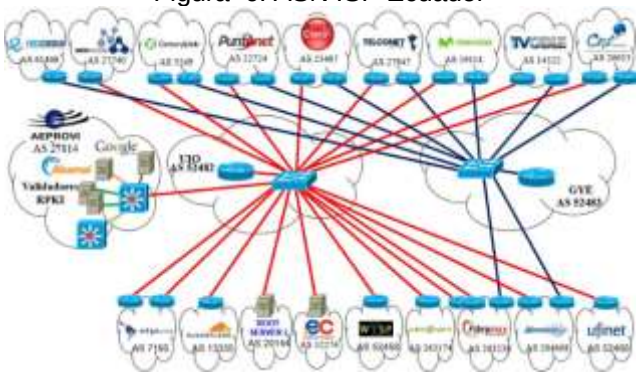
Tabla 1. ISP del Ecuador

ASN	NAME	NUM IPS
AS27947	Telconet S.A	531200

AS28006	CNT	312832
AS27668	ETAPA EP	124928
AS23487	CONECEL	82176
AS22724	PUNTONET S.A.	77568
AS264668	NEDETEL S.A.	62464
AS19114	Otecel S.A.	57088

Fuente: elaboración propia

Figura 6. ASN ISP Ecuador



Fuente: Sitio web de Aeprovid (2020)

1.5.2. Tecnologías para la comunicación clientes corporativos

La interconexión para la comunicación entre clientes corporativos se las realiza de manera segura mediante varias tecnologías de conmutación, entre las principales se tiene la conmutación de etiquetas multiprotocolo (MPLS) y la red de área amplia (SD WAN).

MPLS, un protocolo para un flujo de tráfico de red eficiente entre dos o más ubicaciones, su función es de manera similar a los conmutadores y routers, se sitúa entre las capas 2 y 3. MPLS generalmente brinda una excelente calidad de servicio, al tiempo que evita la pérdida de paquetes y preserva el tráfico más importante de la empresa. Esta confiabilidad es especialmente necesaria para mantener la calidad de los protocolos en tiempo real(Cisco 2021).

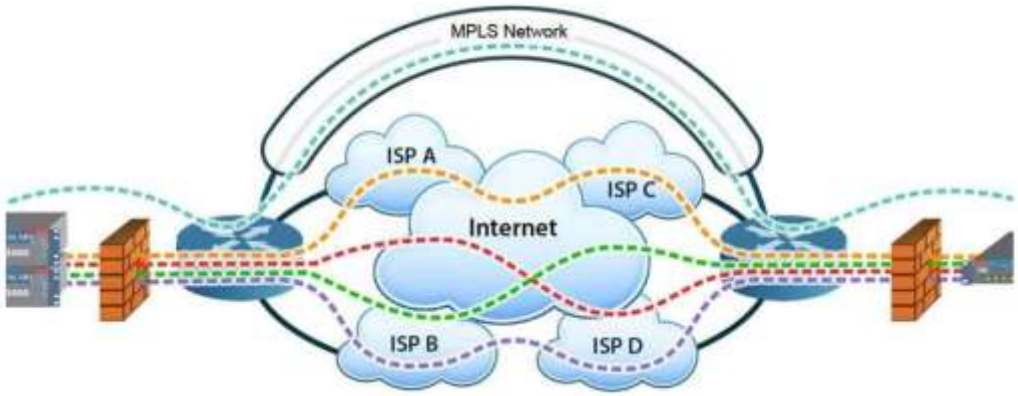
La confiabilidad de MPLS proviene de la etiqueta antes mencionada, que virtualmente aísla los paquetes. Los proveedores de MPLS asignan mayor prioridad al tráfico de red. Estas ventajas dan la impresión de previsibilidad del tráfico en la red. Las rutas de red están predeterminadas, por lo que los paquetes viajan solo a lo largo de las rutas a las que están dirigidas (Cisco 2021). En cuanto al tema de seguridad, una red MPLS no ofrece protección de datos incorporada, y si se implementa incorrectamente, abrirán a la red a vulnerabilidades.

SDWAN es una arquitectura WAN superpuesta distribuida basada en la nube que conecta las sucursales con los centros de datos y los entornos de múltiples nubes, lo que permite a los usuarios conectarse a cualquier aplicación en cualquier lugar a través de una sola textura, difuminar los límites geográficos y mejorar los beneficios clave, como la visibilidad, la escalabilidad, el rendimiento, y control (SD WAN CISCO 2021). La principal ventaja de SD-WAN es la seguridad.

Las compañías de hoy prefieren las arquitecturas de red que integran seguridad y políticas, por lo cual, SD-WAN cubre esas bases para unificar la conectividad segura. En la arquitectura SD-WAN, una empresa, obtiene el beneficio del cifrado de extremo a extremo en toda su red y conectividad a Internet. Todos los dispositivos y puntos finales están completamente autenticados, gracias a una funcionalidad escalable de intercambio de claves y seguridad definida por software (Cisco 2021).

Los beneficios de SD-WAN son difíciles de negar, desde el costo hasta la agilidad, flexibilidad y la facilidad de uso e implementación para una mayor seguridad. Sin embargo, las redes de base privada como MPLS siempre estarán en demanda, especialmente en empresas o instituciones que tienen requisitos de conectividad específicos, la figura 7 ejemplifica la comunicación de las dos tecnologías.

Figura 7. MPLS vs SD WAN



Fuente: SD-WAN *Experts* (2021)

1.5.3. Principales reportes de vulnerabilidades en clientes corporativos

Un ISP recepta a diario inconvenientes de sus clientes corporativos, no solo reportes de caídas del enlace, también eventos relacionados con la seguridad en redes, a continuación, se enlista los principales inconvenientes reportados:

- Ataques de accesos
- IP en listas negras
- *Phishing*
- DHCP *Starvation*
- Ataques de denegación de servicio (*DoS*)
- *Ransomware*
- Ataques de día cero

Ataques de accesos

Los ataques de acceso aprovechan las vulnerabilidades conocidas en los servicios de autenticación, servicios FTP y servicios web para acceder a cuentas web, bases de datos y otra información confidencial. Los ataques de acceso permiten que una

persona obtenga acceso no autorizado a información que no tiene permiso para ver. Los ataques de acceso se dividen en cuatro tipos. Uno de los tipos más comunes de ataques de acceso son los ataques a contraseñas. Los ataques a contraseñas se implementan a través de programas de rastreo de paquetes para obtener cuentas de usuario y contraseñas transmitidas en texto sin cifrar. Los ataques de contraseña son unos intentos repetidos de iniciar sesión en recursos compartidos (como servidores o routers) para identificar cuentas de usuario, contraseñas o ambas.

Listas negras

Una lista negra o *blacklists* son un compendio de direcciones IP identificadas por los proveedores de servicios de Internet como responsables del envío de correo no deseado. Si una dirección IP forma parte de la lista negra de un ISP, significa que el proveedor lo ha marcado al remitente como *spammer*.

No solo las direcciones IP se incluirán en la lista negra, los nombres de dominio (DNS) también se incluirán en la lista negra. Esto significa que incluso si se envía a nuestros correos electrónicos desde diferentes rangos de dirección IP, nuestros correos electrónicos aún son recibidos por estas listas negras, lo que evita que nuestros correos electrónicos lleguen a sus destinos.

Phishing

El *phishing* es una de las estafas más antiguas y conocidas en Internet. Se define, como un tipo de fraude de telecomunicaciones que utiliza trucos de ingeniería social para obtener datos personales de sus víctimas. Los atacantes informáticos están se

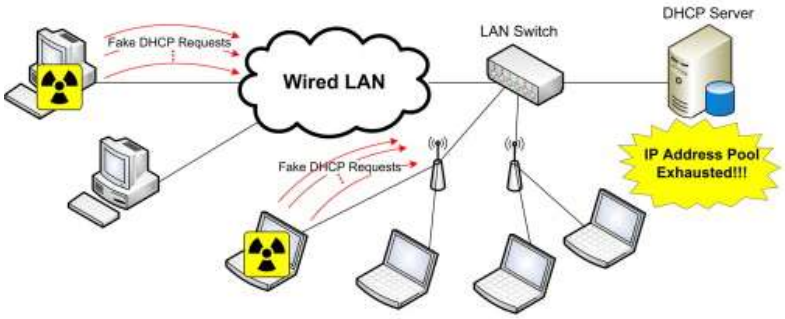
idean nuevas estratagemas para atraer a los empleados a sitios de phishing con el objetivo de obtener las credenciales de cuentas empresariales.

Ya sea que se realice por correo electrónico, redes sociales, SMS o cualquier otro sistema, todos los ataques de *phishing* siguen los mismos principios básicos. El atacante envía comunicaciones dirigidas para convencer a la víctima de hacer clic en un enlace, descargar un archivo adjunto o enviar la información solicitada o incluso realizar un pago, lo que resulta en la identificación o el robo de fondos y también una técnica eficaz para el espionaje industrial y el robo de datos (avast 2021).

DHCP *starvation*

Los clientes de una red utilizan el Protocolo de configuración dinámica de host (DHCP) para configurar su interfaz con la dirección IP y otros parámetros de configuración de red, como su puerta de enlace predeterminada y las direcciones de su servidor DNS. Los servidores DHCP siempre están amenazados por muchos tipos diferentes de ataques, el ataque de inundación DHCP es un ataque contra los servidores DHCP mediante el cual, un atacante genera solicitudes DHCP falsificadas con el objetivo de vaciar los servidores DHCP y agotar todas las direcciones IP disponibles que asigna el servidor DHCP. Bajo este ataque, se negará el servicio a los usuarios legítimos de la red, esto no solo afecta a las direcciones IPv4, se ve afectadas redes IPv6 que afecta los protocolos de configuración de direcciones como DHCPv6 y *StateLess Address Autoconfiguration* (SLAAC), la figura 7 muestra un servidor DHCP.

Figura 8. Servidor DHCP

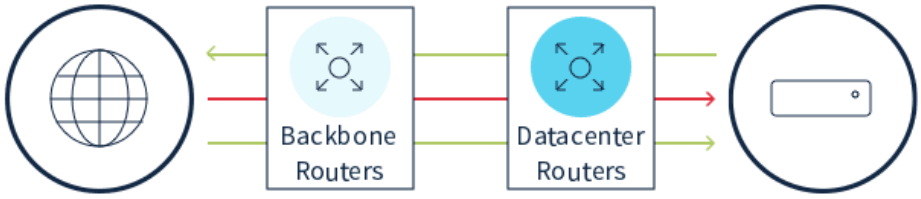


Fuente: Elaborada por el autor

Ataques de denegación de servicio (DOS)

A medida que la cantidad de datos de la red aumenta exponencialmente, los ataques distribuidos de denegación de servicio (DDoS) se han vuelto más frecuentes. Los ataques DDoS están diseñados para deshabilitar servidores, servicios o infraestructura. Los ataques DDoS tomarán muchas formas como por ejemplo la saturación del ancho de banda del servidor para hacerlo inaccesible o agotar los recursos del sistema de la máquina, evita así que responda al tráfico legítimo, en la figura 8 indica la conectividad de dispositivos hacia el Internet

Figura 9. Conexión red



Fuente: Tomada de https://www.ovh.com/world/es/anti-ddos/principio-anti-ddos.xml

Durante un ataque DDoS, se envían varias solicitudes simultáneamente desde diferentes puntos de la red. La intensidad de este tráfico transmitido afecta la estabilidad y, en ocasiones, la disponibilidad del servicio.

Ransomware

El *ransomware* es una clase de *malware*, resulta de combinar los términos “software” y “malicioso”. El término abarca todos los tipos de aplicaciones malignas que comprometerán la seguridad de un dispositivo, existe dos clases de ransomware, de bloqueo, que afecta las funciones básicas del equipo, y el *ransomware* de cifrado que su función principal es la de cifra archivos individuales (ransomware 2021).

La mitigación, consistente en neutralizar de forma efectiva el malware desplegado por el atacante. Para ello se ejecutará las siguientes recomendaciones, rediseñar la red, segmentar los distintos entornos, cambio de credenciales en todo el dominio, actualización y parcheo de los equipos.

Ataques de día cero

La concienciación en las empresas es fundamental para prevenir los ataques desconocidos, pero también la propia naturaleza del ataque de día cero hace que resulten más complejas las medidas de protección. Frente a las amenazas conocidas, en bastantes ocasiones, basta con las soluciones de ciberseguridad tradicionales que ya han probado con éxito soluciones específicas que las eliminan (Security 2019).
Para mitigar este tipo de ataques es recomendable que mantenga una política de control, con revisiones periódicas y desinstalaciones de aquello *software* que lleve tiempo sin utilizar, realizar un análisis de comportamiento, contar siempre con las últimas versiones actualizadas y parches en sistemas operativos y aplicaciones.

CAPÍTULO II. DISEÑO METODOLÓGICO

En el presente capítulo se aborda el tipo de investigación que se realizó, para lo cual, con las diversas técnicas y metodologías de investigación se pretende comprobar la hipótesis planteada y con ayuda de la norma ISO 27032 se abordó el tema de las mejores prácticas de seguridad para clientes corporativos.

El enfoque de la investigación es de tipo cualitativa, la misma es aplicada a un grupo de clientes ya establecidos que han sufrido mayor cantidad de inconvenientes con el servicio, con un diseño experimental con el que se pretende confirmar si el rendimiento de los clientes de datos fijos corporativos mejora, posterior a la aplicabilidad de las recomendaciones brindadas por parte de su ISP.

El uso de la de la norma ISO 27032, como referente de buenas prácticas tanto para el ISP, como para los clientes corporativos, al fin de preservar la integridad, confiabilidad y disponibilidad de la información que circula por el ciberespacio, para preservar los activos de una organización y la accesibilidad del servicio, analiza las principales amenazas que existen el espacio cibernético para llevar a vulnerar un activo o servicio.

2.1. Metodología de Investigación

El método utilizado en el presente proyecto es de tipo científica cualitativa con un diseño experimental, se realizó un análisis de los reportes de clientes corporativos a su ISP. Para lo cual, se ejecutó la revisión de cada cliente y posterior se procederá a confirmar la mejora del rendimiento del servicio para la comprobación de la hipótesis planteada, realizar un análisis de la latencia y disponibilidad del servicio de acuerdo con los parámetros del monitoreo y la tecnología de última milla empleada por cada cliente corporativo.

2.1.1. Investigación Cualitativa

Una investigación cualitativa se basa en comprender o explicar un comportamiento de un grupo, hecho o tema, para lo cual, utiliza un grupo de técnicas de investigación y así obtener una visión general del comportamiento o percepción del tema planteado. Además, de que permite también analizar los datos y adquirir un conocimiento profundo a través del análisis (questionpro 2021).

En el presente proyecto de investigación se realiza la recolección de datos, la misma está orientada a los reportes de los clientes corporativos sobre los inconvenientes que presentan, es decir, mediante la observación y descripción de los problemas que presenta un cliente corporativo se concibe formas para registrar los datos que se van a refinar conforme avanza la investigación.

2.1.2. Diseño experimental

El diseño experimental es la determinación de cómo se desarrolla nuestro experimento u observación. De este modo, trata de definir las variables que van a ser observadas, la relación entre elementos, cómo van a ser las variables medidas y cómo se procede a analizar los datos obtenidos.

Los diseños experimentales cuentan con distintos grupos de experimentación, entre los que existe un grupo de control con el fin de deducir los posibles efectos de variables externas en la muestra analizada. En este tipo de diseños, la medida de la variable dependiente se tomaría antes y después del tratamiento o solamente después.

El proyecto al ser una investigación de tipo experimental existe dos variables principales que son la independiente y dependiente. En la figura 10 se verifica las variables dependientes, el centro de la imagen representa la variable independiente.

2.1.3. Población

La población para el proyecto de investigación es un ISP con alrededor de 10 casos de reportes clientes corporativos, al ser una investigación de tipo cualitativa se pretende analizar los casos de reportes de inconvenientes con su servicio enfocados a temas de seguridad en la red.

Figura 10. Variables del proyecto de investigación

Fuente: elaboración propia.

2.1.4. Técnicas de investigación

La técnica de observación permite describir, explicar, comprender y descubrir patrones a través de los sentidos del observador, en este sentido, en el presente proyecto se utilizó esta técnica, un cliente corporativo realiza el reporte del inconveniente que presenta con su servicio a su ISP, la mesa de soporte técnico realiza la revisión del problema reportado. De todos los eventos reportados se seleccionó los enfocados a temas de ciberseguridad.

Reporte de Clientes Corporativos

Para realizar una investigación ordenada se utilizará varias herramientas y métodos que permiten organizar la información, por lo tanto, la ficha de observación estructurada se adapta a la necesidad del investigador, permite mantener un orden de la información recopilada, se dispone de un grupo de variables ya definidas. En este caso, las variables como referencia son los inconvenientes reportados por los clientes corporativos, como se indica en el cuadro 2.

Cuadro 2. Registro principales reportes

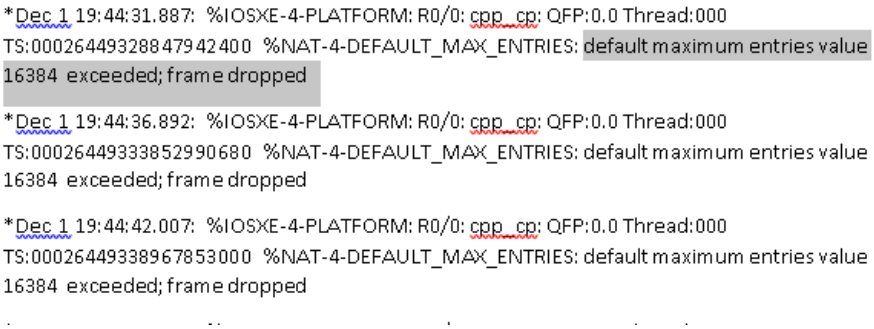
Reporte de Clientes Corporativos					
Ficha de observación: Reportes de clientes de datos fijos					
Principales reportes	**Siempre**	**Casi siempre**	**A veces**	**Nunca**	**Número de reportes**
Caída del servicio					
Degradación del servicio					
Intermitencias de conectividad					
Lentitud de los aplicativos					
Error en la conexión					
Bloqueo de envío de correos					
Intentos de ingreso de equipos					
Caída en lista negra					
Phishing					
Ataque de día cero					

Fuente: Adaptado a partir de milformatos

Logs equipos CPE

Otro elemento de gran importancia para la recolección de información son los registros de los equipos o conocidos también como logs, que sirve para identificar qué hace el equipo, incluye errores, problemas o avisos menores, y cuando ha sucedido eso, indica la fecha, hora y segundo en un sistema operativo o aplicación. En algunos casos se identifica el origen, el usuario y la dirección IP, el análisis de esta información sirve para identificar la causa del inconveniente, en la figura 11 indica un mensaje de logs en un equipo Cisco.

Figura 11. Logs equipo



Fuente: elaboración propia

Base de datos listas negras

Para el tema de seguridad en listas negras, si un cliente corporativo realiza él envió de correo basura *spam*, es perjudicial para su ISP, afectará no solo a una dirección IP en específico, sino que compromete todo un rango de IP, lo que ocasiona que no se realizará él envió de correos. Un servidor web donde se aloja información también es una herramienta útil al momento de realizar la revisión del tema de listas negras, para lo cual, en el proyecto se enfoca en el análisis de la información de la base de datos de lista negra de uceprotect. Por ejemplo, en la figura 12 está las IP que mayor impacto presentan de un ISP conocido del país.

Figura 12. IPs de alto impacto

AS27947 | **Telconet S.A, EC**

Timezone is CET.

IP	Impacts	Latest Impact +/- 1 Minute	Earliest Expiretime
181.39.25.68	1	06.12.2021 06:54	13.12.2021 08:00
181.39.74.170	1	09.12.2021 20:39	16.12.2021 22:00
186.3.23.3	5	06.12.2021 16:39	13.12.2021 18:00
186.101.235.139	1	09.12.2021 00:55	16.12.2021 02:00
200.93.207.5	1	08.12.2021 00:27	15.12.2021 02:00
200.110.77.235	1	06.12.2021 11:35	13.12.2021 13:00

Fuente: tomada de uceprotect

Uceprotect clasifica acorde al número de impactos, si está en nivel 1 significa que su servidor ha enviado *spam* sin darse cuenta. En la red interna se localizaría la fuente

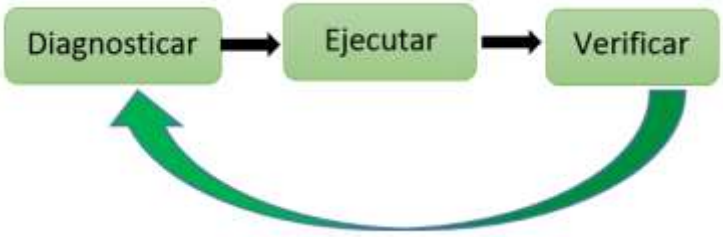
del spam, y aplicar los métodos y técnicas de seguridad y su IP se eliminará de la lista en siete días, si está en nivel 2 indica que su rango de direcciones de red está comprometido, depende de su máscara de red y el número de IP, para la eliminación de esta lista negra se la realizaría a través de su ISP y finalmente si está en nivel 3 es recomendable es presentar una queja al ASN por el cual, el spam continúa, no hay nada que un administrador del servidor final efectué para sacar de esta lista negra.

2.2. Metodología de desarrollo

El ciclo de mejora continua es una metodología que tiene como objetivo clave eliminar las actividades que no agregan valor en la cadena productiva. Esta herramienta tiene un potencial enorme para ayudar así a mejorar la productividad de las empresas, por lo general, el modelo de mejora continua es orientar las actividades hacia las prácticas de gestión, la más utilizada es el planificar, ejecutar, verificar y actuar (PDCA) por lo cual, está compuesto por 4 etapas.

El modelo de mejora continua se basa en que, una vez acabada la etapa final, volvería a la primera y repetir el ciclo. Por lo tanto, las actividades son revaluadas periódicamente para incorporar nuevas mejoras. En el proyecto se toma como referencia, este modelo, para la estructura de la metodología de investigación, en la figura 13 se verifica las etapas a ser utilizadas.

Figura 13. Modelo de mejora continúa



Fuente: elaboración propia

2.2.1. Diagnóstico

La etapa de diagnóstico está centrada en el análisis de los datos recogidos durante la observación realizada, y su interpretación científica, con lo cual, sirve de guía para las siguientes etapas, la figura 14 describe las actividades a ejecutar en esta etapa.

Figura 14. Actividades etapa diagnóstico

Fuente: elaboración propia

Reporte de clientes corporativos

Un cliente corporativo de datos fijos, es un segmento de negocio tipo Business to Business (B2B), es decir, de negocio a negocio y se relaciona principalmente con el comercio mayorista, con ayuda del internet, ha abierto enormes oportunidades al desarrollo de modelos de negocio B2B debido, entre otras, a las siguientes razones:

- Rapidez y seguridad en las comunicaciones.
- Facilidad de integración de procesos y de comunicación interna como lo es intranet.
- Posibilidad de ampliar el ámbito en el que encontrar *partners* con los que colaborar.
- Abaratamiento de los procesos de preventa, con reuniones virtuales, solicitud de propuestas, subasta de contratos.

Por lo general existe confusión entre un servicio de internet residencial y corporativo, la principal diferencia radica en que un servicio corporativo utiliza el internet en una

gran cantidad de equipos de manera simultánea, utiliza transferencia de datos mediante una red, uso de navegadores, correo electrónico, *streaming* de vídeo, conferencias y acceso de escritorio remoto, lo cual, exige una conexión hacia Internet estable, por lo que es un servicio sin compartición de su ancho de banda y alta tasas de velocidad de carga y descarga.

Por otro lado, el uso doméstico tiene en promedio el uso de uno o máximo dos computadoras de escritorio o portátil por cada vivienda. Sumado a los dispositivos móviles como celulares, *tablets* y consolas de videojuegos. El uso de Internet en el hogar presenta compartición de su consumo de ancho de banda con otros clientes residenciales y no requiere una gran cantidad de ancho de banda en carga y descarga comparado con el uso de Internet corporativo.

Un ISP recepta a diario reportes de inconvenientes del servicio de los clientes de datos corporativos, mediante varios canales de comunicación como llamada telefónica, correo electrónico, WhatsApp y otros medios digitales. Un cliente corporativo presentará inconvenientes como caídas o intermitencias de su servicio, por lo que la notificación a su ISP para el respectivo análisis es fundamental para determinar la causa o motivo del inconveniente. En esta fase se pretende conocer el mayor inconveniente que presentan los clientes de datos fijos corporativos y enlistar los mayores ataques que presenta una red corporativa.

La investigación se basa en la recolección de reportes de cliente corporativos a su ISP de los principales inconvenientes de seguridad en la red, para lo cual, con la ayuda de la herramienta de observación, se toma los principales inconvenientes y analizar cada uno de ellos para recomendar las mejores prácticas de seguridad.

Análisis del inconveniente reportado

Encontrar y resolver un problema, es el proceso que se conoce como *troubleshooting*, esto es muy difícil y toma mucho tiempo si se intentan soluciones al azar. Un método de resolución de fallas, efectivo, requiere la combinación de un adecuado conocimiento del sistema, de un esquema de descarte lógico de posibles causas y de un acercamiento estructurado ordenado al problema. Dado que el conocimiento y la experiencia varían en cada persona, todos se beneficiaran con un buen esquema de *troubleshooting* (Sierra Ciudad 2021).

Las fallas en redes, y en cualquier otro sistema, se caracterizan por ciertos síntomas. Estos son generales, por ejemplo, que ciertos clientes no acceden a servidores específicos. También ser más específicos, por ejemplo, una falla en la configuración de un enlace Ethernet, por lo cual, se ejecutará un análisis a detalle del inconveniente reportado, para clasificar a los clientes acorde al problema que presenta, en el cuadro 3 se identifica los mayores inconvenientes que reporta un cliente corporativo a su ISP y con la ayuda de la técnica de observación se logra obtener un número estimado de reportes del cliente corporativos.

Cuadro 3. Encuesta de reportes ISP

Reportes ISP					
Ficha de observación: Reportes de clientes de datos fijos					
Principales reportes	**Siempre**	**Casi siempre**	**A veces**	**Nunca**	**Número de reporte estimado por día**
Caída del servicio	X				20
Degradación del servicio	X				10
Intermitencias de conectividad	X				5
Lentitud de los aplicativos	X				2
Error en la conexión			X		5
Bloqueo de envío de correos		X			6
Intentos de ingreso de equipos			X		2
Caída en lista negra		X			3
Phishing		X			4
Ataque de día cero				X	0

Fuente: elaboración propia

2.2.2. Ejecutar

En esta etapa se llevará a cabo un plan definido y de forma organizada para proceder a ejecutar las mejores técnicas y métodos para solventar un inconveniente, una vez se obtenga los reportes de los clientes corporativos, procede la verificación de configuraciones en el equipo de administración del ISP y notificar las mejores prácticas de seguridad a su cliente, en la figura 15 se identifica los *ítems* que es analizado en esta etapa.

Figura 15. Actividades etapa ejecución

Fuente: elaboración propia

Verificación y análisis

Un equipo CPE en todas las redes es el punto que permite la interconexión entre nuestros dispositivos de red interna hacia el ciberespacio, constituye una puerta de entrada y salida de la información, que no está exenta de sufrir ciberataques, se aplican varios métodos de seguridad, depende del equipo, pero el mismo tiene un limitante, el equipo CPE tiene la funcionalidad de establecer rutas los paquetes hacia su destino y proveer conectividad mediante varios protocolos entre las distintas sedes de clientes corporativas, no es equipo con características amplias para la configuración de todos los métodos y técnicas de seguridad.

El ISP al tener la administración del equipo CPE, que es donde circula toda la información de red, al realizar el *troubleshooting* de un reporte de un cliente corporativo, con ayuda del equipo se verificará conectividad y logs que permiten identificar el inconveniente y depende de lo encontrado aplicar métodos de seguridad con el fin de mitigar la afectación en su servicio o infraestructura de red.

Notificación de mejores prácticas de seguridad

Existen varias normas que están enfocadas en reglas y políticas de seguridad en las redes corporativas e ISP, toda la familia de la ISO 27000 y la ISO 31000, muestran los activos críticos, una evaluación de riesgos tanto del ISP como del usuario corporativo final, proporcionar directrices para la implementación de controles que permitan asegurar de forma adecuada la información.

La ISO 27032 como se ha descrito anteriormente, trabaja y se enfoca en la seguridad de la Información, seguridad de las Redes, seguridad en Internet y la protección de las Infraestructuras críticas para la Información, esta norma establece las mejores prácticas de ciberseguridad que le permitan estar preparado a los clientes corporativos para responder de manera efectiva ante un incidente en el cual, se vea comprometido sus activos y dar continuidad a sus operaciones.

La norma ISO 27032 describe las técnicas que las organizaciones considerarían como usar un “Certificado de Alta Seguridad” para proporcionar una seguridad adicional a los usuarios online, tomar en cuenta que los proveedores de servicios que usan el correo electrónico como su medio primario para comunicarse, por lo que nuca solicitaran información personal; nombres de usuario; contraseñas; y jamás incluirán links relacionados con la seguridad para que el lector les haga *click*, estas son algunas de las recomendaciones que brinda esta norma y está enfocado tanto al usuario final como su ISP.

Una guía de buenas prácticas de seguridad, implementará una empresa, para proteger su información de forma adecuada, el cuadro 4 es una recopilación de las principales recomendaciones de seguridad que una organización implementa para proteger de forma adecuada sus activos, la misma es una adaptación de recomendaciones empleadas en una empresa pública, para la cual, se ha realizado una adaptación para clientes corporativos y la misma está basada en las recomendaciones de seguridad emitidas por la norma ISO 27032.

Cuadro 4. Propuestas de mejores prácticas de seguridad

Práctica de Seguridad	Recomendaciones
Cliente corporativo	• Conocer y aplicar la política de ciberseguridad en la organización
Fortaleza contraseñas	• La contraseña se modificará cada 90 días. • La contraseña estaría compuesta por 8 dígitos como mínimo. • Componerla de letras mayúsculas y minúsculas, algún número y algún carácter especial. • La contraseña no constaría de fechas, nombres o información personal • La contraseña no es apuntada en ningún sitio ni enviarla por correo electrónico. • La contraseña tiene que ser diferente de la que protege cuentas de carácter personal. • No compartir la contraseña con nadie ni solicitar la de otro compañero. • No guardar la contraseña en el navegador de Internet.
Uso de certificados digitales	• Los certificados digitales se protegerán con contraseña y aplicarle a esta las mismas reglas del bloque anterior
Uso del correo electrónico	• No enviar desde cuentas de correo personal información personal de salud, ni proporcionar la dirección para recibir este tipo de datos. • No utilizar su cuenta de correo electrónico corporativa para fines personales, y extremar las medidas de seguridad si va a acceder a ella desde un domicilio particular. • No responder a correos electrónicos que le soliciten la remisión de datos de salud. • Extremar la precaución, al abrir adjuntos de un correo electrónico para no introducir virus en el centro. • Encriptar o codificar los correos electrónicos que contengan datos personales.
Acceso a Internet	• Evitar navegar por: redes sociales, páginas de descargas, páginas de almacenamiento de archivos, mensajería instantánea y juegos online por ser una entrada potencial de amenazas. • Precaución en la descarga de archivos de Internet
Uso de dispositivos y medios extraíbles	• Consultar con el responsable de la información la conveniencia o no de sacar información personal de la organización en un medio extraíble • Encriptar o codificar la información personal de la organización que salga del centro en medios extraíbles o dispositivos portátiles. • Precaución en el uso de medios extraíbles (USB, CD) para evitar la entrada de virus.

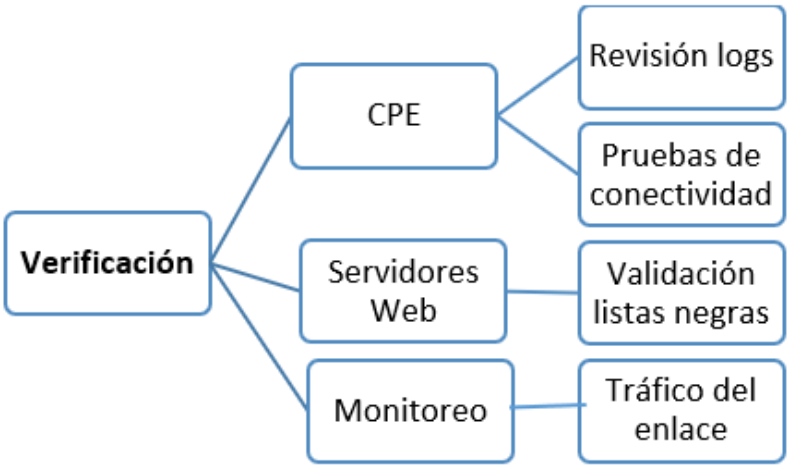
Uso de equipos	• Borrado seguro de medios extraíbles con información personal de la organización al desecharse para evitar que se recupere. • Cerrar la sesión, bloquearla o apagar la pantalla del ordenador cuando vaya a ausentarse del mismo durante 5 min o más • Evitar que los datos desplegados en pantallas sean vistos por personas no autorizadas • No colocar información sensible en unidades del ordenador compartidas con trabajadores que no tengan autorización a acceder a dichos datos • Acceder únicamente a la información indispensable para desempeñar el trabajo. Si se accede a información que no deba ser vista, se informaría al departamento de informática del centro. • Borrar la memoria de las fotocopiadoras de alta capacidad del centro tras fotocopiar información que contenga datos personales de la organización. • Retirar los documentos con datos sensibles de la bandeja de impresión de las impresoras y faxes para que no ser consultados por personal no autorizado.
Instalación de software	• No instalar software no relacionado con las funciones del puesto de trabajo por ser una posible entrada de amenazas. • Cuidar que el software a instalar esté libre de virus.
Incidencias de seguridad	• Conocer el protocolo de actuación frente a la detección de amenazas informáticas • Informar de cualquier anomalía en el funcionamiento del ordenador a quien corresponda según el procedimiento que se definiría por la organización para la notificación de incidencias
Listas negras	• Configuración de SPF, DKIM y DMARC para su dominio. • Agregar listas rbl para análisis de envíos. • Configuración de las cuentas de correo para SMTP con autenticación únicamente. • Separación de envíos de correo electrónico de facturación electrónica a través de otro dominio en otro servidor. • Corrección de vulnerabilidades en PC o equipo de red interna que están afectadas por *malware*. • Configurar umbral de envíos diarios a través de SMTP de cliente. • Configuración de rdns.

Autor: elaboración propia

2.2.3. Verificación

Esta etapa permite revisar si los resultados coinciden con lo esperado, al receptar un reporte de un cliente corporativo como se describe en las anteriores etapas, primero se realizará un diagnóstico y posterior ejecutar las principales acciones y actividades para solventar el inconveniente, en esta etapa se realizó pruebas de conectividad, análisis de logs, verificación en la base de listas negras y monitoreo del tráfico, como se describe en la figura 16.

Figura 16. Actividades etapa verificación



Autor: elaboración propia

Las herramientas de monitoreo de tráfico ayudan a los administradores de red la visibilidad que necesitan para garantizar que el servicio funcione sin problemas, es de gran ayuda para ejecutar un análisis entre su ancho de banda y el consumo de tráfico, al realizar un análisis su consumo y el número de equipos conectados, en tal sentido se abordara dos variables para el monitoreo como lo es la latencia y la disponibilidad del servicio.

La norma ISO 27032 indica que el monitoreo de la red es usado normalmente por las organizaciones para asegurar la confiabilidad y calidad de sus servicios de red. Al mismo tiempo, esta capacidad se aprovecha para buscar condiciones de tráfico de red sospechosas y detectar actividades maliciosas que emerjan de la red. En general, las organizaciones trabajarán de la manera siguiente:

- Entender el tráfico de la red: qué es normal y qué es anormal.
- Usar una herramienta de gestión de red para identificar peaks en el tráfico, tráfico/ puertos “no usuales” y asegurarse de que haya herramientas disponibles para precisar y responder a la causa.

- Probar la capacidad de respuesta antes de ser necesaria frente a un evento real. Refinar las técnicas, procesos y herramientas de respuesta con base en el resultado de simulacros constantes.
- Entender los constituyentes de manera individual. Si alguien quien normalmente es un usuario inactivo repentinamente empieza a llegar al límite del 100% del ancho de banda disponible, es necesario aislar al usuario que no se comporte adecuadamente hasta que se encuentre la razón. El aislamiento de red prevé la propagación de malwares, aunque algunas implementaciones requerirán el consentimiento del usuario o actualizaciones de los Términos de Servicio.
- Considerar el seguimiento de la actividad de puntos inteligentes en una red, tales como un DNS y filtros de mensajería, que también servirá a los dispositivos *flag* que han sido comprometidos con malwares, pero que, por una variedad de razones, no se ven afectados por los servicios antivirus o de IDS.

En el capítulo 3 se describe a detalle la aplicabilidad del resultado de la investigación, con el análisis de logs, monitoreo de tráfico del servicio y validación del estado de servicio con pruebas de conectividad y revisión en las bases de datos.

CAPÍTULO III. ANÁLISIS Y VALIDACIÓN DE RESULTADOS

En este capítulo de análisis y validación del resultado, se realizó el análisis del reporte del cliente corporativo hacia su ISP con el fin de realizar una revisión del inconveniente y posterior realizar un monitoreo de su servicio para verificar el rendimiento posterior a las recomendaciones de seguridad brindadas.

3.1. Reportes de problemas de clientes corporativos

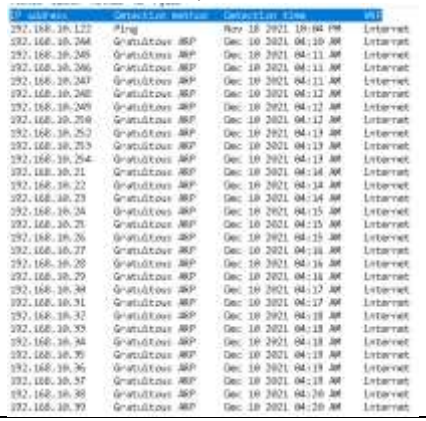
Un cliente corporativo de un ISP solicita la revisión de su servicio, por lo cual, el personal del ISP ejecutara el respectivo *troubleshooting* con las diversas herramientas que dispone, con ayuda de la técnica de observación se logró identificar la mayor causa de inconvenientes enfocados al tema de seguridad que reporta un cliente corporativo al área de soporte de su ISP, como se describe en la tabla 14 del capítulo II.

Con esta información, se procede al análisis de cada caso, enfocado a las recomendaciones de seguridad basado en la norma ISO 27032 para la protección de los activos de manera segura, a continuación, se enlista los principales reportes de clientes corporativos y recomendaciones de seguridad brindadas.

Como primer paso se realizó un análisis del reporte del cliente corporativo hacia su ISP, con la ayuda de las diversas herramientas se procede con el monitoreo y verificación del rendimiento del servicio posterior a la notificación del cliente de las recomendaciones de seguridad, para lo cual, se dispone de tablas donde se validará el tráfico del enlace, análisis de logs, pruebas de conectividad y las conclusiones de cada uno de ellos.

3.2. Casos de cliente corporativos de un ISP

Cuadro 5. Caso 001.- Sin servicio

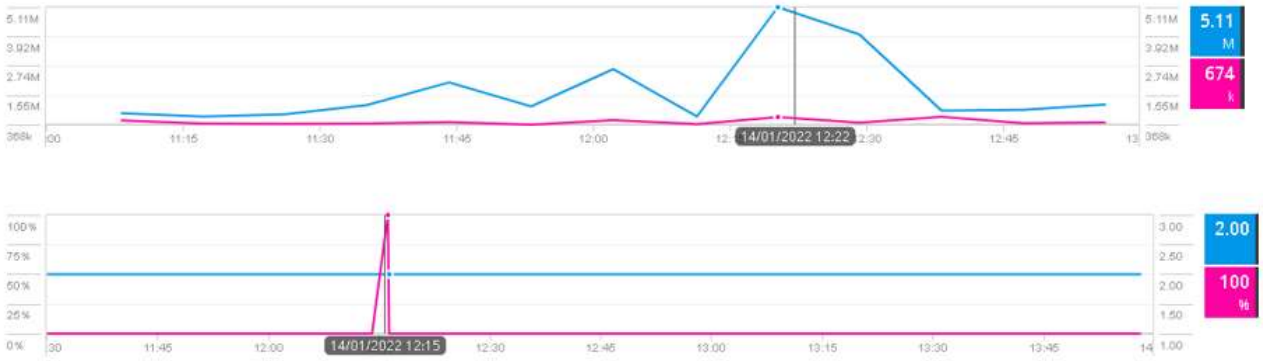
Reporte del cliente	Un cliente corporativo indica que no existe conexión de dispositivos al servicio de internet y algunos logran conectarse, pero no tiene salida hacia Internet, por lo que solicita realizar una revisión urgente del caso, el inconveniente sucede cuando se conectan a la red inalámbrica por el SSID de la agencia.
Análisis del reporte	Al ejecutar el análisis se verifica que en el equipo CPE se tiene configurado dos servicios separados mediante vrf para un servicio de datos e internet, en el CPE se realiza el análisis de logs, donde la Vlan10 asignada al servicio de internet presenta caídas de estado DOWN a UP, se valida conflicto en la asignación de IP mediante DHCP, se llenó casi en totalidad la tabla de DHCP y el cliente ya presentaba intermitencias, en la figura están los logs que genero él equipó CPE, se comprueba que la VLAN asignada a su salida hacia internet presenta intermitencias., en la siguiente la figura indica la tabla DHCP, en la misma se observa que se va llenar con varias IPs.  *Dec 15 19:18:10.470: %LINK-3-UPDOWN: Interface GigabitEthernet0, changed state to down *Dec 15 19:18:11.630: %DTP-5-TRUNKPORTON: Port Gi0 has become dotlq trunk *Dec 15 19:18:12.138: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up *Dec 15 19:18:12.142: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up *Dec 15 19:18:12.146: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan15, changed state to up *Dec 15 19:18:13.122: %LINK-3-UPDOWN: Interface GigabitEthernet0, changed state to up *Dec 15 19:18:14.122: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0, changed state to up *Dec 15 19:19:01.162: %DTP-5-NONTRUNKPORTON: Port Gi0 has become non-trunk *Dec 15 19:19:01.662: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0, changed state to down *Dec 15 19:19:01.662: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to down *Dec 15 19:19:01.662: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to down *Dec 15 19:19:01.662: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan15, changed state to down *Dec 15 19:19:02.662: %LINK-3-UPDOWN: Interface GigabitEthernet0, changed state to down *Dec 15 19:19:03.734: %DTP-5-TRUNKPORTON: Port Gi0 has become dotlq trunk *Dec 15 19:19:04.246: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up *Dec 15 19:19:04.250: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up *Dec 15 19:19:04.250: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan15, changed state to up *Dec 15 19:19:05.226: %LINK-3-UPDOWN: Interface GigabitEthernet0, changed state to up *Dec 15 19:19:06.226: %LINEPROTO-5-UPDOWN: Line protocol on Interface GigabitEthernet0, changed state to up
Troubleshooting y pruebas del servicio	Al ingresar al equipo se verifica que existe un conflicto para la asignación de IP, como se indica en la figura, con el comando *show ip dhcp conflict,* esta instrucción muestra como resultado todas las direcciones IP en las que el *router* ha descubierto conflictos y cómo se descubrió el conflicto, como se verifica en la siguiente figura. 

	Al realizar la limpieza de tabla arp, refrescamiento DHCP y configuración de un *lease* de 10 minutos en el servidor DHCP, se verifica servicio operativo con el cliente final y se confirma que existe equipos conectados al servicio de internet mediante la vlan de internet, se aprende las direcciones MAC de los equipos y en el nombre de la tarjeta de red asociada a la MAC como se muestra en la figura. 
Recomendaciones del ISP a su cliente	✓ Revisar las IP que reportan gran cantidad de eventos. ✓ Ejecutar un full *scan* de las unidades físicas a través del antivirus, tanto a dispositivos móviles como equipos laptop y computador de escritorio. ✓ Validar con los usuarios, si compartieron las credenciales de la conexión mediante el servicio Wifi, de ser así, realizar el cambio de contraseña del SSID. ✓ En la controladora inalámbrica aplicar los métodos de seguridad y dividir en grupos de SSID ✓ La contraseña modificarla cada 90 días y la misma tiene que estar compuesta por 8 dígitos como mínimo. Componerla de letras mayúsculas y minúsculas, algún número y algún carácter especial.

Autor: Elaboración propia

Cuadro 6.Caso 002.- Intermitencia del servicio

Reporte del cliente	Un cliente corporativo realiza el reporte de intermitencias del servicio a su ISP en una de las sucursales del país.
Análisis del reporte	Al realizar el *trobleshooting* se confirma que existe una alta latencia. Al ejecutar el análisis de revisión de tráfico se valida que existe unos picos de saturación en su consumo como se muestra en la figura 20, llega a ocupar el total de su ancho de banda, el cliente tiene un protocolo HSRP para los tipos de fallas, sin embargo, si se conmuta su servicio a su otro proveedor se verifica que aún persistiría el inconveniente.
***Troubleshooting* y pruebas del servicio**	Se identifica varias direcciones de IP que emite un mayor consumo inusual, como sé válida en la figuras, se solicita al cliente realice una revisión del equipo y verificación, para los cuales se emite las respectivas recomendaciones, a nivel de los *logs* no se logra verificar registros.

<table>
<tr>
<td></td>
<td>


<table>
<tr><th>Source</th><th>Destination</th><th>Packets</th><th>Bytes</th></tr>
<tr><td>132.118.0.11</td><td>132.147.10.174</td><td>39263089</td><td>2249178411</td></tr>
<tr><td>132.118.0.12</td><td>132.147.10.174</td><td>2015869</td><td>1127289013</td></tr>
<tr><td>132.118.0.126</td><td>132.147.19.106</td><td>647497</td><td>872547807</td></tr>
<tr><td>132.118.0.15</td><td>132.147.10.174</td><td>714141</td><td>768110955</td></tr>
<tr><td>132.118.0.13</td><td>132.147.10.174</td><td>1797566</td><td>608939570</td></tr>
<tr><td>132.118.0.13</td><td>13.107.6.171</td><td>786340</td><td>325309598</td></tr>
<tr><td>132.118.0.15</td><td>10.16.3.30</td><td>487017</td><td>295543021</td></tr>
<tr><td>132.118.0.11</td><td>10.16.3.30</td><td>485674</td><td>219185422</td></tr>
<tr><td>132.118.0.10</td><td>132.147.10.90</td><td>1851536</td><td>184622380</td></tr>
<tr><td>132.118.0.10</td><td>192.168.29.27</td><td>1582617</td><td>168371812</td></tr>
<tr><td>132.118.0.12</td><td>132.147.10.90</td><td>2112431</td><td>152655152</td></tr>
<tr><td>132.118.0.19</td><td>10.16.3.30</td><td>301887</td><td>150132654</td></tr>
<tr><td>132.118.0.12</td><td>192.168.29.23</td><td>1750754</td><td>133010878</td></tr>
<tr><td>132.118.0.12</td><td>192.168.29.27</td><td>1519017</td><td>130156509</td></tr>
<tr><td>132.118.0.10</td><td>192.168.29.23</td><td>1321302</td><td>129229537</td></tr>
<tr><td>132.118.0.15</td><td>192.168.29.23</td><td>1338748</td><td>116279705</td></tr>
<tr><td>132.118.0.17</td><td>132.147.10.90</td><td>1301247</td><td>109978776</td></tr>
<tr><td>132.118.0.12</td><td>10.16.3.30</td><td>209814</td><td>106990358</td></tr>
<tr><td>132.118.0.13</td><td>192.168.29.27</td><td>1282336</td><td>103919568</td></tr>
</table>
</td>
</tr>
<tr>
<td>Recomendaciones del ISP a su cliente</td>
<td>
✓ Revisar las direcciones IP internas y externas que generan este tipo de tráfico.
✓ Revisar el comportamiento de las direcciones IP en relación con las diferentes aplicaciones, con la finalidad de identificar aquellas que generan mayor cantidad de tráfico.
✓ Se recomienda realizar una validación de las direcciones IP externas desconocidas y realizar el bloqueo de las mismas de ser necesario.
✓ Revisar que los equipos internos reportados cuenten con todos los parches de seguridad actualizados.
✓ Revisar que los equipos cuenten con el agente antivirus con las firmas actualizadas y con la última versión de antivirus.
</td>
</tr>
</table>

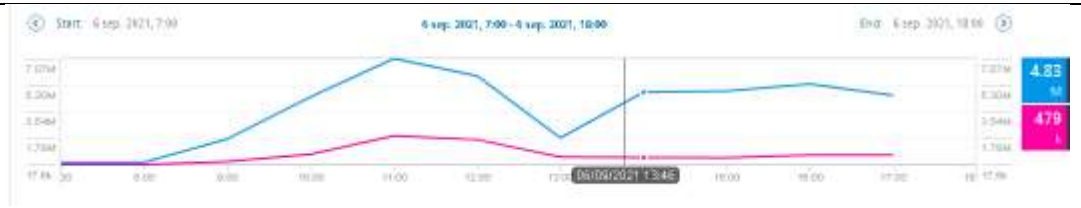
Autor: Elaboración propia

Cuadro 7. Caso 003.- Bloqueo de Salida de correo

Reporte del cliente	Un cliente corporativo de datos fijos reporta a su ISP que tiene problemas con el servicio de internet y no tiene problemas con él envío de correos.

Análisis del reporte	Por parte del ISP realiza el trobleshooting se verifica conectividad correcta con una prueba de ping hacia los DNS de Google.
	`Type escape sequence to abort.`
	`Sending 200, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:`
	`Packet sent with a source address of 200.7.217.217`
	`!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!`
	`!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!`
	`!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!`
	`Success rate is 100 percent (200/200), round-trip min/avg/max = 56/57/60 ms`
	En el tráfico del cliente, se verifica que en la mañana consumo un ancho de banca de 10 Mbps, posterior a la hora de reporte se confirma que el tráfico disminuye a 1.55 Mbps.
	 

Troubleshooting y pruebas del servicio	Al realizar el análisis de las IP en para verificar que cayó en listas negras, se comprueba que está enlistada en Spamhaus ZEN, el ISP ejecuta las acciones necesarias para sacar la IP de la lista negra y se mantiene en monitoreo para verificar posterior a 5 días realizar una nueva revisión. Checking **200.7.217.217** against **83** known blacklists... Listed **1** times with **1** timeouts Blacklist: Spamhaus ZEN — Reason: 200.7.217.217 was listed — LISTED — Detail Pasado los 5 días se verifica que la IP salió de listas negras y se analiza el tráfico posterior a esta fecha, en la misma se verifica acorde al histórico que el tráfico está normalizado, se valida el tráfico del enlace y en la figura muestra la validación de que la IP se des enlisto de la lista negra.

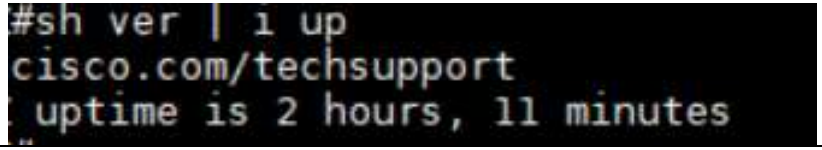
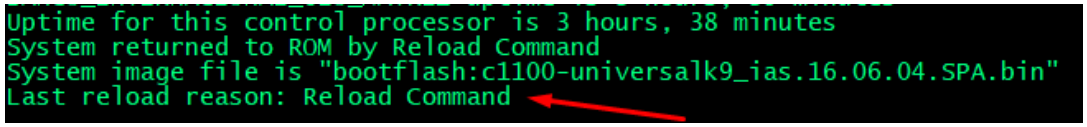
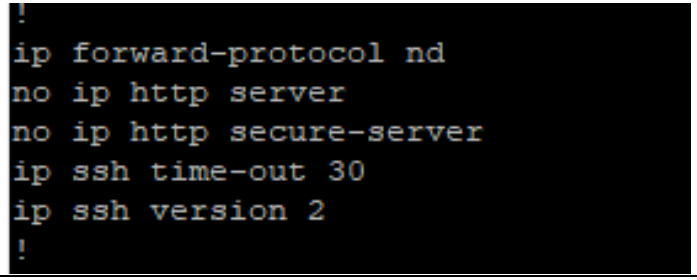
<table>
<tr>
<td></td>
<td>



El cliente del IPS indica que es muy recurrente que caída en listas negras y afecte su servicio de internet al utilizar su IP pública como servidor de correo, por qué cometa que al tener un FW Fortinet, se realice las respectivas configuraciones de seguridad y se emitan las recomendaciones de seguridad. Por parte del área de seguridad, SOC realiza la habilitación, se añade un perfil de EmailFilter para monitoreo en la política de salida de correos y evitar una nueva caída las listas negras.


</td>
</tr>
<tr>
<td>Recomendaciones del ISP a su cliente</td>
<td>
✓ Configuración de SPF, DKIM y DMARC para su dominio
✓ Agregar listas RBL para análisis de envíos
✓ Configuración de las cuentas de correo para SMTP con autenticación únicamente.
✓ Separación de envíos de correo electrónico de facturación electrónica a través de otro dominio en otro servidor.
✓ Corrección de vulnerabilidades en PC o equipo de red interna que están afectadas por malware.
✓ Configurar umbral de envíos diarios a través de SMTP de cliente
✓ Configuración de RDNS.
</td>
</tr>
</table>

Autor: Elaboración propia

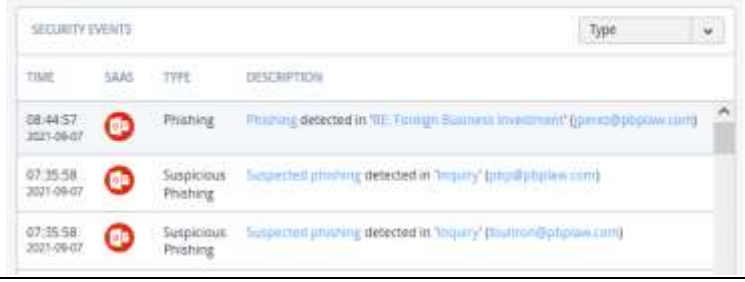
Cuadro 8. Caso 004.- Ingreso no autorizado de equipos

Reporte del cliente	Una entidad financiera del ISP reporta un reinicio de su equipo, al ser un giro de negocio que mantiene sus equipos en un Datacenter conectado a UPS y no tener algún mantenimiento programado le causa preocupación que se presente un reinicio sobre su servicio de internet corporativo de su agencia Matriz.
Análisis del reporte	El cliente comparte el *uptime*, del equipo donde se verifica que existe un reinicio hace 2 horas aproximadamente, en la figura se verifica el log facilitado por el cliente. 
Troubleshooting y pruebas del servicio	Al ejecutar el *troubleshooting se* verifica en los logs que el reinicio del equipo fue realizado remotamente con el comando *Reload*, por lo que se descartan problemas de energía u operatividad del equipo. El *booteo* del equipo finaliza normalmente y el BGP levanta sin novedad como se evidencia en el tiempo de establecimiento de sesión, dado que los logs se borran al apagarse el equipo no se registra el usuario que realizó el reinicio, como sé válida en los *logs* del equipo.  Como medida adicional se escala al equipo de soporte para realizar una revisión adicional a nivel de FW por sesiones de ingreso realizadas en el día del evento y no se observan usuarios de soporte ingresados el día del evento. Se realiza el cambio de contraseña para evitar accesos no autorizados al equipo. Adicional se procede a configurar el acceso al equipo con doble *checking* y se valida que el acceso Web está bloqueado. 
Recomendaciones del ISP a su cliente	✓ Revisar el listado de usuarios que están autorizados para ingresar a los equipos. Caso contrario eliminarlos o generar reglas de accesos en el equipo.

	✓ Revisar si los equipos relacionados con las conexiones directas sobre el router, cuentan con las firmas de antivirus y parches de seguridad actualizados, además, desinstalar aplicaciones no autorizadas. ✓ Validar con los usuarios, si compartieron sus credenciales, de ser así, cerrar la sesión en todos los equipos, eliminar credenciales almacenadas en navegadores y el administrador de credenciales de Windows y cambiar la contraseña. ✓ Eliminar los usuarios o cuentas de los equipos si los mismos ya no están en la institución. ✓ Ejecutar un full *scan* de las unidades físicas a través del antivirus.

Autor: Elaboración propia

Cuadro 9. Caso 005.- Phishing

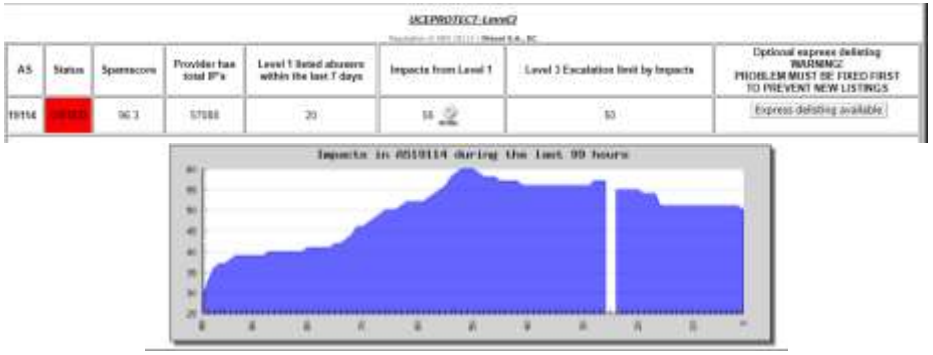
Reporte del cliente	Un cliente corporativo tiene contratado un servicio de seguridad con un equipo checkpoint reporta que en el Dashboard me muestra 100% de remediaciones realizadas con respecto a Phishing, sin embargo, en los eventos de seguridad aparecen incidentes relacionados con Phishing,por lo que solicita al ISP ejecutar la revisión en conjunto con su área de SOC. 
Análisis del reporte	Posterior a las revisiones en conjunto, se verifica que al tener la política en “Detect and Remediate”, las acciones de detección o contención son casi automáticas por la herramienta y no requieren una aprobación o veredicto por parte del administrador para realizar alguna gestión.
Troubleshooting y pruebas del servicio	Al ejecutar el *troubleshooting* se colocarían en detención y remediación, la política estaba solo aplicada para la detección.  El “Security Events” mostrará todo el flujo de correos categorizados como maliciosos, como se valida en la figura. Se recomienda colocar la política en Prevent con un nivel más restrictivo y automatizado, a la par se requiere que se realicen las recomendaciones de seguridad a nivel de su red interna y colaboradores de la empresa. 

	En monitoreo se verifica que existe bajo consumo del tráfico, se realiza pruebas de conectividad WAN, el consumo de ancho de banda del cliente es constante acorde a los históricos. 
Recomendaciones del ISP a su cliente	✓ No enviar desde cuentas de correo personal información personal, ni proporcionar la dirección para recibir este tipo de datos. ✓ No utilizar su cuenta de correo electrónico corporativa para fines personales, y extremar las medidas de seguridad si va a acceder a ella desde un domicilio particular. ✓ No responder a correos electrónicos que le soliciten la remisión de datos de salud. ✓ Extremar la precaución, al abrir adjuntos de un correo electrónico para no introducir virus en el centro. ✓ Encriptar o codificar los correos electrónicos que contengan datos personales.

Autor: Elaboración propia

Cuadro 10. Caso 006.- Lista negra UCEPROTECT

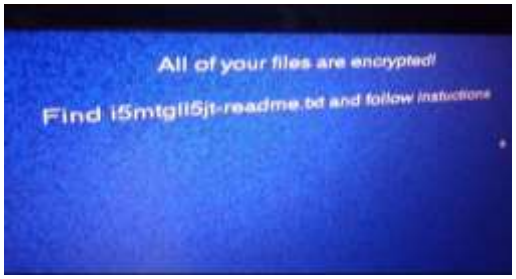
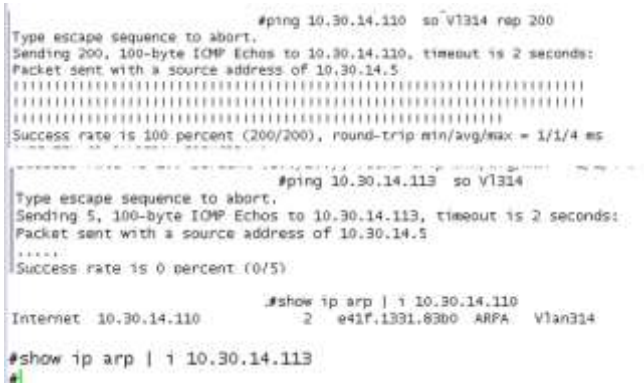
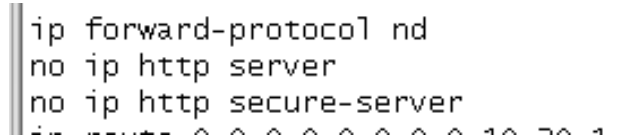
Reporte del cliente	El ISP recepta por parte de aproximadamente 10 clientes corporativos que tienen inconvenientes en él envió de correos,
Análisis del reporte	Con ayuda del repositorio web de uceprotect, se ejecuta el *trobleshooting* del inconveniente reportado, se hace un análisis del ASN del ISP da como resultado varias IP enlistadas en nivel 3, en la que incluye las direcciones IP de los clientes reportados

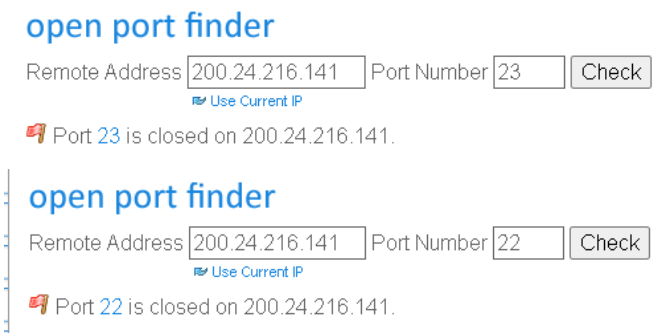
Troubleshooting y pruebas del servicio	Al ejecutar el análisis de se verifica que el ASN está comprometido varios rangos de direcciones IP, se valida en la página web la gráfica del incremento de enlistamiento de IPs.
	 
	Autor: Tomada de uceprotect
	Por parte del ISP inmediatamente toma acciones para solventar el inconveniente, los clientes que no dispongan un FW se realiza el bloqueo de puertos en el equipo CPE y creación de ACL, se realiza el bloqueo de IP(s) a nivel de protocolo SMTP (puertos:465, 587, 25, 2525). A la par se da recomendaciones a los clientes de datos fijos para que implementen en sus servidores de correo electrónico.
	`Extended IP access list BLACKLIST`
	`10 deny tcp host 200.24.221.182 any eq smtp (3 matches)`
	`20 deny tcp host 200.24.221.182 any eq 465`
	`30 deny tcp host 200.24.221.182 any eq 587`
	`40 deny tcp host 200.24.221.182 any eq 2525`
	`50 deny tcp any host 200.24.221.182 eq smtp`
	`60 deny tcp any host 200.24.221.182 eq 465`
	`70 deny tcp any host 200.24.221.182 eq 587`
	`80 deny tcp any host 200.24.221.182 eq 2525`
	`90 permit ip any any (44723 matches)`

Recomendaciones del ISP a su cliente	✓ Configuración de SPF, DKIM y DMARC para su dominio ✓ Agregar listas RBL para análisis de envíos ✓ Configuración de las cuentas de correo para SMTP con autenticación únicamente. ✓ Separación de envíos de correo electrónico de facturación electrónica a través de otro dominio en otro servidor. ✓ Corrección de vulnerabilidades en PC o equipo de red interna que están afectadas por *malware*. ✓ Configurar umbral de envíos diarios a través de SMTP de cliente ✓ Configuración de RDNS.

Autor: Elaboración propia

Cuadro 11. Caso 007.- Ransomware

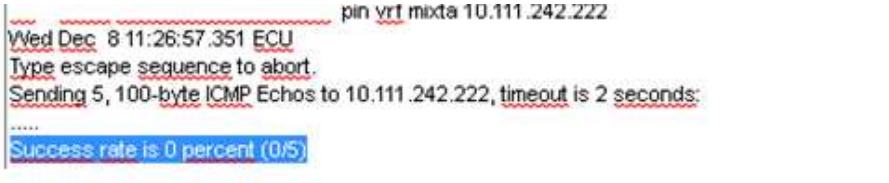
Reporte del cliente	Un cliente corporativo indica que tiene problemas de accesos para un servidor y solicita nivel FW validar el acceso de las IP que se conectaron a los servidores con IP 10.30.14.110 y 10.30.14.113
Análisis del reporte	El cliente remite el mensaje que le muestra al conectarse al servidor, con lo cual, se verifica que fue un ataque de tipo *ransomware*, inmediatamente se realiza la revisión con el área de seguridad SOC en conjunto con el área de soporte N1 del ISP. 
Troubleshooting y pruebas del servicio	Al ejecutar pruebas sobre el equipo CPE se verifica que la red está configurada y se tiene conectividad hacia el servidor con IP 110, pero el de IP terminada en 113, ya no se tiene conectividad y tampoco aprende MAC en la tabla ARP, a continuación, se muestra el *troubleshooting* realizado.  En el equipo se verifica que la IP pública está cerrada el puerto de conexión mediante ssh y *telnet*, en el equipo CPE se verifica que se tiene deshabilitado el acceso mediante http y https. 

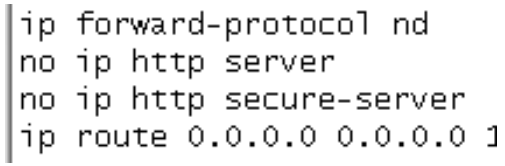
<table>
<tr>
<td></td>
<td>


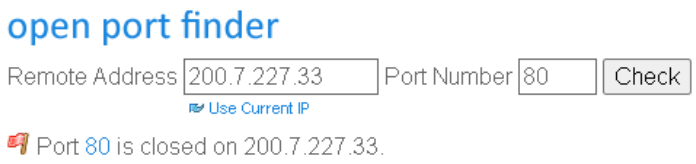
Por parte del área de seguridad emite el informe de accesos a nivel del FW, sin embargo, no se identifica que usuario o desde que IP ingresaron, a nivel del log en el CPE no se visualiza ingresos por el equipo, como sé válida en los logs, por lo que el cliente inmediatamente desconecta el servidor de la red.
<pre>
*Jan 17 21:27:30.089: %HSRP-5-STATECHANGE: Vlan3034 Grp 50 state Standby -> Active
*Jan 17 21:27:31.354: %HSRP-5-STATECHANGE: Vlan20 Grp 0 state Speak -> Active
*Jan 17 21:27:32.141: %HSRP-5-STATECHANGE: Vlan3034 Grp 40 state Standby -> Active
</pre>
</td>
</tr>
<tr>
<td>Recomendaciones del ISP a su cliente</td>
<td>
✓ Revisar el listado de usuarios que están autorizados para ingresar a los equipos. Caso contrario eliminarlos o generar reglas de accesos en el equipo.
✓ Revisar si los equipos relacionados con las conexiones directas sobre el router, cuentan con las firmas de antivirus y parches de seguridad actualizados, además, desinstalar aplicaciones no autorizadas.
✓ Validar con los usuarios, si compartieron sus credenciales, de ser así, cerrar la sesión en todos los equipos, eliminar credenciales almacenadas en navegadores y el administrador de credenciales de Windows y cambiar la contraseña.
✓ Eliminar los usuarios o cuentas de los equipos si los mismos ya no están en la institución.
✓ Ejecutar un full scan de las unidades físicas a través del antivirus.
✓ Realizar unidades de respaldo de sus servidores
</td>
</tr>
</table>

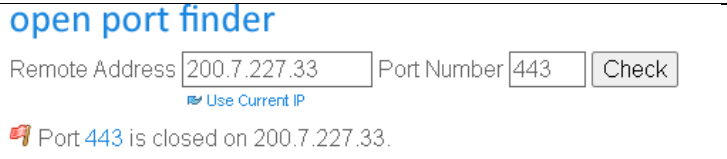
Autor: Elaboración propia

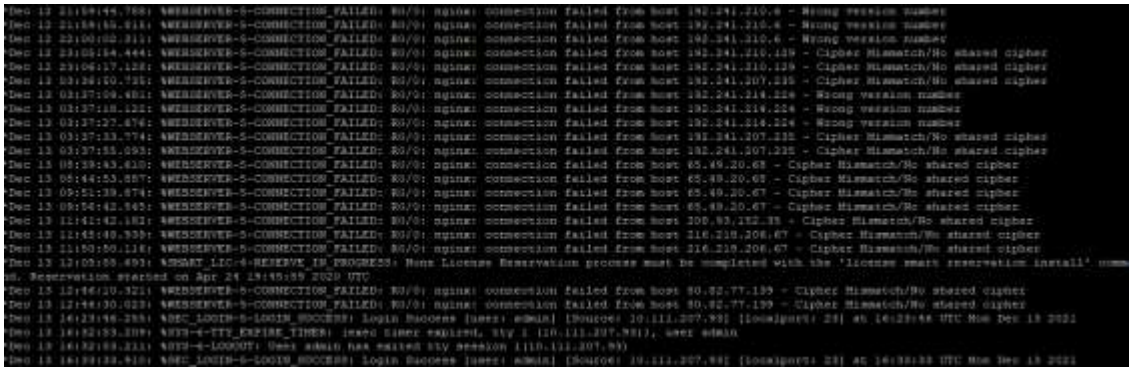
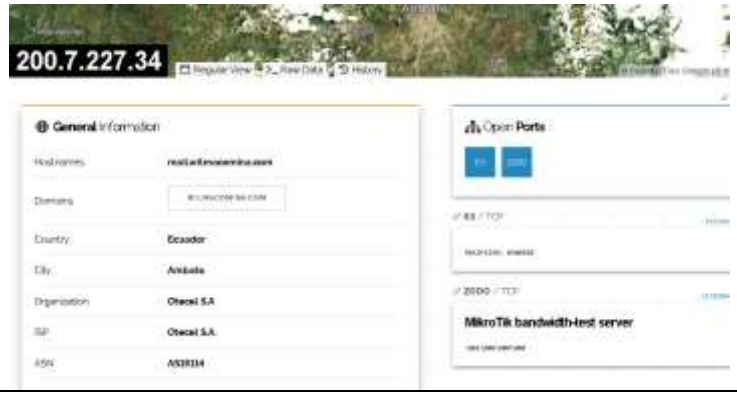
Cuadro 12. Caso 008.- Denegación de servicio

<table>
<tr><td>Reporte del cliente</td><td>Un cliente corporativo indica que no tiene servicio de internet, solicita la revisión inmediata a su ISP para restablecer el servicio.</td></tr>
<tr><td>Análisis del reporte</td><td>Se procede con la revisión y análisis del inconveniente reportado, se valida que no existe conectividad a nivel WAN, no se tiene gestión del equipo y a nivel del tráfico se verifica disminución de este.</td></tr>
<tr><td>Troubleshooting y pruebas del servicio</td><td>Pruebas a nivel WAN sin conectividad, como se muestra la prueba de ping hacia la IP del cliente y el tráfico del enlace, se verifica con personal en sitio que se borró la configuración del equipo, para lo cual, se procede a configurar el equipo para restablecer el servicio.


En los logs refleja intentos de ingreso al equipo mediante http y https, se procede con la configuración en el equipo para evitar este tipo de accesos, para lo cual, se procede con el bloquea del acceso web.



</td></tr>
</table>

<table>
<tr>
<td></td>
<td>



El cliente tiene un equipo de red interna, se verifica el puerto 53 TCP abierto, lo cual, es una puerta para un ataque de DoS, como se indica en las pruebas realizadas en shodan


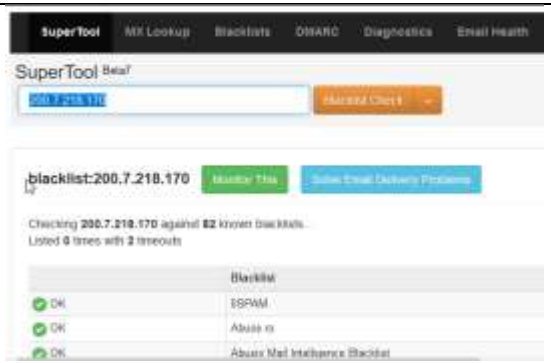
</td>
</tr>
<tr>
<td>Recomendaciones del ISP a su cliente</td>
<td>
✓ Revisar el listado de usuarios que están autorizados para ingresar a los equipos. Caso contrario eliminarlos o generar reglas de accesos en el equipo.
✓ Revisar si los equipos relacionados con las conexiones directas sobre el router, cuentan con las firmas de antivirus y parches de seguridad actualizados, además, desinstalar aplicaciones no autorizadas.
</td>
</tr>
</table>

	✓ Validar con los usuarios, si compartieron sus credenciales, de ser así, cerrar la sesión en todos los equipos, eliminar credenciales almacenadas en navegadores y el administrador de credenciales de Windows y cambiar la contraseña. ✓ Eliminar los usuarios o cuentas de los equipos si los mismos ya no están en la institución. ✓ Ejecutar un full *scan* de los puertos abiertos en el equipo de red interna con el fin de validar la posibilidad de cerrar los mismos.

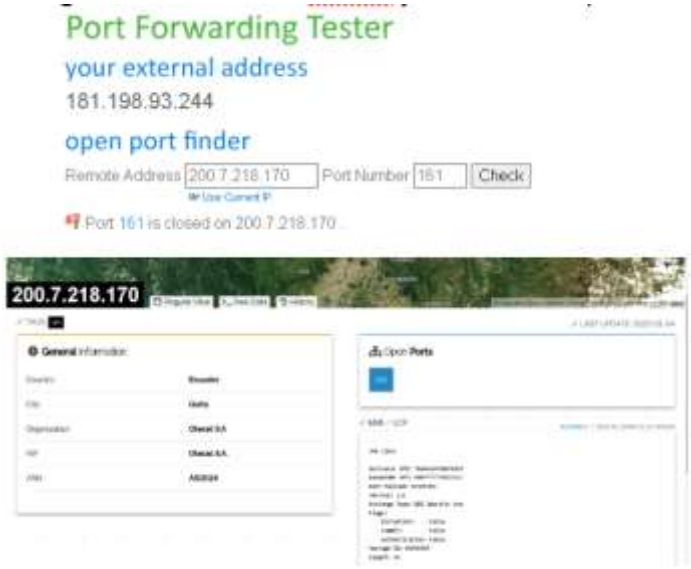
Autor: Elaboración propia

Cuadro 13. Caso 009.- Reporte vulnerabilidad

Reporte del cliente	Un cliente corporativo, entidad financiera, indica que se requiere la revisión de la siguiente vulnerabilidad reportada para la empresa que se encarga de la seguridad de la institución, adjunta la captura de pantalla de la vulnerabilidad que se encontró
Análisis del reporte	Al analizar la imagen enviada, se verifica que es de un equipo de su red interna con IP 200.7.218.170. 
Troubleshooting y pruebas del servicio	Al ejecutar la revisión desde el equipo CPE se valida conectividad hacia el equipo, sin embargo, se verifica que aprende la MAC del equipo correspondiente a la IP 200.7.218.170 la misma corresponde a un equipo Meraki.  La IP reportada no se verifica que está enlistada en alguna lista negra, como se aprecia en la figura de la base de datos de mxtoolbox.



En *shodan* se verifica que tiene abierto solo el puerto 500 UDP, este puerto es utilizado por el protocolo de VPN IPsec, concretamente se usa por *Internet Security Association Key Management Protocol* ISAKMP para el establecimiento de la conexión con IPsec. Al ser un equipo de red interna no se realiza el bloqueo de puerto por lo que la acción correctiva vendría del lado del cliente, a nivel del CPE se tiene todo correctamente configurado en tema de seguridad, adicional se verifica que la IP tiene cerrara el puerto 161 como se muestra en la figura.



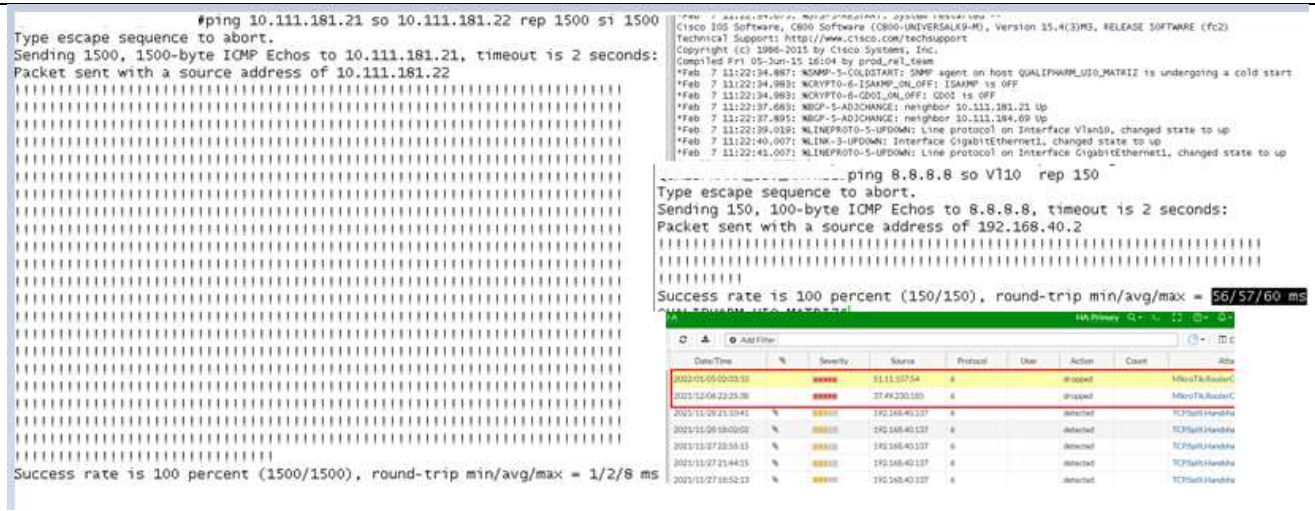
Recomendaciones del ISP a su cliente	✓ Realizar el cierre del puerto abierto en el equipo de red interna si no se utiliza para algún servicio. ✓ Configurar correctamente el firewall para permitir acceso al equipo a personal autorizado y aplicar políticas de seguridad en el firewall. ✓ Realizar *hardening* a los servicios y dispositivo. ✓ Actualización de los dispositivos de red interna del sistema operativo y firmware del equipo reportado.

Autor: Elaboración propia

Cuadro 14. Caso 010.- Ataque Phishing

<table>
<tr><td>Reporte del cliente</td><td>Un cliente corporativo indica que recepto un correo con un link para acceder y solicita verificar el dominio de correo del remitente, e indican que si se corre algún riesgo adicional por motivo de que una de las personas que recibió este correo abrió el HTML en su celular.</td></tr>
<tr><td>Análisis del reporte</td><td>Al analizar el dominio del correo gsplab.co.jp y se observa que la IP asociada es 210.131.0.40, misma que pertenece al ISP Fujitsu localizado en Japón. El dominio se encuentra registrado como una gran fuente de phishing.
 

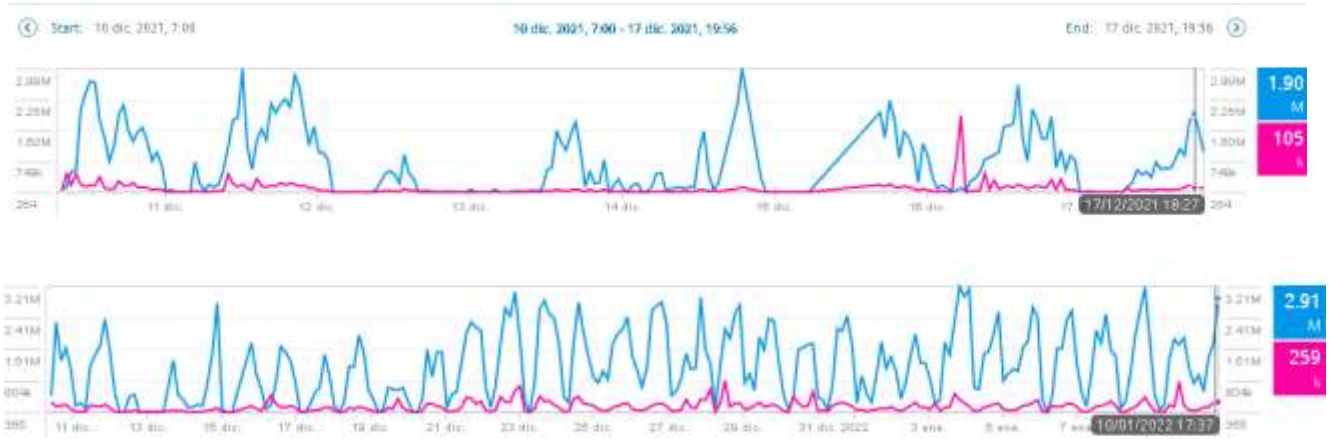

</td></tr>
<tr><td>Troubleshooting y pruebas del servicio</td><td>En el equipo al ingresar se valida que se tiene salida hacia Internet, a nivel del equipo CPE no se verifica logs de caídas del enlace y se valida que se tiene todos los elementos de seguridad configurados en el mismo. En conjunto con el área de SOC se realiza la verificación a nivel del equipo FW Fortinet donde no se evidencia problemas, referente a algún tipo de “possible attack” con la IP en mención. Se evidencia el equipo que el último intento de ataque fue el 5 de enero; sin embargo, no hubo ningún peligro y el mismo fue dropeado.</td></tr>
</table>

<table>
<tr><td></td><td> 
</td></tr>
<tr><td>Recomendaciones del ISP a su cliente</td><td>✓ No enviar desde cuentas de correo personal información personal, ni proporcionar la dirección para recibir este tipo de datos.
✓ No utilizar su cuenta de correo electrónico corporativa para fines personales, y extremar las medidas de seguridad si va a acceder a ella desde un domicilio particular.
✓ No responder a correos electrónicos que le soliciten la remisión de datos de salud.
✓ Extremar la precaución, al abrir adjuntos de un correo electrónico para no introducir virus en el centro.
✓ Encriptar o codificar los correos electrónicos que contengan datos personales.</td></tr>
</table>

Autor: Elaboración propia

3.3. Validación de la propuesta de solución

Cuadro 15. Monitoreo Caso 001.- Sin servicio

Tráfico del enlace	A nivel del tráfico del enlace se verifica que el mismo ha permanecido estable, no se verifica caídas en el tráfico, se ha tomado un rango de una semana y un mes posterior al evento suscitado, se valida el tráfico de una semana y el de un mes. 
Análisis logs	En el equipo CPE se verifica logs, nuevamente se verifica flapeos de la VLAN asigna al internet. *Jan 15 15:43:35.699: %DTP-5-TRUNKPORTON: Port Gi0 has become dot1q trunk *Jan 15 15:43:36.207: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan1, changed state to up *Jan 15 15:43:36.211: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan10, changed state to up *Jan 15 15:43:36.215: %LINEPROTO-5-UPDOWN: Line protocol on Interface Vlan15, changed state to up *Jan 15 15:43:37.191: %LINK-3-UPDOWN: Interface GigabitEthernet0, changed state to up El 22 del mes de diciembre se verifica nuevamente conflicto de asignación de dhcp, sin embargo, la tabla no está llena como cuando reporto el cliente y presentaba inconveniente con el servicio. A nivel del equipo se verifica que existen equipos conectados al servicio de Internet mediante el Wifi, se enlista las MAC de los equipos.

<table>
<tr>
<td></td>
<td>
/# show ip dhcp conflict
IP address Detection method Detection time VRF
192.168.10.164 Gratuitous ARP Dec 22 2021 08:44 AM internet
192.168.10.165 Gratuitous ARP Dec 22 2021 08:44 AM internet
192.168.10.166 Gratuitous ARP Dec 22 2021 08:44 AM internet
192.168.10.167 Gratuitous ARP Dec 22 2021 08:45 AM internet
192.168.10.168 Gratuitous ARP Dec 22 2021 08:45 AM internet
192.168.10.169 Gratuitous ARP Dec 22 2021 08:45 AM internet
192.168.10.170 Gratuitous ARP Dec 22 2021 08:46 AM internet
192.168.10.171 Gratuitous ARP Dec 22 2021 08:47 AM internet
192.168.10.174 Gratuitous ARP Dec 22 2021 09:11 AM internet
192.168.10.179 Gratuitous ARP Dec 22 2021 09:26 AM internet
192.168.10.180 Gratuitous ARP Dec 22 2021 09:36 AM internet
192.168.10.184 Gratuitous ARP Dec 22 2021 09:59 AM internet
192.168.10.189 Gratuitous ARP Dec 22 2021 09:59 AM internet
192.168.10.190 Gratuitous ARP Dec 22 2021 09:59 AM internet
192.168.10.191 Gratuitous ARP Dec 22 2021 10:04 AM internet
192.168.10.195 Gratuitous ARP Dec 22 2021 10:12 AM internet
192.168.10.199 Gratuitous ARP Dec 22 2021 10:34 AM internet
192.168.10.201 Gratuitous ARP Dec 22 2021 10:34 AM internet
192.168.10.202 Gratuitous ARP Dec 22 2021 10:34 AM internet
192.168.10.203 Gratuitous ARP Dec 22 2021 10:34 AM internet
192.168.10.150 Gratuitous ARP Dec 23 2021 04:09 AM internet
/#

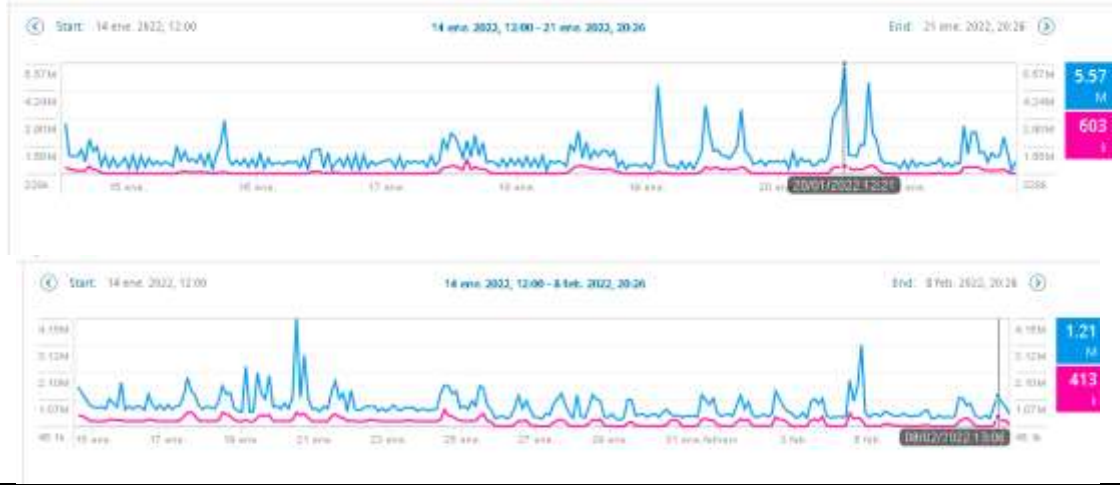

#show mac-address-table | i GigabitEthernet0
8caa.ce62.4f48 Dynamic 10 GigabitEthernet0
1209.f3da.153e Dynamic 10 GigabitEthernet0
187c.0b2e.0e20 Dynamic 15 GigabitEthernet0
fefc.e098.3b13 Dynamic 10 GigabitEthernet0
a0cc.2b91.4c6c Dynamic 10 GigabitEthernet0
187c.0b2e.0e20 Dynamic 1 GigabitEthernet0
1496.e5bb.93ad Dynamic 10 GigabitEthernet0
947b.e72f.b98a Dynamic 10 GigabitEthernet0
246f.8c3a.064f Dynamic 10 GigabitEthernet0
e207.7221.387a Dynamic 10 GigabitEthernet0
a041.4749.da81 Dynamic 10 GigabitEthernet0
c0d2.f381.d6bc Dynamic 10 GigabitEthernet0
4e53.2393.f890 Dynamic 10 GigabitEthernet0
4a2a.1934.7a14 Dynamic 10 GigabitEthernet0
00b5.d070.2041 Dynamic 10 GigabitEthernet0
8a34.e886.5728 Dynamic 10 GigabitEthernet0
0008.2284.8ffb Dynamic 10 GigabitEthernet0
0056.cdab.8807 Dynamic 10 GigabitEthernet0
9c5a.81f5.60fe Dynamic 10 GigabitEthernet0
2aad.123b.e974 Dynamic 10 GigabitEthernet0
a6e3.3d8c.9e3e Dynamic 10 GigabitEthernet0
460c.66df.ce76 Dynamic 10 GigabitEthernet0
705f.a35e.14a4 Dynamic 10 GigabitEthernet0
8291.6402.a47b Dynamic 10 GigabitEthernet0
4a07.5566.e40a Dynamic 10 GigabitEthernet0
a240.dfc0.799a Dynamic 10 GigabitEthernet0
8608.f575.ac51 Dynamic 10 GigabitEthernet0
</td>
</tr>
<tr>
<td>Conectividad pruebas</td>
<td>
Se realizan pruebas de conectividad hacia los DNS de Google, se verifica ping de manera exitosa, los tiempos está acorde a la última milla empleada y a nivel WAN de igual manera se verifica conectividad de manera exitosa.

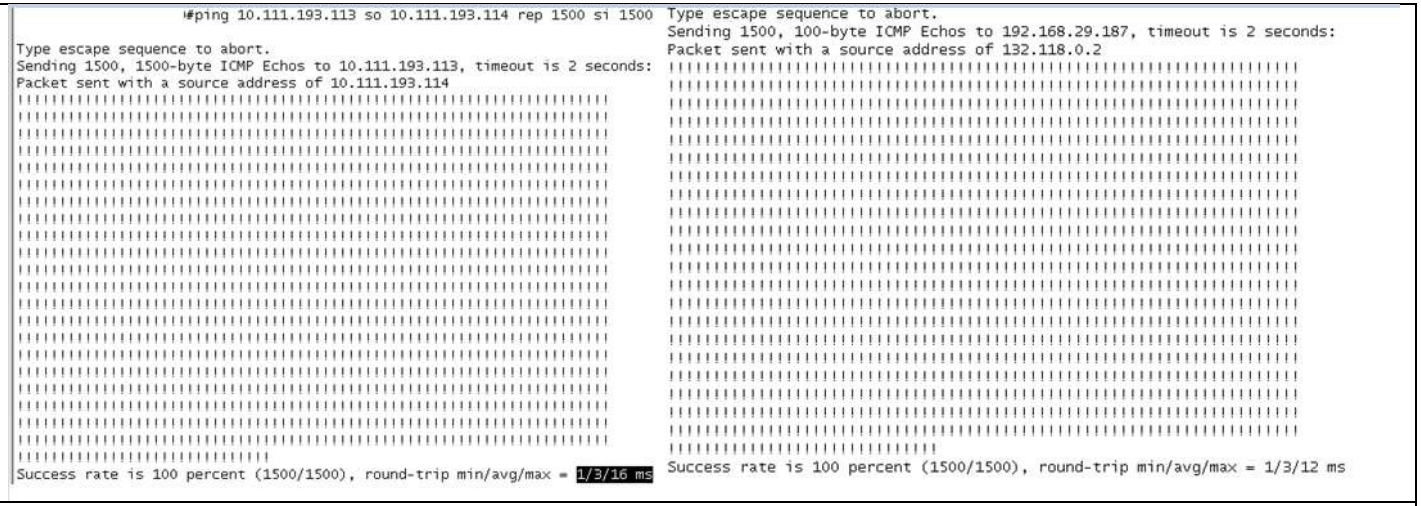
#ping vrf internet 10.112.187.137 so 10.112.187.138 rep 500
Type escape sequence to abort.
Sending 500, 100-byte ICMP Echos to 10.112.187.137, timeout is 2 seconds:
Packet sent with a source address of 10.112.187.138
!!
!!
!!
!!
!!
!!
!!
!!!!!!!!!!
Success rate is 100 percent (500/500), round-trip min/avg/max = 1/2/8 ms
#pin vrf internet 8.8.8.8 so Vl10
Type escape sequence to abort.
Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 192.168.10.1
!!!!!
Success rate is 100 percent (5/5), round-trip min/avg/max = 60/60/60 ms
</td>
</tr>
<tr>
<td>Conclusión</td>
<td>Con las acciones realizadas y recomendaciones brindadas al cliente se verifica que pese al borrado de conflicto y configuración del lease del DHCP se presenta aun logs en el equipo con los flapeos de la vlan de internet; sin embargo, el</td>
</tr>
</table>

	cliente indica que el servicio se ha mantenido estable por lo que se aplicaría este tipo de configuración para solventar el inconveniente, no en su totalidad, pero parcialmente se logra superar el inconveniente con el servicio, tomar en cuenta que se requiere el apoyo del cliente corporativo para mitigar nuevamente una afectación con las recomendaciones de seguridad brindadas.

Autor: Elaboración propia

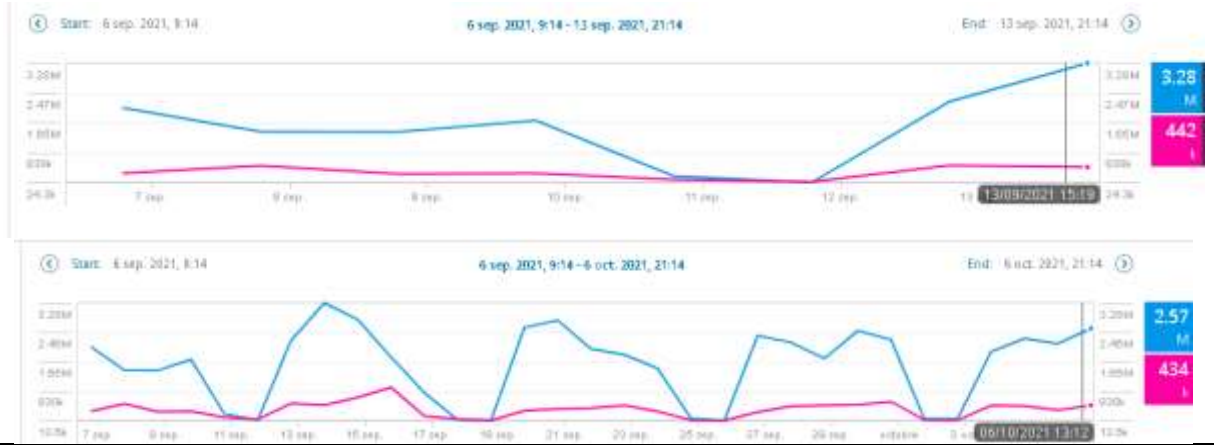
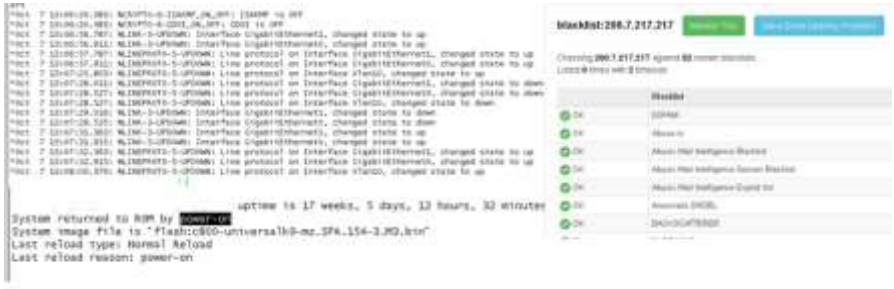
Cuadro 16. Monitoreo Caso 002.- Intermitencia del servicio

Tráfico del enlace	Al realizar el análisis de tráfico se verifica que existen una disminución de tráfico sin saturación del enlace por 5 días posterior a las acciones realizadas y recomendaciones de seguridad brindadas, como se valida en el tráfico de una semana y un mes respectivamente. 
Análisis de logs	El equipo tiene deshabilitado los logs, causan alto procesamiento al equipo, por lo cual, el cliente solicita mantener desactivado. 
Pruebas Conectividad	En conectividad el enlace no presenta perdidas de paquetes a nivel WAN y LAN, se ha replicado las pruebas con MTU de 1500 sin existir perdidas de paquetes, los tiempos están acorde a la tecnología de última milla empleada, las pruebas a nivel WAN y LAN son exitosas.

	
Conclusión	Con las recomendaciones de seguridad brindadas, se verifica que el enlace no presenta saturación, el cliente realizo la revisión y aplico las recomendaciones de seguridad en el equipo de red interna que causo que el enlace sature, con lo cual, se llega a comprobar que las acciones realizadas en este caso logro solventar el inconveniente.

Autor: Elaboración propia

Cuadro 17. Monitoreo Caso 003.- Bloqueo de Salida de correo

Tráfico del enlace	Al realizar el análisis del tráfico se verifica que el mismo se ha mantenido estable y no ha presentado disminución. Se valida el tráfico de una semana y un mes. 
Análisis de logs	Al verificar los logs en el equipo solo se presenta caídas de los puertos, al verificar se valida un reinicio del equipo por temas eléctricos en la agencia del cliente, se realiza la verificación de la IP en lista negra, al momento ya no ha vuelto a enlistarse, se realiza las validaciones y pruebas sobre el servicio. 

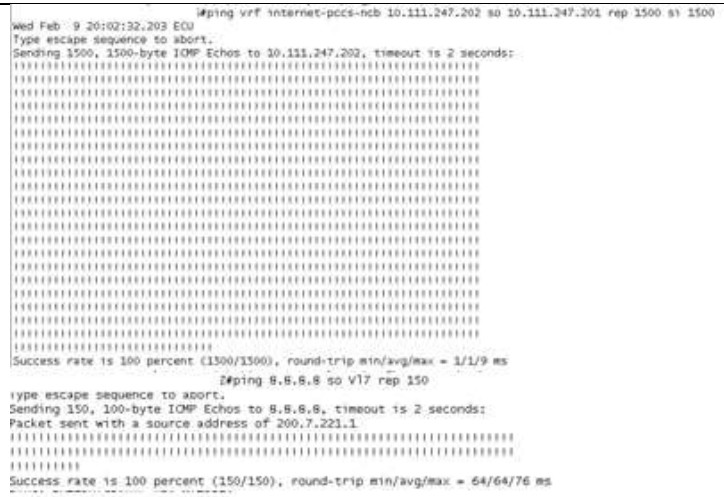
Pruebas de conectividad	Se realizan pruebas de conectividad hacia internet sin tener pérdidas de paquetes, como se visualiza en la prueba LAN y WAN.
	`#ping 8.8.8.8 so Vl10`
	`Type escape sequence to abort.`
	`Sending 5, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:`
	`Packet sent with a source address of 200.7.217.217`
	`!!!!!`
	`Success rate is 100 percent (5/5), round-trip min/avg/max = 56/57/60 ms`

<table>
<tr>
<td></td>
<td><pre>
                                        #ping 10.111.236.237 so 10.111.236.238 rep 1500 si 1500
Type escape sequence to abort.
Sending 1500, 1500-byte ICMP Echos to 10.111.236.237, timeout is 2 seconds:
Packet sent with a source address of 10.111.236.238
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1500/1500), round-trip min/avg/max = 1/1/8 ms
</pre></td>
</tr>
<tr>
<td>Conclusión</td>
<td>Con la aplicabilidad de recomendaciones de seguridad y en el equipo FW Fortinet del cliente, la activación de un perfil de EmailFilter, se logra verificar que la caída de la IP ya no está enlistada en una lista negra y el servicio no ha presentado inconvenientes.</td>
</tr>
</table>

Autor: Elaboración propia

Cuadro 18. Monitoreo Caso 004.- Ingreso no autorizado de equipos

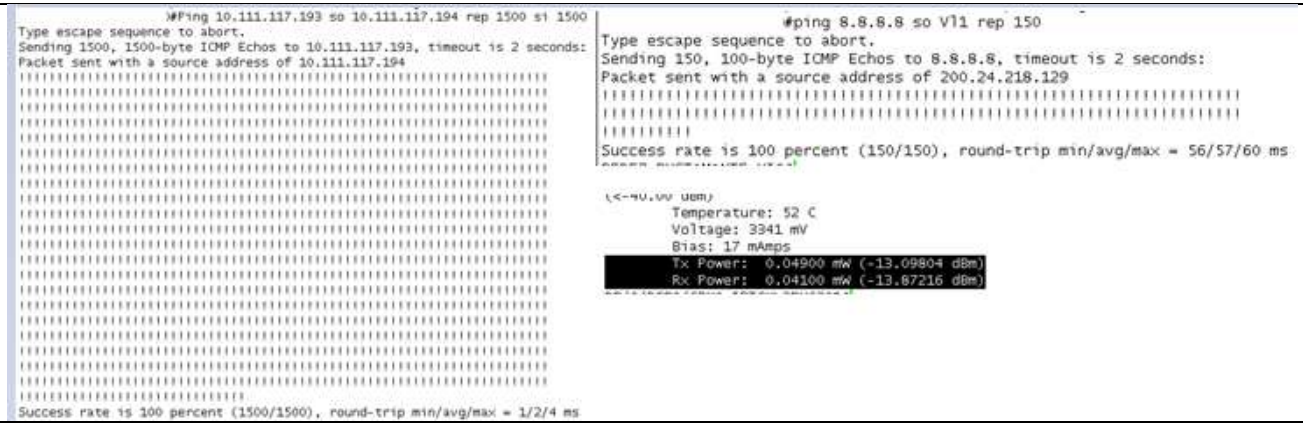
Tráfico del enlace	El evento de reinicio del equipo fue realizado el día 11 de noviembre del 2021, al verificar el tráfico de una semana se verifica que no existe caída del tráfico, al sacar el dato de un mes, de igual manera no se verifica caídas del tráfico, está acorde al histórico de consumo de ancho de banda. 
Análisis de logs	Al ingresar al equipo se verifica que ya no existe logs de reinicio, el *uptime* del equipo es de más de 12 semanas y a nivel de monitoreo el enlace ha presentado estabilidad sin caídas del mismo. 
Pruebas de conectividad	Por el inconveniente presentado, al momento se tiene acceso al equipo mediante SSH para las pruebas se verifica a nivel WAN sin perdidas de paquetes y los tiempos acordes a la tecnología de última milla empleada, a nivel LAN se verifica las pruebas de conectividad de manera exitosa.

	
Conclusión	Según la verificación en los logs y con el uptime del equipo se verifica que posterior a las recomendaciones brindadas el servicio ha permanecido operativo y no registra ingresos al equipo.

Autor: Elaboración propia

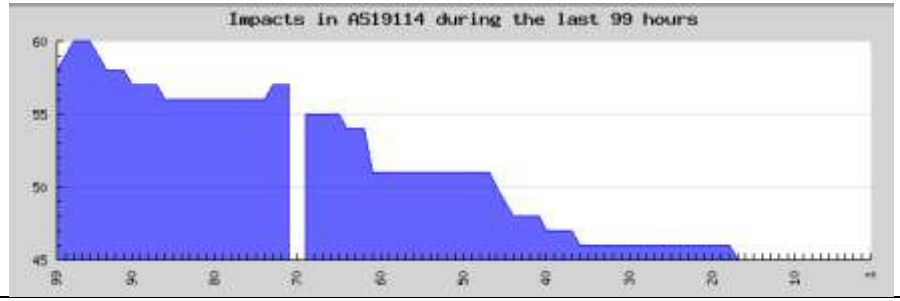
Cuadro 19. Monitoreo Caso 005.- Phishing

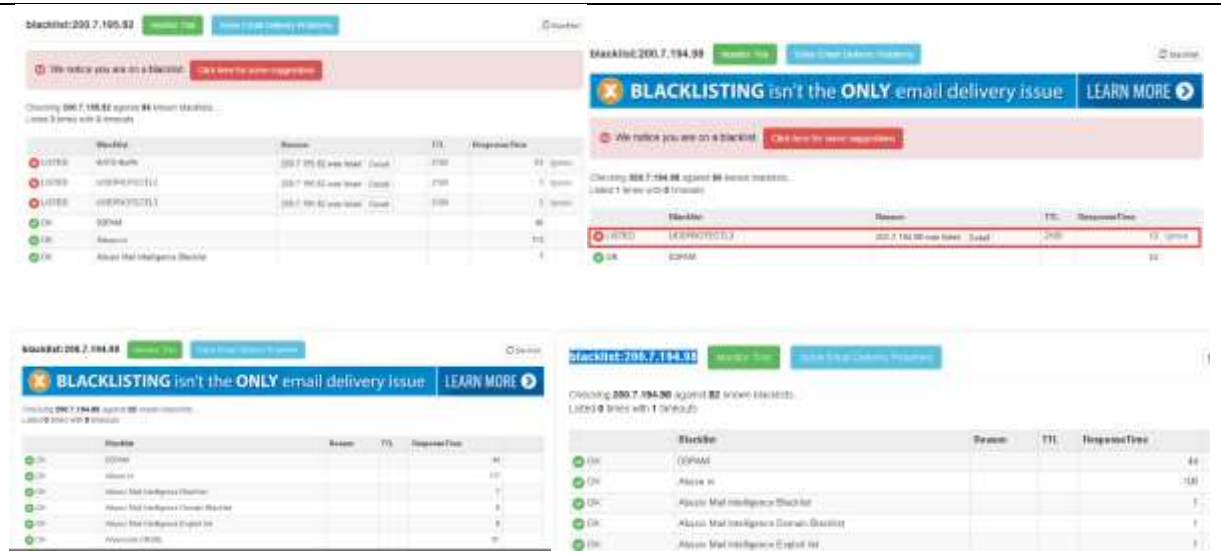
Tráfico del enlace	A nivel del tráfico, el mismo ha permanecido estable y no ha presentado caídas durante el monitoreo realizado de una semana y un mes. 
Análisis de logs	A verificación de logs no se verifica que exista algún inconveniente del servicio, sé válida una alarmar de caída de bgp la misma pertenece a la caída del enlace por temas de energía, el *uptime* coincide con el BGP. 
Pruebas de conectividad	A nivel de conectividad, se verifica salida hacia internet sin perdidas de paquetes, tampoco existe perdidas de paquetes a nivel WAN, los tiempos acordes a la última milla y la potencia esta correcta.

	
Conclusión	Se verifica a nivel de los canales de reporte que el cliente no ha presentado nuevamente este intento de ataque de phishing, no se recepto algún reporte, a nivel del equipo de administración CPE se verifica que el equipo no ha presentado inconvenientes y el servicio se ha mantenido estable y sin inconvenientes posteriores a las recomendaciones de seguridad brindadas al cliente.

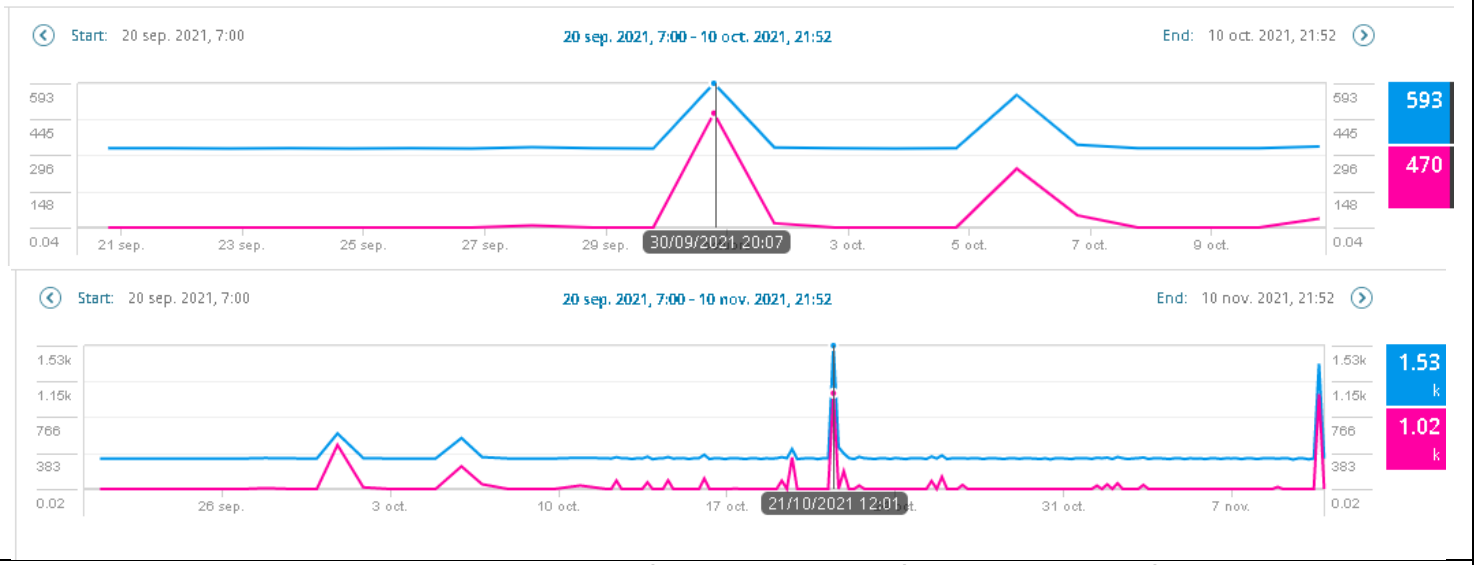
Autor: Elaboración propia

Cuadro 20. Monitoreo Caso 006.- Lista negra UCEPROTECT

Tráfico del enlace	Con ayuda de la página de enlistamiento de lista negra uceprotect se verifica que el número de IPs disminuye posterior al monitoreo del servicio de 7 días. 
Análisis de logs	A nivel de logs en la página, se verifica que el número de IPs que caen en listas negras eran de 50, se verificaba que el ASN presentaba alerta de color rojo.  Posterior a las recomendaciones realizadas y bloqueo de puertos se valida que el ASN tiene alerta amarilla y el número de IPS enlistado están disminuye, se valida la información brindada por la página de *Uceprotect*. 
Pruebas de conectividad	Con ayuda de la herramienta Mxtoolbox al analizar las IPS enlistadas, se valida que salieron en su totalidad y no presentan enlistamiento, los clientes confirman que ya envían correos electrónicos, en la figuras están antes del inconveniente reportado y después del bloqueo de puertos realizados.

	
Conclusión	Con las acciones realizadas de bloqueos de puertos y recomendaciones a los clientes de las acciones que ejecutaran en sus equipos de red interna, se valida que el ASN del ISP sale de lista negra y los clientes recuperan el servicio de envío de correos.

Autor: Elaboración propia

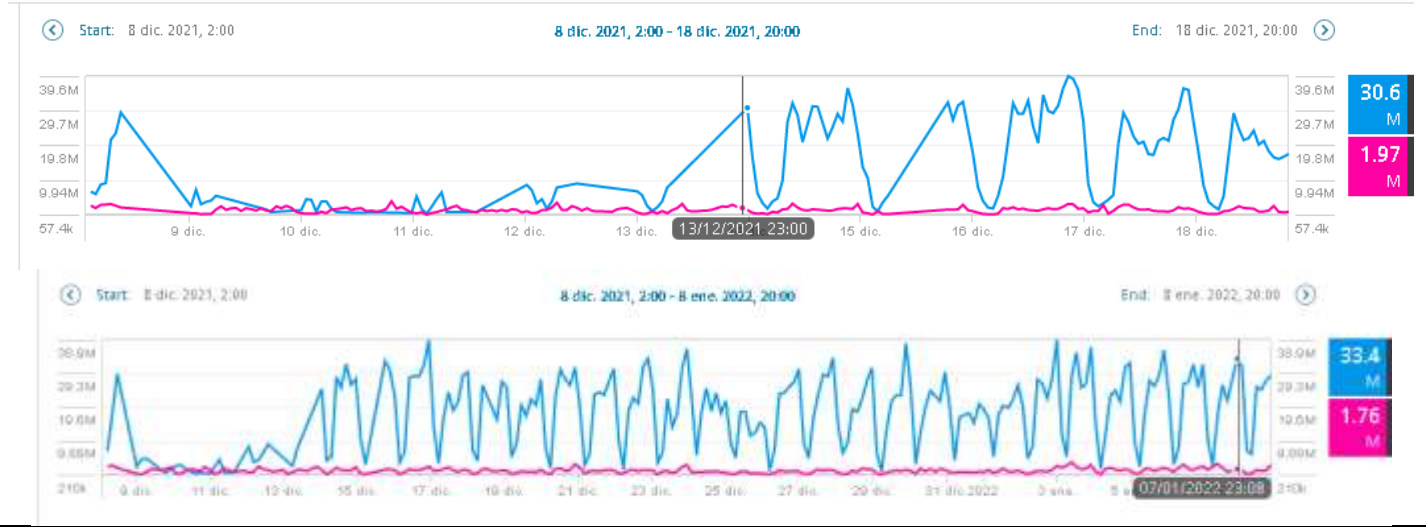
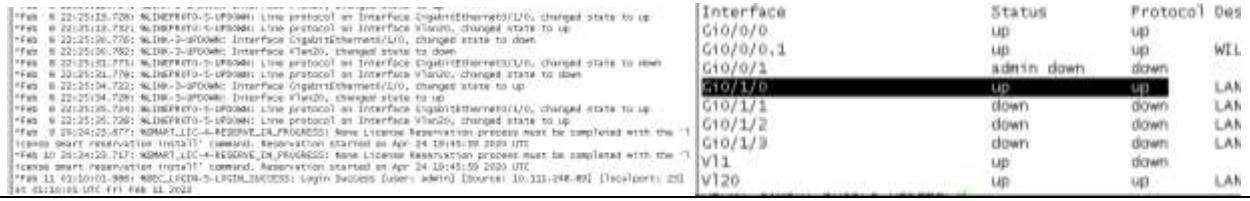
<table>
<tr><th colspan="2">Cuadro 21. Monitoreo Caso 007.- Ransomware</th></tr>
<tr><td>Tráfico del enlace</td><td>A nivel del tráfico del enlace se verifica que el mismo ha presentado estable y no presenta caídas, se remite el reporte de una semana y del mes posterior al evento.
 
</td></tr>
<tr><td>Análisis logs</td><td>En el equipo al validar los logs, no se verifican que algún log cause afectación del servicio, también el cliente ha contratado un servicio SDWAN posterior al ataque sufrido, con lo cual, migraron los servicios hacia dichos equipos.

*Jan 31 21:14:53.129: %TRACK-6-STATE: 6 ip sla 6 reachability Down -> Up
*Jan 31 21:14:53.165: %HSRP-5-STATECHANGE: Vlan3034 Grp 50 state Standby -> Active
*Jan 31 21:14:53.211: %HSRP-5-STATECHANGE: Vlan20 Grp 0 state Standby -> Active
*Jan 31 21:14:53.436: %HSRP-5-STATECHANGE: Vlan3034 Grp 40 state Standby -> Active
*Jan 31 21:14:54.126: %HSRP-5-STATECHANGE: Vlan301 Grp 100 state Standby -> Active
*Jan 31 21:14:54.651: %HSRP-5-STATECHANGE: Vlan314 Grp 20 state Standby -> Active</td></tr>
<tr><td>Pruebas de conectividad</td><td>Se verifica que el cliente ya desconecto el server en su totalidad que se vio afectado y para los otros equipos indica que implemento las medidas de seguridad necesarias para no presentar inconvenientes con sus equipos. Al verificar la tabla arp las IPs asignadas para los servers con MAC de equipos IBM, se verifica conectividad hacia los equipos sin perdidas, como se visualiza en la figura que son las pruebas de trobleshooting realizada.</td></tr>
</table>

	
Conclusión	El cliente no ha presentado nuevamente un ataque de tipo *ransowere,* el mismo indica que realizo las recomendaciones de seguridad emitidas, adicional por temas de seguridad, contrato un servicio SDWAN para conectividad entre todas las agencias, esto se valida que a nivel de logs no se verifica algún inconveniente del servicio, pruebas de conectividad de manera exitosa sin perdidas a nivel LAN y WAN.

Autor: Elaboración propia

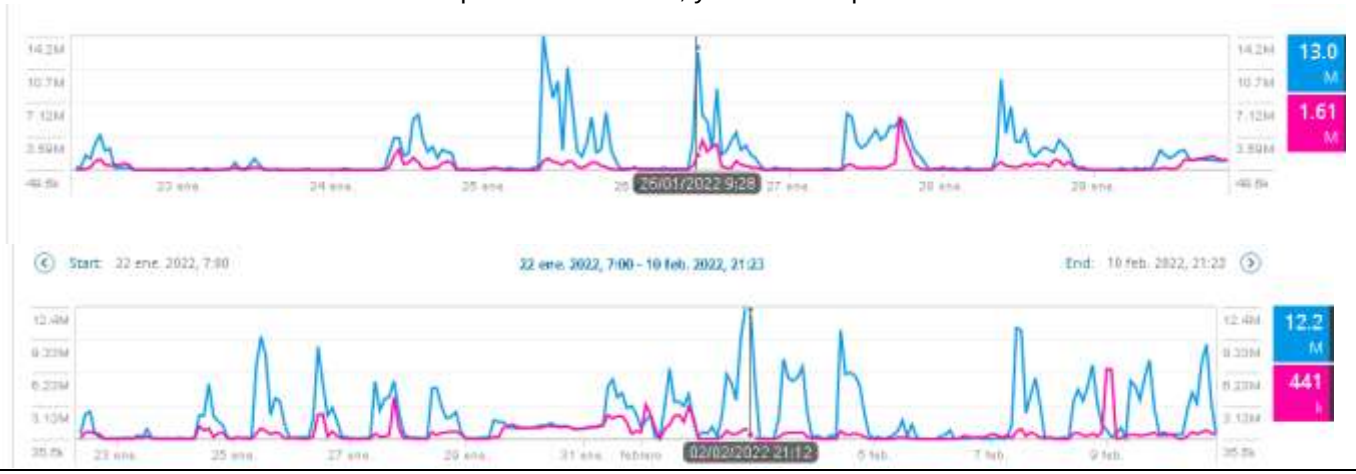
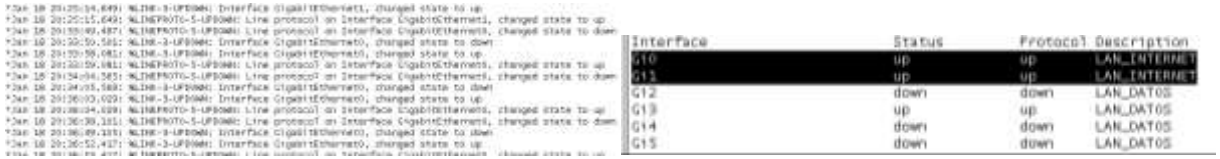
Cuadro 22. Monitoreo Caso 008.- Denegación de servicio

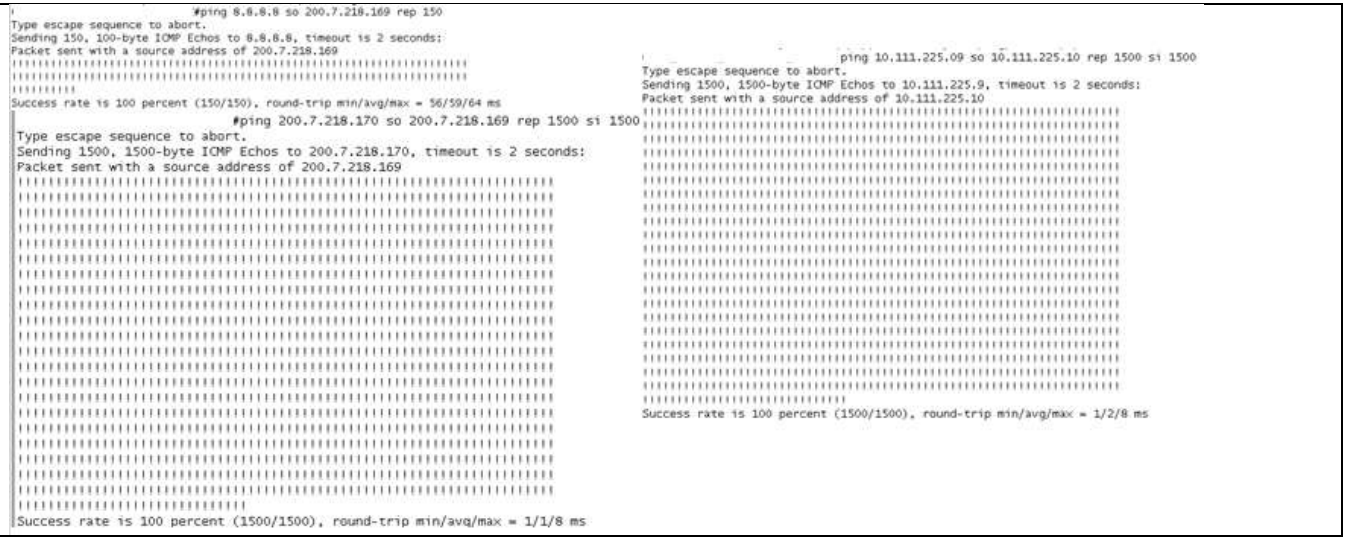
Tráfico del enlace	Al analizar el tráfico posterior al evento se valida que existe disminución del tráfico durante 4 días, posterior se restablece con normalidad, en el tráfico de una semana se nota como recupera consumo el enlace, en el tráfico de un mes está acorde a las demás semanas. 
Análisis de logs	Al ingresar al equipo CPE no se verifica logs que indica ingreso al equipo, se verifica unos flapeos en el puerto de la red LAN. 
Pruebas de conectividad	En el equipo se ejecuta pruebas a nivel LAN hacia los DNS de google, se valida los tiempos acordes a la última milla empleada, a nivel WAN se presenta conectividad del servicio sin perdidas de paquetes.

<table>
<tr><td></td><td>L#ping 8.8.8.8 so 200.7.227.33 rep 150
Type escape sequence to abort.
Sending 150, 100-byte ICMP Echos to 8.8.8.8, timeout is 2 seconds:
Packet sent with a source address of 200.7.227.33
!!
!!
!!!!!!!!!!
Success rate is 100 percent (150/150), round-trip min/avg/max = 60/60/64 ms
.#ping 10.111.242.221 so 10.111.242.222 rep 1500 si 1500
Type escape sequence to abort.
Sending 1500, 1500-byte ICMP Echos to 10.111.242.221, timeout is 2 seconds:
Packet sent with a source address of 10.111.242.222
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!
!!!!!!!!!!!!!!!!!!!!!!!!!!!!!!
Success rate is 100 percent (1500/1500), round-trip min/avg/max = 1/2/8 ms</td></tr>
<tr><td>Conclusión</td><td>Con las configuraciones de seguridad en el equipo CPE, el bloqueo al acceso web, se verifica que el servicio permanece estable sin perdidas de paquetes, adicional el cliente confirma que aplico las recomendaciones brindadas y capacitación a su personal para no volver a presentar el inconveniente.</td></tr>
</table>

Autor: Elaboración propia

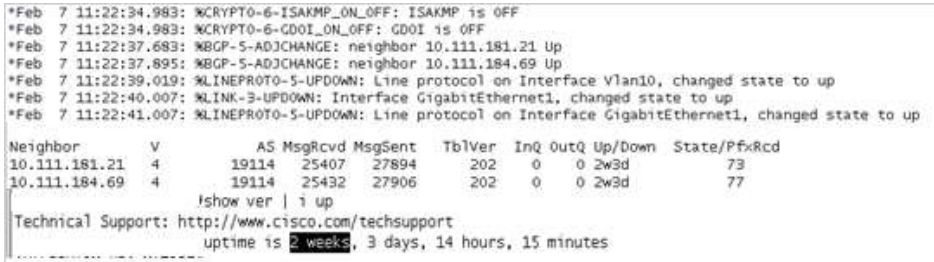
Cuadro 23. Monitoreo Caso 009.- Escaneo de puertos

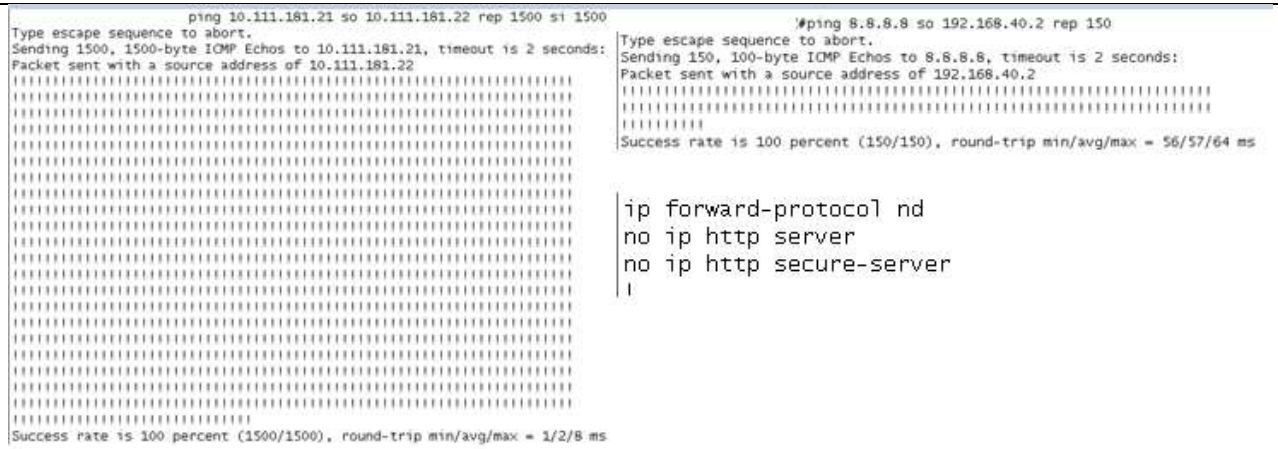
Tráfico del enlace	El tráfico de este enlace esta normal no ha presentado caídas, y se verifica que está acorde a su históricos. 
Análisis de logs	Al ser un equipo de red interna no se verificará algún log en dicho equipo, pero a nivel del CPE no se verifica logs de escaneo de puertos, se valida la interfaz Gi0 y Gi1 presentan flapeos los mismos son puertos de la red interna, como dato adicional los servicios están separados por VRF. 
Pruebas de conectividad	Las pruebas de conectividad en el equipo no presentan perdidas de paquetes, hacia los DNS de google, equipo de red interna y a nivel WAN sin inconvenientes, en la figura están las pruebas realizadas sobre el servicio.

	
Conclusión	El equipo CPE al realizar un análisis el mismo presenta las configuraciones de seguridad para evitar ataques de accesos, el equipo que sé válida el puerto abierto es el de la red interna, para lo cual, al cliente se le emitió las recomendaciones que aplique a nivel del su equipo, en cuanto al monitoreo del enlace y pruebas se verifica el servicio estable y sin inconvenientes.

Autor: Elaboración propia

Cuadro 24. Monitoreo 010.- Ataque Phishing

<table>
<tr><td>Tráfico del enlace</td><td>Al realizar el monitoreo del tráfico del enlace del evento presentado, no se verifica disminución de este, está conforme al histórico el tráfico tanto en el consumo de una semana como el de un mes.
 
</td></tr>
<tr><td>Análisis de logs</td><td>Al verificar los logs se llega a confirmar que no presenta inconvenientes el servicio de caídas y acceso al equipo, se ve una caída del bgp el mismo es por un tema eléctrico en la sede y el uptime del equipo concuerda con la caída de BGP.
 
</td></tr>
<tr><td>Pruebas de conectividad</td><td>En el equipo al realizar pruebas de conectividad no presenta perdidas de paquetes, el enlace adicional tiene configurado el bloqueo de acceso mediante web.</td></tr>
</table>

	
Conclusión	Con las recomendaciones de seguridad brindadas y la revisión realizada por parte de nuestra área del SOC se llega a validar que el servicio no se ha visto afectado, se tienen conectividad sin perdidas y el tráfico del servicio no ha presentado variación. El equipo de seguridad que tiene el cliente *dropeo* el intento de ataque y el cliente realizará las acciones necesarias para la capacitación del personal sobre el tema de *phishing.*

Autor: Elaboración propia

3.4. Verificación de la hipótesis

En los ítems anteriores, con ayuda de la herramienta de observación, se recopiló un total de 10 casos reportes de clientes corporativos que presentaron inconvenientes con su servicio, enfocado el mismo al tema de ciberseguridad. Por lo tanto, la hipótesis planteada para el presente proyecto indica que la aplicación de un conjunto de técnicas de ciberseguridad en la infraestructura de red a nivel de capa tres ofrecerá el mejor rendimiento de los clientes de datos fijos, con ayuda del monitoreo realizado del servicio posterior a las acciones realizadas y recomendaciones brindadas por su ISP se procede a analizar las variables para la demostración de la hipótesis planteada.

Para la comprobación de la hipótesis, se ha tomado dos variables para analizar, la latencia y la disponibilidad del servicio. En primera instancia se validaron que los valores recolectados provengan de una distribución normal. En las siguientes tablas 2 y 3 consecutivamente, se encuentra la información de la latencia y disponibilidad.

Tabla 2. Latencia de los casos analizados

Latencia		
CASO	PRE-TEST	POST-TEST
1	9 ms	6 ms
2	2 ms	2,84 ms
3	2 ms	1 ms
4	2 ms	1 ms
5	15 ms	10 ms
6	18 ms	8 ms
7	2 ms	1 ms
8	10 ms	10 ms
9	3 ms	3 ms
10	1 ms	1 ms

Autor: Elaboración propia

Tabla 3. Disponibilidad del servicio de los casos analizados

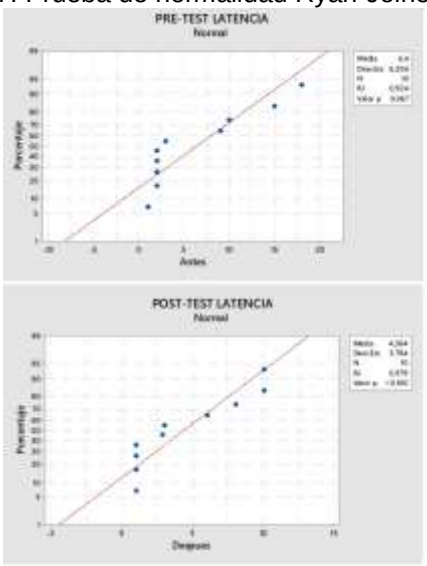
Disponibilidad		
CASO	PRE-TEST	POST-TEST
1	97,890 %	97,877 %
2	100,000 %	100,000 %
3	100,000 %	100,000 %
4	99,960 %	99,959 %
5	100,000 %	100,000 %
6	99,973 %	99,973 %
7	99,960 %	99,973 %
8	96,720 %	98,779 %
9	94,110 %	100,000 %
10	100,000 %	100,000 %

Autor: Elaboración propia

3.4.1. Prueba de normalidad

Esta prueba sirve para determinar si el conjunto de datos obtenidos está bien modelado para una distribución normal, con lo cual, permite utilizar un método estadístico para la comprobación de la hipótesis, al realizar el análisis del rendimiento y disponibilidad del servicio, con ayuda del *software Minitab*, posee varias técnicas para calcular la normalidad de los datos entre ellas está la prueba de normalidad de Ryan-Joiner, que calcula la correlación entre los datos y las puntuaciones normales de los datos. Si el coeficiente de correlación se encuentra cerca de 1, es probable que la población sea normal. En esta muestra de 10 datos de la latencia, él antes y después, el valor RJ resultante es 0,924 pres-test y 0,979 del *post-test* se encuentra cercano a 1, se tiene suficiente evidencia para concluir que los datos siguen la distribución normal, los resultados de los cálculos se evidencian en la figura 17. Por lo tanto, se aplicará un estadístico paramétrico *t-student*, para contrastar la hipótesis del proyecto de investigación.

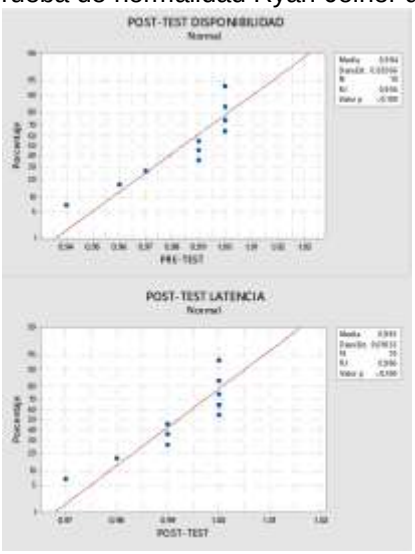
Figura 17. Prueba de normalidad Ryan-Joiner latencia



Autor: Elaboración propia

En cuanto a la disponibilidad del servicio, la muestra igual es de 10 datos que indican el resultado de *pre-test* con un valor en RJ de 0,956 y el *post-test* con un valor de 0,986, se encuentra cercano a 1 con lo que se comprueban que los valores son normales (Ver figura 18).

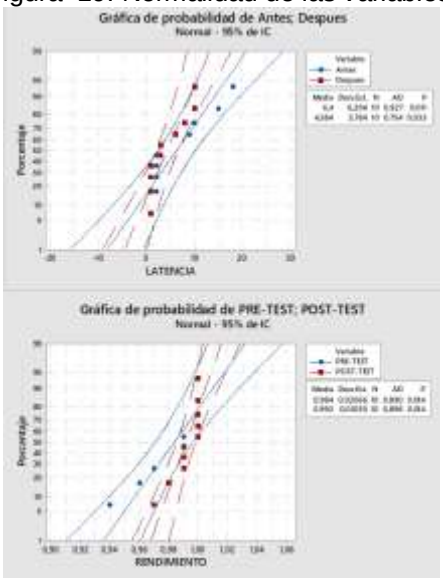
Figura 18: Prueba de normalidad Ryan-Joiner disponibilidad



Autor: Elaboración propia

En la figura 19 se valida que la probabilidad de la latencia, el valor de *p* es 0,011 y 0, 033 y en la gráfica del rendimiento el valor de *p* es 0,014, tanto para el pre como post test.

Figura 19. Normalidad de las variables.



Autor: Elaboración propia

3.4.2. Prueba estadística T-student

La hipótesis planteada en el proyecto de investigación indica:

- **H0=** La propuesta de mejores prácticas a nivel de infraestructura de red a los clientes corporativos mejorará el rendimiento de red, disminuye el reporte de incidentes del servicio a su proveedor.
- **H1=** La propuesta de mejores prácticas a nivel de infraestructura de red a los clientes corporativos no mejorará el rendimiento de red, aumenta el reporte de incidentes del servicio a su proveedor.

Con el planteamiento de las hipótesis se procede a realizar el cálculo con ayuda de Excel, arrojo los siguientes valores en la tabla 4 para la variable de la latencia. El resultado de la aplicabilidad de la técnica de comprobación de la hipótesis, indica que

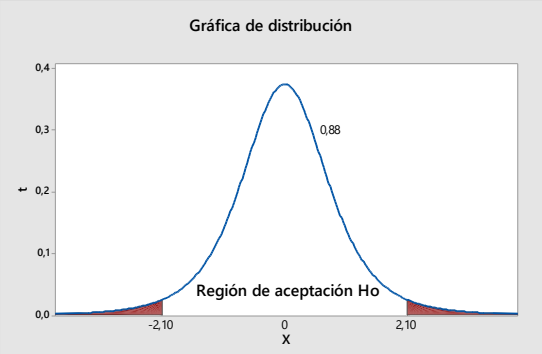
el valor de t es 0,88, lo cual, cae en la zona de aceptación, como se valida en la Figura 20, con lo que se comprueba que posterior a la aplicabilidad de las recomendaciones de seguridad los clientes corporativos disminuyen la latencia de sus servicios.

Tabla 4. Calculo valor t-student latencia

	PRE-TEST	*POST-TEST*
Media	6,4	4,384
Varianza	38,48888889	14,31900444
Observaciones	10	10
Varianza agrupada	26,40394667	
Diferencia hipotética de las medias	0	
Grados de libertad	18	
Estadístico t	0,877285814	
P(T<=t) una cola	0,195945192	
Valor crítico de t (una cola)	1,734063607	
P(T<=t) dos colas	0,391890384	
Valor crítico de t (dos colas)	2,10092204	

Autor: Elaboración propia

Figura 20. Gráfica distribución latencia

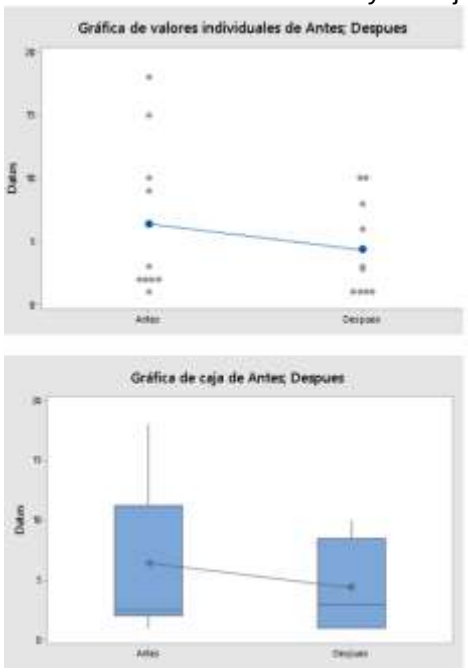


Autor: Elaboración propia

En paralelo se obtuvo las gráficas de valores individuales y la gráfica de caja, como se visualiza en la figura 21, en la misma también es visible la disminución de latencia del

servicio, en el anexo 1 se ubica las gráficas de latencia obtenidas para la recolección de datos de los clientes corporativos.

Figura 21. Gráfica valores individuales y de caja latencia



Autor: Elaboración propia

La otra variable planteada para la comprobación de la hipótesis es la disponibilidad de los clientes corporativos, con base en los datos del monitoreo de los enlaces se obtuvo la información de cada uno de ellos (ver tabla 5).

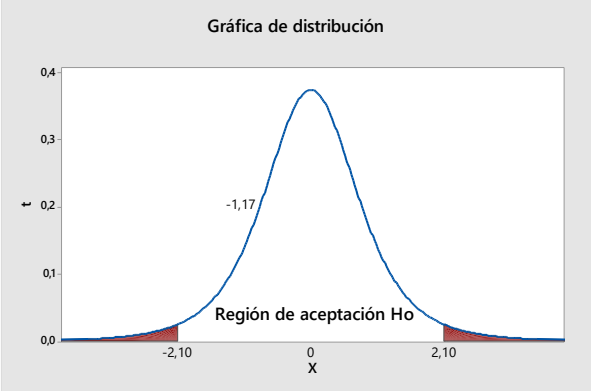
Tabla 5. Prueba t-student disponibilidad

	PRE-TEST	*POST-TEST*
Media	98,8613	99,6561
Varianza	4,104461344	0,535381878
Observaciones	10	10
Varianza agrupada	2,319921611	
Diferencia hipotética de las medias	0	
Grados de libertad	18	
Estadístico t	-1,166826289	
P(T<=t) una cola	0,129253479	
Valor crítico de t (una cola)	1,734063607	
P(T<=t) dos colas	0,258506958	
Valor crítico de t (dos colas)	2,10092204	

Autor: Elaboración propia

En este caso, el valor de t indica que está dentro del rango de aceptación, para lo cual, se llega a comprobar que existe mayor disponibilidad del servicio de los clientes corporativos, como se indica en la gráfica 22, el valor de t está dentro del rango de aceptación.

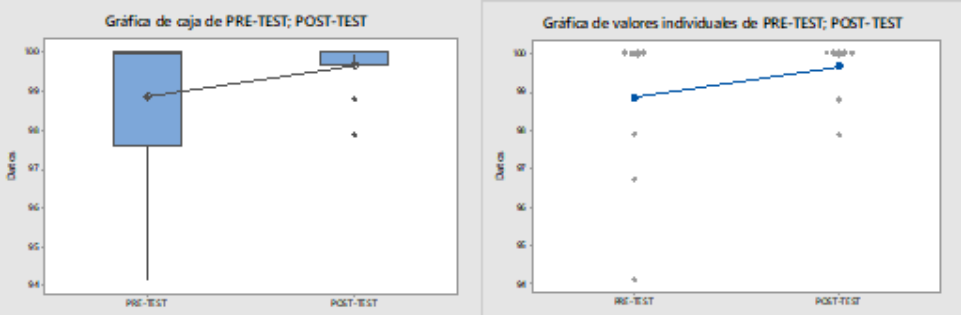
Figura 22. Gráfica distribución disponibilidad



Autor: Elaboración propia

Otras gráficas donde se verifica que existe el incremento de disponibilidad del servicio es la gráfica de caja y la gráfica de los valores individuales. En la figura 23, se valida que el servicio tiene una mayor disponibilidad. En el Anexo 2 se ubica la data de la obtención de los valores de la disponibilidad que se realizó el análisis.

Figura 23. Gráfica valores individuales y de caja, disponibilidad



Autor: Elaboración propia

Finalmente, se comprueba que la propuesta de mejores prácticas a nivel de infraestructura de red a los clientes corporativos mejorará el rendimiento de red, disminuye el reporte de incidentes del servicio a su proveedor.

CONCLUSIONES

- La descripción de los principales problemas de ciberseguridad de clientes corporativos en la infraestructura de un ISP, sirve de base para la propuesta de solución, y la implementación de las diferentes técnicas de investigación; se identificó los principales problemas de ciberseguridad, que presentan los clientes corporativos ligados a la infraestructura de su ISP, con lo cual; y, con ayuda de la norma ISO 27032, como referencia para la obtención de las mejores prácticas de seguridad, en relación con el inconveniente presentado o reportado por el cliente corporativo.

- La realización del estudio comparativo de los diferentes ataques de ciberseguridad que se han producido en los clientes corporativos dentro de un ISP, permitió verificar que el mayor ataque que presentan los clientes corporativos es de DoS, para lo cual, con el respectivo *troubleshooting* se logró restablecer el servicio y posterior brindar las recomendaciones de seguridad para la aplicabilidad en sus equipos de red interna.

- La definición de un conjunto de recomendaciones en la red LAN (Red de Área Local) de clientes corporativos y el análisis de la norma ISO 27032, son la base, para la generación de recomendaciones de seguridad, estas fueron emitidas a los clientes del ISP, para la aplicabilidad de normas o políticas de seguridad interna, para que, en futuros eventos de seguridad, disminuya la afectación de un ataque de red y restablecer su servicio en el menor tiempo posible.

RECOMENDACIONES

- Un cliente corporativo, cuando presente problemas con su servicio, por lo general realiza el reporte a la mesa técnica de su ISP para la revisión del inconveniente, sin embargo, si de lado del cliente corporativo no realiza las acciones necesarias para evitar que sus activos de red se vean comprometidos, el personal especializado del ISP ejecutara las revisiones necesarias al alcance de los equipos que se posea la administración, por lo cual, es de suma importancia que se realice la revisión y análisis de seguridad de la red interna cada cliente corporativo.

- El mayor inconveniente que reportan los clientes corporativos, representa la denegación del servicio, para lo cual, el área de TI de cada empresa aplicara los diversos métodos y técnicas de seguridad, necesarios para la mitigación de la afectación, así como, capacitar al personal, realizar pruebas de seguridad e invertir en el área de seguridad de las empresas para afrontar en caso de cualquier eventualidad de ataques de seguridad en su red.

- La norma ISO 27032 es una herramienta útil para el aseguramiento de los activos de red interna, por lo tanto, cada empresa tomará como referencia dicha norma para generar planes de contingencia. El uso de esta norma como referencia para recomendaciones de seguridad es de gran utilidad en la actualidad, con el incremento de nuevos métodos y la identificación de vulnerabilidades de día cero ayudaran a estar prevenidos en caso de presentar un ataque de seguridad en la empresa.

BIBLIOGRAFÍA

Aguilar, L. J. (2017). Ciberseguridad: la colaboración público-privada en la era de la cuarta revolución industrial (Industria 4.0 versus ciberseguridad 4.0). Cuadernos de estrategia, 185, 19–64.https://dialnet.unirioja.es/servlet/articulo?codigo=6115620

Arefin, M. T., Uddin, M. R., Evan, N. A., & Alam, M. R. (2021). Enterprise network: Security enhancement and policy management using next-generation firewall (NGFW). En Computer Networks, Big Data and IoT (pp. 753–769). Springer Singapore.

Armendáriz, D. N. L. (2017). Modelo de gestión de los servicios de tecnología de información basado en COBIT, ITIL e ISO/IEC 27000. Revista Tecnológica - ESPOL, 30(1). http://200.10.150.204/index.php/tecnologica/article/view/581

Avast. 2021. «Guía esencial del phishing: cómo funciona y cómo defenderse». Guía esencial del phishing: cómo funciona y cómo defenderse. (https://wwwa vast. com/es-es/c-phishing).

Briceño, Edgar Vega. 2021. Seguridad de la información. Ciencias.

Buchner, T. (2022). A SDN-operated MEC node for network cybersecurity assurance. 2022 International Conference on Optical Network Design and Modeling (ONDM), 1

Chinchilla, E. J. S., & Allende, J. S. (2017). Riesgos de ciberseguridad en las Empresas. Tecnología y desarrollo, 15(0). https://revistas.uax.es/index.php/tec_des/article/view/1174

Cisco. 2021. «What Is the Difference Between SD-WAN and MPLS» Cisco. (https:/www.cisco.com/c/en/us/products/routers/what-is-the-difference-between-sd-wan-and-mpls.html).

Contreras, C. SD-WAN: Cómo mejorar la seguridad de la infraestructura IT. Estrategia y Negocios. https://www.estrategiaynegocios.net/tecnologia-cultura-digital/sd-wan-como-mejorar-la-seguridad-de-la-infraestructura-it-JX6716964

Cruzado Puente de la Vega, C. F., & Rodriguez Baca, L. S. (2022). Marco de referencia "HOGO" para ciberseguridad en PyMES basado en ISO 27002 y 27032. Universidad Peruana Unión.

Cruzado, C. F., Rodriguez-Baca, L. S., Huanca-Lopez, L. G., & Acuna-Salinas, E. I. (2022). Reference framework "HOGO" for cybersecurity in SMEs based on ISO 27002 and 27032. 2022 12th International Conference on Cloud Computing, Data Science & Engineering (Confluence), 35–40

Danilo Jaramillo, H., Cabrera, S. A., Abad, E. M., Torres, V. A., & Verdum, J. C. (2015). Definition of cybersecurity businness framework based on ADM-TOGAF. 2015 10th Iberian Conference on Information Systems and Technologies (CISTI),1–7

Datta Business Innovation. 2021. «Malware: más de la mitad de las empresas en América Latina están preocupadas». Datta Business Innovation.(https://datta.com.ec/articulo/malware-mas-de-la-mitad-de-las-empresas-en-america-latina-estan-preocupadas).

Dominguez, A. H. (2018). Sistema para la detección de ataques PHISHING utilizando correo electrónico. Telem@tica (La Habana), 17(2), 60–70. https://revistatelematica.cujae.edu.cu/index.php/tele/article/view/304

Guzmán Solano, Sandra Liliana. 2019. «Guía para la implementación de la norma ISO 27032». 69.

Hashiyana, V., Haiduwa, T., Suresh, N., Bratha, A., & Ouma, F. K. (2020). Design and implementation of an IPSec Virtual Private Network: A case study at the University of Namibia. 2020 IST-Africa Conference (IST-Africa), 1–6.

Hernández Dominguez, A., & Baluja García, W. (2021). Principales mecanismos para el enfrentamiento al phishing en las redes de datos. https://repositorio.ucicu/handle/123456789/9692

Infante-Moro, A., Infante-Moro, J. C., & Gallardo-Pérez, J. (2022). Factores claves para concienciar la ciberseguridad en los empleados. Revista de pensamiento estratégico y seguridad CISDE, 7(1), 69–79. http://uajournals.com/ojs/index.php/cisdejournal/article/view/1126

ISO 27000. 2021. «Serie 27k». Serie «27000».(ht tps ://www.iso27000.es/is o27000 .html).

Kalashnikov, A. O., & Anikina, E. V. (2019). Complex network cybersecurity monitoring method. 2019 Twelfth International Conference “Management of large-scale system development” (MLSD), 1–3.

Karnatar, anmohamm. 2021. «Ejemplo de Configuración de las Funciones de Seguridad de Capa 2 en los Switches de Configuración Fija de Capa 3 de Cisco Catalyst». Cisco. (https://ww w.cisco.co m/c/es_m x/support/ docs/switc hes/ca taly st-3750-series-switches/72846-layer2-secftrs-catl3fixed.html).

López, F., & Bryan, K. (2017). Estudio y análisis de ciberataques en América Latina, su influencia en las empresas del Ecuador y propuesta de políticas de ciberseguridad. Universidad Católica de Santiago de Guayaquil.

Maldonado, M., & Mónica, N. (2021). Estado de la Ciberseguridad en las Empresas del Sector Público del Ecuador: Una Revisión Sistemática

Meriah, I., & Arfa Rabai, L. B. (2019). Comparative study of ontologies based ISO 27000 series security standards. Procedia Computer Science, 160, 85–92. https://doi.org/10.1016/j.procs.2019.09.447

Pamplin, S. (2021). SD-WAN revolutionises IoT and edge security. Network Security, 2021(8), 14–15. https://doi.org/10.1016/s1353-4858(21)00090-8

Pérez, André. 2020. La seguridad de las redes. ISTE Group. Questionpro. 2021. «Investigación cualitativa | QuestionPro». ¿Qué es la investigación cualitativa? (https://www.questionpro.com/es/investigacion-cualitativa.html).

Puchianu, D. C., Angelescu, N., Predusca, G., Circiumarescu, D., & Diaconu, E. (2020). Comparative study of power consumption on Mikrotik and Fortigate routers. 2020 12th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), 1–4.

Ransomware. 2021. «El ransomware: qué es, cómo se lo evita, cómo se elimina». latam.kaspersky.com.(https://latam.kaspersky.com/resource-center/threats/ransomware).

Regina Baena, G., Mendoza Mendez, R. V., & Joel Coronado, E. D. (2019). Importancia de la norma ISO/EIC 27000 en la implementación de un sistema de gestión de la seguridad de la información. contribuciones a la Economía, junio. https://www.eumed.net/rev/ce/2019/2/norma-iso-eic.html

Rianafirin, K., & Kurniawan, M. T. (2017). Design network security infrastructure cabling using network development life cycle methodology and ISO/IEC 27000 series in

Yayasan Kesehatan (Yakes) Telkom Bandung. 2017 4th International Conference on Computer Applications and Information Processing Technology (CAIPT),

Rochina, R., & Gonzalo, C. (2021). Diseño y evaluación de una metodología para reducir los ciberataques originados a través de correo electrónico mediante la aplicación de filtros y reglas sobre un Gateway. Escuela Superior Politécnica de Chimborazo.

Roeder, G. S., & Bailis, J. M. (2000). The pachytene checkpoint. Trends in Genetics: TIG, 16(9), 395–403. https://doi.org/10.1016/s0168-9525(00)02080-1

Sánchez-Henarejos, Ana, José Luis Fernández-Alemán, Ambrosio Toval, Isabel Hernández-Hernández, Ana Belén Sánchez-García, y Juan Manuel Carrillo de Gea. 2014. «Guía de buenas prácticas de seguridad informática en el tratamiento de datos de salud para el personal sanitario en atención primaria». Atención Primaria 46(4):214-22. doi: 10.1016/j.aprim.2013.10.008.

SD WAN CISCO. 2021. «Oferta del paquete de Cisco Cloud ACI y Cisco SDWAN». Cisco.(https://www.cisco.com/c/es_mx/solutions/data-center-virtualization/application-centric-infrastructure/cloud-aci-sdwan-offer.html).

Security, Panda. 2019. «¿Cómo Evitar Los Ataques de Día Cero?» Panda Security Mediacenter. (https://www.pandasecurity.com/es/mediacenter/consejos/como-evitar-los-ataques-de-dia-cero/).

Sierra Ciudad, Jose Carlos. 2021. «Troubleshooting ISP | PDF». Scribd.(https://esscribd.com/document/334114849/Troubleshooting-ISP).

Tello Baquero, K. I., & Director, F. C. L. (2020). Implementación de un clúster de firewall -checkpoint para reemplazar el firewall-router de una Administradora de Fondos Complementarios Provisional Cerrado. ESPOL. FIEC.

Tipton, H. F. (2001). Information security management handbook, fourth edition, volu me III. Auerbach.

Wen, Y., & Liu, T. (2018). WIFI security certification through device information. 2018 International Conference on Sensor Networks and Signal Processing (SNSP), 302–305.

Zafft, A., & Agu, E. (2017). Malicious WiFi networks: A first look. 37th Annual IEEE C onference on Local Computer Networks -- Workshops, 1038–1043.

ANEXOS

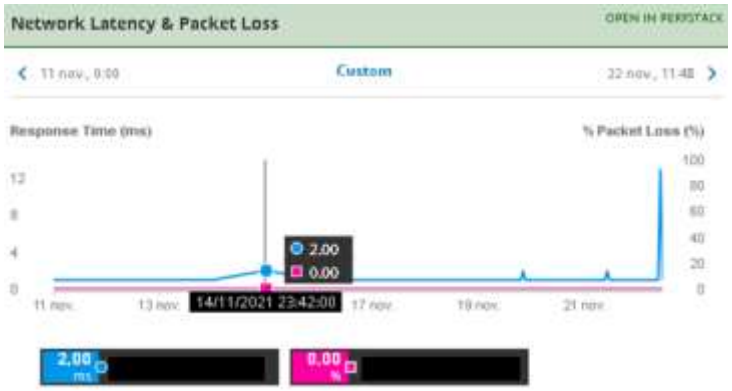
Anexo 1

Latencia de clientes corporativos

Caso 01

Caso 02

Caso 03



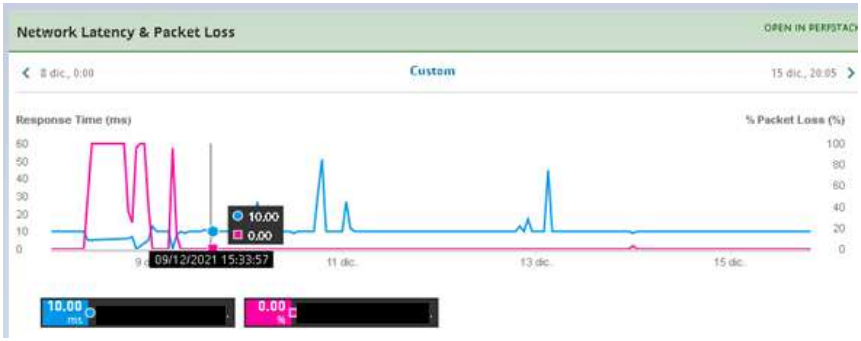
Caso 04

Caso 05

Caso 06

Caso 07

Caso 08



Caso 09

Caso 10

ANEXO 2

Caso 01

Availability Statistics

PERIOD	AVAILABILITY
Today	100,000 %
Yesterday	100,000 %
Last 7 Days	100,000 %
Last 30 Days	97,877 %
This Month	100,000 %
Last Month	97,890 %
This Year	99,303 %

Caso 02

PERIOD	AVAILABILITY
Today	100,000 %
Yesterday	100,000 %
Last 7 Days	100,000 %
Last 30 Days	100,000 %
This Month	100,000 %
Last Month	100,000 %
This Year	100,000 %

Caso 03

Availability Statistics HELP

PERIOD	AVAILABILITY
Today	100,000 %
Yesterday	100,000 %
Last 7 Days	100,000 %
Last 30 Days	100,000 %
This Month	100,000 %
Last Month	100,000 %
This Year	100,000 %

Caso 4

Availability Statistics

PERIOD	AVAILABILITY
Today	100,000 %
Yesterday	100,000 %
Last 7 Days	100,000 %
Last 30 Days	99,959 %
This Month	100,000 %
Last Month	99,960 %
This Year	99,987 %

Caso 05

Availability Statistics

PERIOD	AVAILABILITY
Today	100,000 %
Yesterday	100,000 %
Last 7 Days	100,000 %
Last 30 Days	100,000 %
This Month	100,000 %
Last Month	100,000 %
This Year	100,000 %

Caso 06

Availability Statistics

PERIOD	AVAILABILITY
Today	100,000 %
Yesterday	100,000 %
Last 7 Days	100,000 %
Last 30 Days	99,973 %
This Month	100,000 %
Last Month	99,973 %
This Year	99,781 %

Caso 07

Availability Statistics

PERIOD	AVAILABILITY
Today	100,000 %
Yesterday	100,000 %
Last 7 Days	100,000 %
Last 30 Days	99,973 %
This Month	100,000 %
Last Month	99,960 %
This Year	99,785 %

Caso 08

Availability Statistics

PERIOD	AVAILABILITY
Today	100,000 %
Yesterday	100,000 %
Last 7 Days	100,000 %
Last 30 Days	98,779 %
This Month	100,000 %
Last Month	96,720 %
This Year	98,903 %

Caso 09

Availability Statistics

PERIOD	AVAILABILITY
Today	100,000 %
Yesterday	100,000 %
Last 7 Days	100,000 %
Last 30 Days	100,000 %
This Month	100,000 %
Last Month	94,110 %
This Year	97,410 %

Caso 10

Availability Statistics

PERIOD	AVAILABILITY
Today	100,000 %
Yesterday	100,000 %
Last 7 Days	100,000 %
Last 30 Days	100,000 %
This Month	100,000 %
Last Month	100,000 %
This Year	94,168 %