ESCUELA DE POSGRADO NEWMAN

MAESTRÍA EN

GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN

Propuesta de mejora para la gestión de la seguridad de la compañía ADESGAE CÍA LTDA, Ecuador 2022

Trabajo de Investigación

para optar el Grado a Nombre de la Nación de:

Maestro en
Gestión de Tecnologías de la Información

Autor:

Bach. Vinces Flores, Alex Mauricio

Director:

Mtro. Díaz Zelada, Yvan Francisco

TACNA – PERÚ

2022

“El texto final, datos, expresiones, opiniones y apreciaciones contenidas en este trabajo son de exclusiva responsabilidad del autor”

TABLA DE CONTENIDO

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

RESUMEN

El presente trabajo de investigación tiene como finalidad mejorar la gestión de seguridad en la compañía Adesgae Cía Ltda, dentro de la cual se proponen medidas de corrección y de control para su infraestructura, ambientes locales, servidores y equipos de cómputo de los usuarios finales; la misma servirá para aplicar métodos de seguridad, a través de herramientas necesarias e importantes como antivirus, parches de actualizaciones en los sistemas operativos, políticas de navegación segmentada por cargos y roles, seguridad perimetral y filtrado web, cierre de brechas de vulnerabilidades en la arquitectura, aplicar políticas de control de acceso a los diferentes sistemas de información. Además de proponer métodos de contingencia ante situaciones críticas y actuar de manera ágil ante eventos de recuperación de desastres, permitiendo contribuir con acciones que faciliten y garanticen la continuidad del negocio.

INTRODUCCIÓN

El origen de las aplicaciones de negocio y plataformas informáticas cada vez se vuelven más importantes y cotidianas en las actividades diarias de las personas permitiendo así que exista mayor accesibilidad desde cualquier lugar del mundo; La tecnología avanza y con aquello también nuevas costumbres con la humanidad, herramientas o aplicaciones que no se usaban actualmente son la rutina diaria de muchas personas para cumplir sus tareas educativas, laborales, personales, etc.

Prepararse rápidamente para optar nuevas costumbres también tiene trabajo por debajo que muchas veces no se analiza y se debe considerar para evitar problemas a futuro; a muchas organizaciones les toca empezar a revisar sus riesgos y vulnerabilidades puesto que los ataques cibernéticos también juegan un papel importante en la vida diaria de los administradores de redes y seguridades. Monitorear, encontrar, corregir, solventar y volver a monitorear son funciones que hoy en día se deben considerar dentro de los temas de seguridad en las organizaciones. Capacitar o preparar a los usuarios es clave para evitar ataques o riesgos que puedan perjudicar a las organizaciones, por este motivo se direcciona el presente trabajo de investigación para determinar posibles riesgos que se tienen en las organizaciones y dar una visión de cómo poder mitigarlos y corregirlos a tiempo a través de la ciberseguridad, considerando muchos aspectos o herramientas necesarias para controlar de manera óptima y minimizar los riesgos a los cuales se está expuesto a nivel global. La seguridad y compromiso debe ser responsabilidad de todos.

CAPITULO I: ANTECEDENTES DE ESTUDIO

1.1 Título

Propuesta de mejora para la gestión de la seguridad de la compañía ADESGAE CÍA LTDA, Ecuador 2022.

1.2 Planteamiento del problema

La presente investigación busca diseñar e implementar una propuesta de mejora para la gestión de la seguridad física y lógica en la compañía ADESGAE CÍA LTDA, en base a acciones, herramientas y aplicaciones de controles. Tras la auditoria de procesos y seguridades de la norma ISO 27001, muestran el estado de la situación de la compañía, lo que permite mantener una visión clara de donde estamos, las deficiencias que se mantienen, los riesgos y vulnerabilidades que afectan gravemente a la organización.

Al realizar el análisis y levantamiento de información en la organización, según el diagnóstico de la situación actual de la compañía ADESGAE CÍA LTDA se procede a determinar los hallazgos encontrados, los mismos que se detallan de la siguiente forma:

- La compañía no cuenta con sistemas de recuperación anti-desastres que permitan generar una reconstrucción rápida ante posibles problemas de seguridad.
- No se ha ejecutado un análisis de vulnerabilidades en aplicaciones o sitios publicados para determinar o cerrar brechas de seguridad existentes.
- No se mantiene un firewall, ni políticas de funcionalidades para la

seguridad perimetral.

- Existen equipos con sistemas operativos desactualizados dentro de su infraestructura, con versiones que ya no mantienen soporte del fabricante.
- No se mantiene una consola de administración de antivirus en los equipos se encuentran dos versiones con licencias caducadas las mismas que no permiten el control y administración de los equipos de cómputo de manera óptima.
- No existe una matriz de riesgos que permita encontrar los posibles errores que puedan ocasionar un desastre organizacional.
- No se mantienen políticas de control de contraseñas y protocolo de seguimiento constante.
- Se mantienen activos los ingresos a servidores por servicio RDP de Windows.

Figura 1

Visualización de vulnerabilidades

Podemos confirmar que la situación actual mantiene riesgos muy altos, tentativamente las causas son producto de descuidos en la administración de los servicios IT de la compañía, así también al poco control y presupuesto destinado anualmente, es primordial poder emitir las consecuencias cuantificables acerca de este estatus, puesto que el impacto de mantener brechas de seguridad y vulnerabilidades podrían considerar pérdidas considerables en la operación y fidelización de clientes. Una hora de NO OPERACIÓN debido a un ataque cibernético, en uno de los 5 establecimientos que bordea una facturación diaria de $25.000 con un margen de utilidad del 12% podría representar un margen muy delicado para la rentabilidad y estabilidad operacional.

Las deficiencias y falencias encontradas son de apoyo para poder aclarar el ambiente de la situación, en el caso de no atender esta necesidad, se genera un impacto considerable para la organización, afectaría directamente a sus ventas, a sus ingresos, rentabilidad y fidelización de clientes; no se garantiza la continuidad del negocio y perjudica notablemente el crecimiento y expansión, tomando en cuenta que la idea y visión de todo core de negocio es mantener, crecer y mejorar sus productos y servicios; los mismos deben estar ligados con herramientas o controles tecnológicos que puedan garantizar la seguridad de su información, la imagen corporativa, los datos de la compañía y la de los clientes.

Para mitigar estas vulnerabilidades y poder emitir acciones correctivas es necesario empezar a cerrar cada una de estas brechas, podemos establecer el objetivo de la propuesta de mejora centrándonos en (Controlar, administrar y

monitorear las diferentes aplicaciones del negocio a través de agentes de seguridad para las herramientas, equipos y accesorios garantizando la operatividad de los sistemas de información de la compañía ADESGAE CÍA LTDA). Como medida de control procederemos a implementar herramientas de monitoreo como Falcon, Qualys y Lumu, que permiten mantener sensores en los equipos y servidores. Del mismo modo agregar un firewall en modo (activo/pasivo) siendo este un pilar de balanceo en el caso de surgir un evento fortuito, no verse afectado el servicio de internet en el negocio estableciendo roles de navegación, filtrado web y accesos VPN; otros detalles y acciones son la implementación de Directorio Activo con políticas de grupos, controles de análisis de vulnerabilidades y ethical hacking anuales como medida de control a los sistemas actuales y a las posibles nuevas herramientas, las mismas que no deben colocarse en producción sin la debida autorización y cierre de brechas, puntos muy importantes como la elaboración del proceso de recuperación anti-desastres, servidores WSUS para actualización de parches y actualizaciones en Sistemas Operativos, establecer políticas de seguridad de contraseñas y documentación necesaria para las matrices de riesgos son fundamentales pero deberán realizarse en fases para evitar empezar proyectos a la par que podrían ocasionar o dilatar la prioridad de la necesidad.

Figura 2

Infraestructura de red con protección de firewall

Es importante recalcar los costos iniciales dependiendo de la cantidad de licencias, equipos o infraestructura a adquirir en cada proyecto con sus debidos indicadores y métricas de control considerando tiempos de respuestas, recursos y rutas de implementación.

1.3 Objetivos

El presente trabajo investigativo tiene como objetivo general y objetivos específicos los que se enuncian a continuación:

1.3.1 Objetivo general

- Diseñar una propuesta de mejora para la seguridad informática física y lógica en la empresa ADESGAE CÍA LTDA como consecuencia de los ataques cibernéticos mundiales. Ecuador, 2022.

1.3.2 Objetivos específicos

- Analizar las brechas de seguridad en la infraestructura de la compañía, a través del levantamiento de información, análisis forense y pintest.
- Diseñar herramientas de control, accesos, auditoría y de monitoreo con la finalidad de velar y garantizar la operación a través de las conexiones DNS's, conexiones RPD a los servidores de producción, y control antivirus

en los endpoints con la finalidad de evaluar el comportamiento de las aplicaciones y equipos de la organización.

- Proponer actualizaciones de sistemas operativos en Servidores y migraciones de versiones de los servidores de Producción.
- Actualizar o revisar políticas de navegación y seguridad perimetral de FW. Del mismo modo validar accesos y usuarios VPN.
- Definir procesos de recuperación anti-desastres en los servidores de BD.

1.4 Metodología

La propuesta de mejora se realiza en la compañía “ADESGAE CÍA LTDA”, revisando la infraestructura actual, haciendo un levantamiento de información en base a los detalles observados por el área de IT, realizaremos la investigación aplicada. Este tipo de investigaciones están orientadas a mejorar, perfeccionar u optimizar el funcionamiento de los sistemas, los procedimientos, normas, reglas tecnológicas actuales a la luz de los avances de la ciencia y la tecnología; por tanto, este tipo de investigación no se presta a la calificación de verdadero, falso o probable sino a la de eficiente, deficiente, ineficiente, eficaz o ineficaz *(Ñaupas H., Mejía, E., Novoa, E. & Villagomez, A. 2013).*

Se justifica la metodología ya que en la propuesta procedemos a detallar las herramientas y estrategias de control para la gestión de la seguridad en la organización indicada y así lograr el objetivo propuesto.

Figura 3

Tipos y diseños de la metodología

Una vez establecido el tipo de metodología procedemos a realizar el diseño, considerando todo el conjunto de métodos a usar en la propuesta de mejora, el diseño será en campo, en la misma organización, a través de consultas, encuestas, estadísticas y validaciones a los integrantes del departamento de Sistemas; para analizar la problemática y establecer los caminos necesarios.

Se establecen medios para obtener información inicial, se obtiene el inventario de equipos de cómputo para establecer cantidad de licencias a utilizar, se solicita información de datacenter ’s y host ’s para evaluar las implementaciones de servicios, se considera el presupuesto para evaluar el costo/beneficio de la propuesta, se validan herramientas actuales que puedan servir para la propuesta y así evitar renovaciones anuales o servicios de mantenimientos con los proveedores actuales.

Se procede a realizar las encuestas a dos personas de soporte del área de Sistemas (Técnico de infraestructura y Técnico de Soporte) para determinar bases o pilares desde el punto de vista tecnológico:

Técnico de Infraestructura

¿Considera que mantiene seguridad idónea en su infraestructura tecnológica?

¿Se ha realizado un análisis de vulnerabilidades el año en curso?

¿Mantiene el control de los accesos a los sistemas y Servidores Locales?

¿Tiene un control de las políticas de navegación y seguridad perimetral en el Firewall?

¿Maneja un sistema de recuperación anti-desastres actualmente?

¿Consideras que implementar herramientas de seguridad ayudaría a prevenir incidentes de seguridad en la organización?

¿Requieres herramientas para administración, control y monitoreo de seguridad?

Técnico de Soporte

¿Mantienen los equipos de cómputo todas las actualizaciones y parches de seguridad del sistema operativo?

¿Mantienen los respaldos de las BD de los servidores de producción en caso de daños?

¿Mantienen controles de accesos a las aplicaciones locales?

¿Mantienen los roles y accesos determinados para los usuarios con políticas de cambios?

¿Mantienen los antivirus actualizados en los equipos de los usuarios?

Se procede a realizar una encuesta al departamento financiero para conocer estatus presupuestarios que puedan servir como base para las inversiones que se requieran realizar (Gerente Financiero):

Gerencia Financiera

¿Se mantiene vigente presupuesto para Tecnología?

¿Se ha evaluado la inversión para la parte de seguridad en la compañía?

¿Estaría de acuerdo en evaluar inversión en seguridad para la compañía?

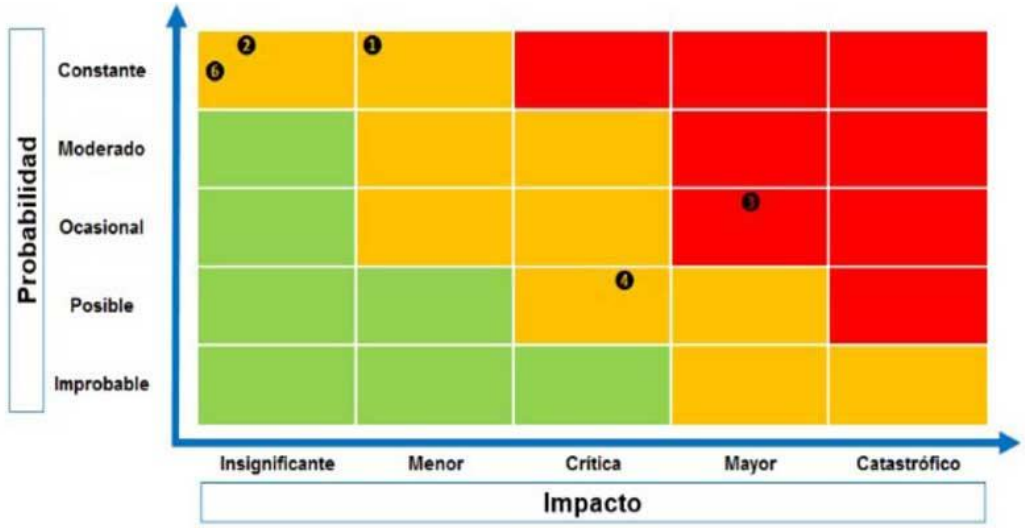
¿Podría gestionar la compra / adquisición de licenciamiento o equipos necesarios para la seguridad de la compañía?

Se realizará inicialmente un análisis de vulnerabilidades con un proveedor para poder determinar el grado de criticidad de inseguridad de la compañía, y partir con resultados evidentes para empezar a diseñar la propuesta de mejora (Herramientas de control y Monitoreo, Antivirus, Actualizaciones y parches de seguridad, políticas de navegación, sistema de recuperación anti-desastres). Los informes o documentación que se requiere para llevar a cabo la metodología se centrarán en los siguientes:

- Informe de Vulnerabilidades a la infraestructura local (Caja Gris)
- Inventario de equipos de cómputo y datacenter’s actualizado.
- Matriz de riesgos
- Listado de usuarios (Activos, Inactivos) con sus roles específicos
- Presupuesto de IT

Figura 4

Formato de diseño de matriz de riesgos



Toda la información recolectada es indispensable, importante, prescindible para la toma de decisiones, genera gran expectativa ya que las respuestas de estos funcionarios más los resultados de dichos informes, sirven para justificar con respaldos evidentes la propuesta de mejora a la organización. Al final se entregará un documento o informe final acompañado de un plan de trabajo o cronograma de actividades, en donde se encontrarán todas las observaciones de las revisiones anteriores, así mismo incluirá la inversión que ameritará la mejora.

1.5 Justificación.

Dado el origen del tema y socializando los procesos de seguridad actuales, que se detallaron inicialmente en este documento, la presente propuesta es importante y se justifica en los siguientes puntos:

- Existe la necesidad de cerrar las brechas de seguridad para garantizar la confidencialidad de los datos y de los sistemas de información, al no

tener controles lastimosamente está expuesta a robos o secuestro que pueden desencadenar en pérdidas económicas o reducción de ingresos considerables para la compañía en los procesos de facturación en sus EDS y TDC.

- Se requiere controlar los accesos a los sistemas de información de la compañía para evitar ingresos desconocidos o no autorizados.
- La propuesta se realiza con el propósito de controlar los equipos de cómputo de la compañía, asegurando que no se puedan ejecutar o instalar aplicaciones desconocidas a través de herramientas de monitoreo y antivirus.
- Mantener actualizados los sistemas operativos en los equipos de cómputo, a través de parches de seguridad o actualizaciones propias de los sistemas, reduciendo así vulnerabilidades que pueden desencadenar en ingresos no autorizados por ciberataques.
- Se necesita establecer procesos de recuperación anti-desastres tras posibles eventos de seguridad o de daño de hardware/software en los diferentes ambientes de la organización.

1.6 Alcance y limitaciones

Al analizar y evaluar la necesidad dentro de la propuesta de mejora, definimos el alcance del trabajo de investigación:

- Cerrar brechas de seguridad a la infraestructura local (Servidores, Host, sitios publicados, NAT’s locales).
- Implementación de consola de monitoreo de Antivirus en los equipos de cómputo y servidores.

- Control de parches de seguridad y actualizaciones automáticas en los equipos de cómputo y servidores.
- Proponer un plan de revisión de cuentas de usuarios, roles, accesos y perfiles para evitar accesos no autorizados y controlados.
- Diseñar políticas de navegación seguras en el FW, colocando roles de accesos y navegación por cargos o funciones.
- Elaborar el proceso de respaldos diarios e incrementales, incluido el plan de recuperación anti-desastres para la continuidad del negocio.

Las limitaciones o aspectos que pueden presentar un obstáculo en la propuesta de la mejora pueden ser:

- Presupuesto acortado, sin opción a la inversión mínima para la ejecución de la propuesta
- Tiempo de los recursos de IT para el acompañamiento y diseño correspondiente debido a carga operativa en los requerimientos diarios.
- Poco acceso a la información requerida para el levantamiento de datos inicial.
- Inventarios o licenciamiento de equipos desactualizado, que perjudican con estadísticas erróneas.

Con estos alcances podemos argumentar nuestro límite, no sin antes tener claro el objetivo y siendo proactivos posteriormente a las revisiones constantes de las herramientas proporcionadas para así gestionar de una forma eficiente la seguridad en la organización. Los límites pueden presentarnos obstáculos, pero debemos considerarlos desde el inicio, para informar, alertar y gestionar lo necesario.

CAPITULO II: MARCO TEÓRICO

2.1 Bases Teóricas

La infraestructura de una organización, institución o empresa constituye un valor importante para la seguridad de los datos y la informática, por ende, cada vez es más susceptible a una amplia variedad de ataques cibernéticos, con varias herramientas se puede detectar a tiempo las amenazas que acechan la seguridad e integridad de los equipos y los datos. Por este motivo, muchas entidades actualmente invierten en tecnologías o herramientas que puedan controlar y administrar la seguridad, monitoreando y siendo proactivos ante cualquier anomalía que se presente con la finalidad de garantizar la seguridad en sus sistemas de información.

En base a la información del mapa de tiempo real del sitio Cybermap de Kaspersky (https://cybermap.kaspersky.com/es/stats), se puede evidenciar que (Rusia, EEUU, Brasil, Alemania y China) son los 5 países más atacados en lo que va del 2022:

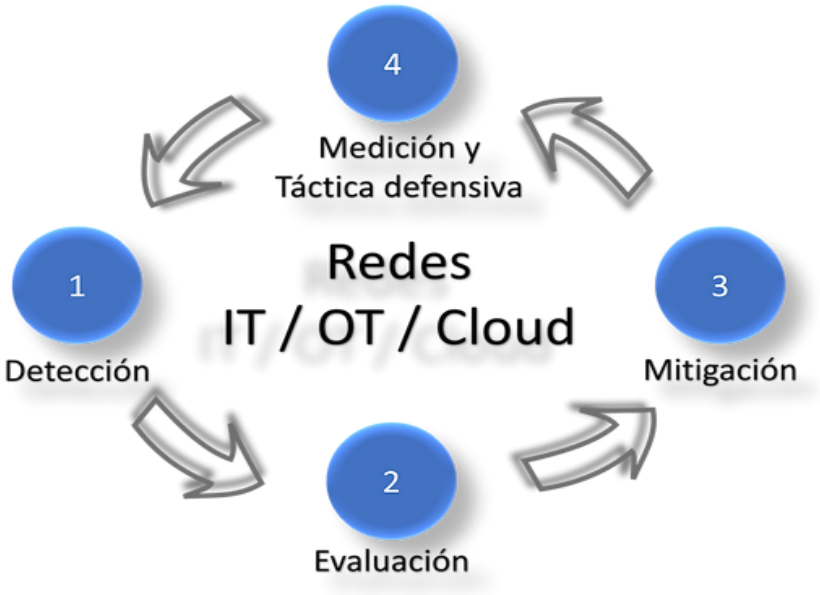
Figura 5

Mapa mundial de países más atacados del 2022, cybermap

Esto permite que en la actualidad existan grupos que se dedican al rapto de información con fines u objetivos dañinos para cualquier organización. Al realizar monitoreos en tiempo real, se puede determinar los ataques a países en consecutivo, esto genera alarmas a nivel mundial y a cada organización para empezar a desplegar planes o acciones que protejan la integridad de sus clientes y su información.

Figura 6

Plan de acción para protección de infraestructura



De acuerdo a (*David, A., Gayoso, V., & Hernández, L., 2020)* en su libro "Ciberseguridad", "Cualquier acción que comprometa alguno de los objetivos de seguridad y privacidad se considera una amenaza, mientras que una vulnerabilidad es una debilidad en el sistema que puede ser explotada por una amenaza", nos pueden determinar que es necesario realizar análisis de vulnerabilidades cada cierto tiempo con el afán de que estas no se consideren una amenaza posteriormente y que se puedan mitigar y así evitar desastres posteriormente; las brechas de seguridad

pueden existir al desplegar un proyecto sin revisar detalles como Bases de Datos, puertos locales, la publicación de un Website, la habilitación de un puerto en el firewall, la desactualización de Firmware, desactualización de sistema operativo, parches de seguridad en servidores, aplicaciones de orígenes desconocidos, hasta en los mismos dispositivos smartphones que se conecten a la misma red en donde se encuentra la infraestructura local, etc. Son detalles que muchas veces no se consideran y que generan brechas de seguridad que pueden llevar a expandir una amenaza en la organización.

En la certificación *(Norma ISO, 27000)*, la seguridad de información es la protección de datos en un amplio rango de amenazas con el fin de asegurar y garantizar la continuidad del negocio, minimizando el riesgo comercial y maximizando el retorno de las inversiones para las oportunidades comerciales; esto solo se puede lograr implementando un adecuado conjunto de controles, políticas, procedimientos, procesos funcionalidades de sistemas, y estructuras organizacionales. Para así poder garantizar la operatividad o manejar sistemas de contingencia que permitan sostener los procesos operativos.

Figura 7

Análisis del riesgo en las arquitecturas de sistemas

Vale mencionar que los controles no garantizan que se pueda evitar por completo un ataque cibernético, pero minimiza el impacto al momento de ser proactivos y preventivos ante situaciones que puedan salirse de control. El objetivo es plasmar los controles, cerrar brechas de vulnerabilidad, generar procesos de identificación de amenazas o riesgos, minimizar el impacto, mantener planes de contingencia y recuperarse de cualquier incidente en el menor tiempo posible.

En cambio, al hablar de términos de seguridad, para *(Aguilera, 2011)*, la seguridad informática se la define como la disciplina encargada de plantear y diseñar las normas, procedimientos, métodos y técnicas con el fin de obtener que un sistema de información sea seguro, confiable y sobre todo que tenga disponibilidad. Si evaluamos este concepto, en comparación de la Certificación ISO, el objetivo es precautelar y garantizar la disponibilidad de los diferentes servicios o sistemas de información a los usuarios o personas, teniendo en cuenta el punto de vista de algo ya implementado y controlado.

Una evaluación de la seguridad informática se puede caracterizar como aquel proceso cuyo fin principal es determinar si el objetivo de la evaluación ya sea éste un host en una red, un sistema de información, una base de datos, una red, un procedimiento, o inclusive un individuo, satisface determinados objetivos de seguridad establecidos previamente o definidos por las buenas prácticas y estándares de la industria *(Tejada, 2015)*. Podemos mencionar también en una definición más exhaustiva con respecto a la evaluación de seguridad, que la misma puede ser conducida desde afuera del perímetro de la seguridad de la organización. Ya que esto ofrece la posibilidad de entender cómo el sistema de seguridad de la organización

puede ser percibida por una visión externa a la misma, por ejemplo, cómo se ve desde internet.

Este punto es muy importante ya que no solo se define la evaluación de la seguridad, sino que nos permite estar en una posición la cual nos puede servir para conocer cómo se ve desde afuera de nuestra infraestructura y porqué no tratar de explotarla para poner a prueba nuestro nivel de estabilidad y de rigurosidad frente a ataques informáticos.

Al considerar el avance tecnológico a nivel mundial, la sociedad se vuelve más digital, pero se debe considerar al mismo tiempo evaluar los riesgos que puedan aparecer al momento de estar más conectados a mayor alcance, por esto nos comparte *(Solarte, F., Enriquez Rosero, E., & Benavides, M. 2015),* dado que el avance hacia una sociedad más digitalizada e hiperconectada en donde las empresas cada vez hacen un uso más exhaustivo de las Tecnologías de información y Comunicación, se hace necesario evaluar la seguridad de los sistemas de información de forma integral como parte de una cultura organizacional.

Según los resultados mencionados por el proveedor TELCONET LATAM en su primer reporte de tráfico malicioso a sus clientes en Ecuador (https://telconet.net/traficomalicioso), los datos proporcionados por NETSCOUT en el año 2021 para Ecuador, indican que se mantuvo un registro de 68.700 ataques cibernéticos, y durante los últimos 3 meses hubo un incremento de aproximadamente 7 veces más que los meses anteriores. Esto origina que se tomen medidas de controles extremas para contrarrestar posibles ataques, así prevenir incidentes de

seguridad que puedan ocasionar pérdidas corporativas o en gran escala de forma masiva considerando que existen muchos proveedores que mantienen relaciones comerciales con varias organizaciones.

En el libro “Seguridad de la información, redes, informática y sistemas de información”, *(Aretto, 2008)*, afirma que un área de especialización de seguridad es la de Seguridad física, la misma que debe velar por los accesos a los sistemas solo a quienes lo necesitan y están autorizados; el control de accesos es muy importante para mitigar accesos no autorizados, manteniendo un proceso de habilitar/deshabilitar usuarios en el tiempo adecuado, dentro de estas aplicaciones puede ingresar un usuario de acceso VPN (Virtual Protocol Network) el cual es muy importante, puesto que al dejar un usuario VPN habilitado y que ya no usa, puede ser una brecha de vulnerabilidad muy alta.

Muchas Herramientas como Crowdstrike, Qualys, Cyberack, Fortinet y otras, pueden otorgar seguridad a nivel organizacional, brindando un control a usuarios y a los sistemas de información que se mantienen a nivel corporativo. Dentro de sus alcances podemos encontrar monitoreos online en los equipos de usuarios con respecto a direccionamiento de enlaces url’s no permitidos, ejecución de programas o contenido dañino, uso inusual de credenciales que pueden desencadenar en suplantación de identidad, apertura de archivos con extensiones extrañas, conexión de dispositivos o accesorios no identificados o aprobados por las áreas de IT, etc.

El propio gigante de la informática Microsoft, en la actualidad brinda seguridad en sus plataformas, con su herramienta MFA (Multi-Factor Authentication) agregando así una capa de protección en los inicios de sesión en sus plataformas o herramientas,

permitiendo satisfacer las necesidades de protección de la organización y sus usuarios. Esta herramienta permite el ingreso con un código de verificación que llega como mensaje de texto al celular registrado, huella o acceso desde el aplicativo en Android o iOS.

Figura 8

Esquema de doble factor de autenticación de Microsoft, MFA

Para *(Martinez, 2015)*, en su libro Planes de Contingencia, se debe considerar un plan de continuidad de negocio como un proyecto de toda organización dentro de la seguridad de los datos y acciones preestablecidas dentro de la operatividad, con un líder de proyecto y sus aliados que establezcan procedimientos anti-desastres o planes de ejecución tras algún evento de seguridad para precautelar a los sistemas de información y los procesos organizacionales, esto se determina posteriormente a un análisis de riesgos y un análisis de impacto como medida de protección en caso de problemas de seguridad a nivel corporativo.

Al hablar seguridad muchas veces lo primero que se nos acerca a la realidad son los virus informáticos, estos conceptos que muchas veces los nombramos a diario, pero que posiblemente no identificamos tipos o funcionalidad que mantienen. *(Vieites, 2013)*, menciona que se define a un virus informático como un programa desarrollado

en un determinado lenguaje de programación (C++, ensamblador, etc.) con el objetivo de infectar a uno o varios sistemas informáticos, usando varios mecanismos de propagación o auto replicación, el cual trata de producirse de forma acelerada para extender su alcance.

Virus es un código malicioso incrustado en el código normal de un programa anfitrión. El virus se propaga de un ordenador a otro, pero para ello necesita la intervención humana. Puede afectar el funcionamiento del software, hardware y las propiedades de la información y causar un impacto desde leve a muy grave sobre su objetivo *(Lopez, P. & Valencia, H. 2017).*

Al evaluar los conceptos de virus, podremos argumentar que los mismos podemos encontrarlos y ejecutarlos sin conocimiento, estos muchas veces son punto flojo en personas sin una base informática o desconocimiento de lo que pueda tener un programa descargado gratuito o parches que puedan servir para activar algún programa con licenciamiento free. Es recomendable trabajar mucho dentro de las organizaciones con los usuarios para volverlos un poco más activos ante este tipo de escenarios que pueden terminar en incidentes de seguridad.

Las medidas de seguridad o gestión de seguridad en muchas compañías actualmente ha evolucionado y se ha convertido en política interna, han nacido áreas de ciberseguridad y seguridad lógica, las mismas que sirven para colocar controles, supervisar y velar por los ingresos de los usuarios a los sistemas de información; agentes de seguridad o ingenieros de seguridad deben realizar planes de evolución para los usuarios que necesitan acompañamiento o reforzar medidas de control y así

evitar ser víctimas de fraudes o rapto de credenciales de acceso. Uno de los errores más comunes y que sirven para que piratas cibernéticos realicen suplantación de identidad, es que muchas personas asocian sus correos corporativos en cuentas de redes sociales o sitios de publicidad, en donde no se mantiene privacidad y que puede ser perjudicial para la compañía u organización.

Como análisis final dentro de las bases teóricas, existen puntos claves para mantener y garantizar la seguridad dentro de las compañías (Controles, Monitoreos y mejora en los procesos de accesos a la información), debe ser clave para asegurar la continuidad operativa y no sufrir posteriormente de ataques cibernéticos que pueden perjudicar severamente a los procesos de facturación y operatividad.

CAPITULO III: MARCO REFENCIAL

La estructura y jerarquía de una organización, institución o empresa es la base fundamental de su negocio, se enfoca en brindar toda la información correspondiente a su actividad y su giro de negocio, su plan actual de estabilidad y a donde se pretende llegar con su visión, por este motivo se procede a detallar todos estos aspectos importantes de la entidad ADESGAE CÍA LTDA (Administración estratégica de gasolineras del Ecuador Cía Ltda).

3.1 Su historia

Su sede principal, fue creada el 17 de Julio del 2015 de la mano del Gerente General, de la compañía Lutexsa Cía Ltda, Fabio Castro, la constituyó con el objeto de llevar a cabo el negocio minorista en el país; en especial a la operación de Estaciones de Servicio y tiendas de conveniencia, ajustando así el modelo de Terpel en el Ecuador. Se realizó una inversión de USD $9.999 que corresponde al noventa y nueve, coma nueve por ciento (99,9%) de participación en dicha sociedad.

ADESGAE nació con la finalidad de ser la operadora directa de LUTEXSA INDUSTRIAL COMERCIAL CÍA LTDA, esto definiría que se administre la cadena de gasolineras propias de la marca Terpel. Iniciando la operación en la ciudad de Guayaquil de una estación de servicio (EDS) en el año 2015 específicamente en la EDS GARITA CHIMBORAZO (Ubicada en la Av. Primero de Mayo y Av. Quito), ADESGAE empezó su crecimiento en torno a la toma de operaciones directas; para finales del 2018 ya mantenía en operación a 4 EDS (GARITA CHIMBORAZO, TRUCKSTOP, AUTOSUR, R&G) ubicada en Guayaquil, Quito y Santo Domingo; Adicionalmente realizó la vinculación de su primera tienda de conveniencia (TDC) en la ciudad de Quito (TDC TERPEL 1) . A mediados del 2019 se inicia un proyecto de

crecimiento, se vinculan recursos de diferentes áreas como (Administración, Operaciones, GGHH, Sistemas, etc); para poder abarcar el crecimiento que se tenía planificado de una forma más organizada, teniendo el objetivo claro de llegar a ser la operadora directa número 1 a nivel nacional de Terpel Ecuador.

Figura 9

Primera operación directa ADESGAE (Eds Autosur)

Así empezó el proyecto “Pegasus” el que se planificó con todas las áreas involucradas para dar los resultados que se esperaban de parte de los directivos y altos mandos; actualmente en menos de 3 años ADESGAE mantiene una operación directa de 43 establecimientos (29 EDS y 14 TDC), siendo este un camino inicial fomentando el crecimiento operacional de la mano de diferentes áreas, en busca de un objetivo en común, manteniendo el valor del servicio como principal base para buscar fidelización de clientes y permitir generar plazas de trabajos a nivel nacional.

Vale mencionar que la organización Padre (Terpel Comercial Ecuador) maneja la administración y control de varias áreas de gestión para Adesgae, permitiendo así se cumplan los estándares organizacionales.

Figura 10

Imagen actual de gasolineras Terpel (Edc y Tdc Terpel 1), 2022

3.2 Misión

Generar experiencias memorables a nuestros clientes en todas nuestras líneas de negocio, permitiendo acaparar el mercado y siendo permanentes en el servicio de nuestros establecimientos.

3.3 Visión

Ser el aliado estratégico para el servicio al cliente #1 en el corazón de nuestros consumidores.

3.4 Valores

- Actuar con integridad
- Respeto
- Trabajo en equipo
- Perspectiva a largo plazo
- Inspirar a otros con el ejemplo

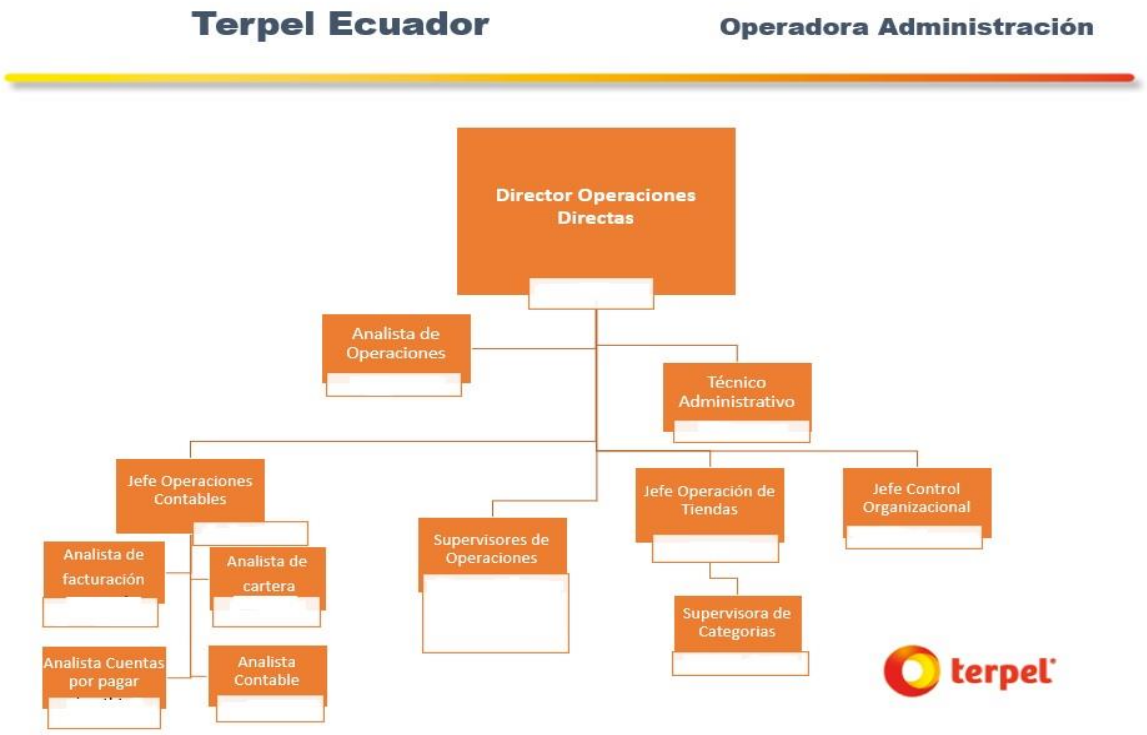
- Satisfacción al cliente
- Coherencia entre lo que se dice y se hace
- Comunicación fluida y abierta
- Crecimiento de la organización

3.5 Organigrama

En este espacio adjuntamos la jerarquía o estructura organizacional de la compañía ADESGAE, la misma cuenta con áreas básicas netamente operativas, puesto que las áreas de la compañía TERPEL COMERCIAL ECUADOR CÍA LTDA gestiona sus procesos a nivel de (Sistemas, GGHH, Dirección y Mercadeo):

Figura 11

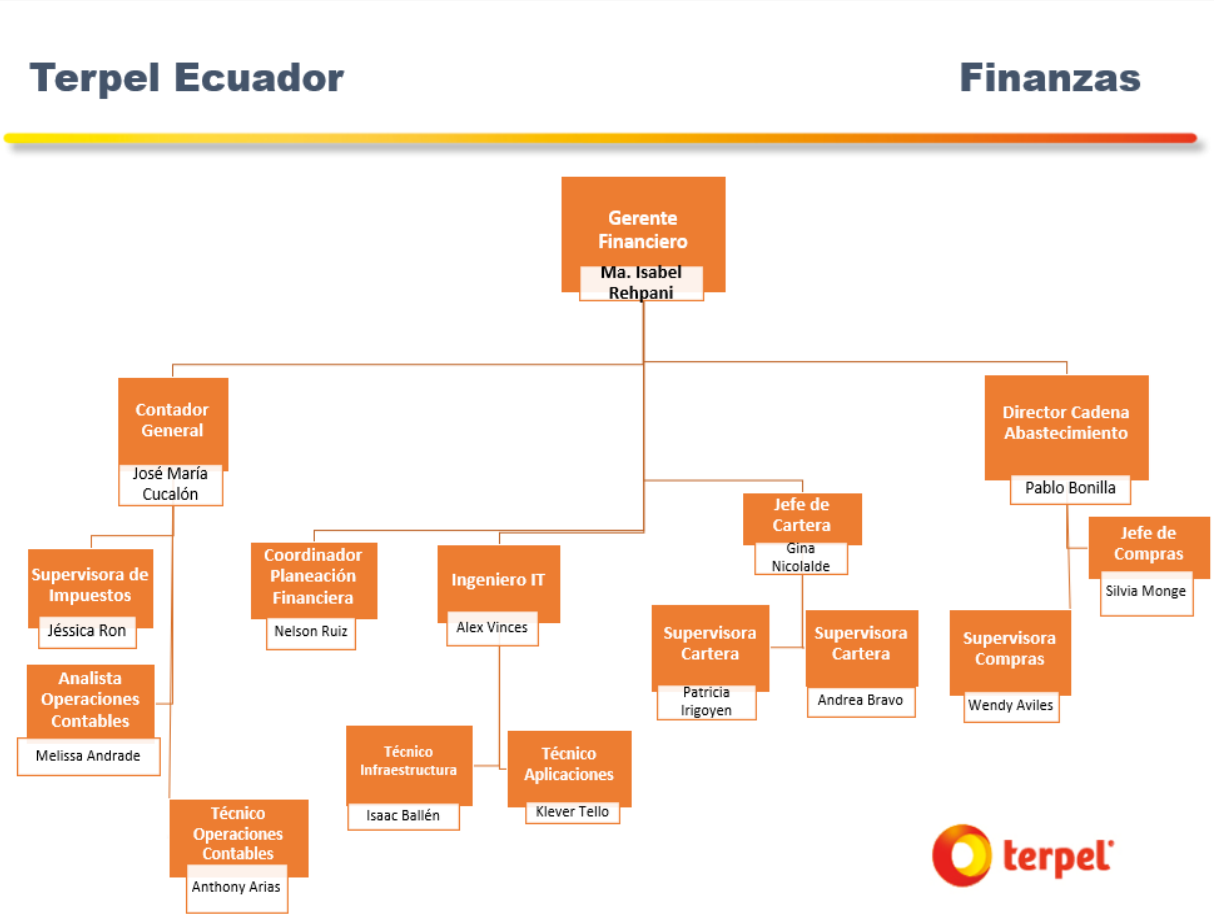
Organigrama operador ADESGAE CÍA LTDA, 2022



Se brinda mayor detalle de los cargos que involucrarán la propuesta de mejora, por ejemplo el departamento de Sistemas es de la Sociedad Terpel Comercial Ecuador, quienes manejan la administración y gestión de procesos de IT de la operadora, el mismo pasó por una restructuración recientemente y se emite el organigrama del departamento de Sistemas:

Figura 12

Organigrama Comercializador TERPEL ECUADOR CÍA LTDA, 2022



Funciones Técnico de Infraestructura

- Administrar las redes y comunicaciones de la organización.
- Análisis, control y establecimiento de nuevos segmentos de redes para nuevos puntos.
- Definición de nuevas arquitecturas de nuevos puntos de establecimiento.
- Coordinación con proveedor de Comunicaciones nuevos puntos de enlaces e internet.
- Monitoreo de redes (Enlace/Internet/Wifi) de todos los puntos (TERPEL – ADESGAE).
- Evaluar, diagnosticar y solucionar problemas con las redes e infraestructura.
- Coordinar mantenimientos preventivos y correctivos con proveedores.
- Velar por el funcionamiento de Servidores y Herramientas de respaldos.
- Capacidad de análisis y procesamiento crítico sobre métodos Anti-desastres.
- Control de Inventarios de activos fijos.
- Gestión documental (formatos y procedimientos).
- Administración de Data Center.
- Administración de Servidores (DNS, DHCP, ACTIVE DIRECTORY).
- Administración de controlador firewall y accesos de internet.
- Garantizar la continuidad del negocio con métodos de contingencia.
- Soporte remoto y telefónico con usuarios nivel 2.
- Coordinar con proveedores la implementación de los sistemas CCTV de los puntos.
- Administrar seguridad perimetral y control de filtrado web en los equipos de la organización y operación.
- Actualizar y estudiar metodologías nuevas para arquitecturas óptimas

Funciones Técnico de Soporte

- Soporte técnico de primer nivel a EDS y TDC.
- Administración de ticket’s y mesa de ayuda.
- Responder a salidas en vivo de Operación EDS y TDC.
- Control de Inventarios y Licenciamiento de TDC y EDS.
- Validación de configuraciones de equipos de cómputo TDC y EDS.
- Administración de aplicaciones en equipos de cómputo TDC y EDS.
- Revisión de equipos, elaboración de informes técnicos y gestión de garantías.
- Gestión de baja de activos y reemplazo de equipos.
- Gestión de nuevos requerimientos para garantizar la operación.
- Servicio al usuario y proveedores finales
- Gestión de cuentas de usuario y correos electrónicos.
- Control documental (Formatos, Procedimientos, Actas de asignación, etc.).
- Garantizar la operación de los sistemas de facturación.
- Responder de manera oportuna sobre incidentes y requerimientos solicitados por Administradores.
- Velar por el correcto funcionamiento del sistema CCTV de todos los puntos.
- Ejecutar trabajos programados (Supervisión de actividades con proveedores) cableado, eléctrico UPS, Controladora de dispensadores, etc.
- Coordinar con proveedores los accesos para soportes externos.

Funciones Técnico de Aplicaciones

- Control de bases de datos de sistemas de facturación de EDS y TDC.
- Desarrollo y análisis de nuevas plataformas o aplicaciones.
- Capacitaciones de Sistemas a Administradores de EDS y TDC.

- Gestión de nuevas implementaciones de sistemas de facturación.
- Validación de nuevas aplicaciones para actualización y agilidad de procesos de facturación.
- Seguimientos de casos A1clic (Aplicaciones).
- Soporte primer y segundo nivel aplicaciones (Sistemas Zencillo – RP3).
- Control de licenciamiento de aplicaciones (Ofimática, Office 365, Microsoft Teams, SAP, Correo).
- Control de accesos aplicaciones locales (Cuentas sistemas Zencillo, RP3, Control de Acceso)
- Garantizar cuentas de control de servidores y administraciones sistemas varios.
- Garantizar funcionamiento de herramienta de Inventario de equipos.
- Gestión documental (Manuales técnicos, Manuales de usuarios, procesos IT, etc.).
- Aplicar políticas de respaldos (plan de recuperación y producción)
- Servicio al usuario y proveedores finales Aplicaciones.

3.6 Productos y Servicios

ADESGAE CÍA LTDA se especializa en ser una compañía de venta minorista, pero con crecimiento rotundo, el mismo que desde su constitución han crecido también sus productos y servicio, se manejan en el siguiente detalle:

- Venta al por menor de combustibles para vehículos automotores y Motocicletas en establecimientos especializados.
- Venta al por mayor de combustibles líquidos nafta, gasolina, biocombustible incluye grasas, lubricantes y aceites.
- Venta al por menor de gran variedad de productos en tiendas, entre los que

predominan, los productos alimenticios, las bebidas o el tabaco, como productos de primera necesidad y varios otros tipos de productos.

- Administración de bienes inmuebles a cambio de una retribución o por contrato.
- Venta al por menor de gran variedad de productos en supermercados, entre los que predominan, los productos alimenticios, las bebidas o el tabaco, como productos de primera necesidad y varios otros tipos de productos, como prendas de vestir, muebles, aparatos, artículos de ferretería, cosméticos, etc.
- Venta de comidas y bebidas en cafeterías, incluso para llevar.

3.7 Análisis de la Gestión Empresarial

Una vez realizado todo el esquema organizacional de la compañía ADESGAE, procedemos a realizar el diagnóstico de la situación empresarial a través de una herramienta muy conocida como es el FODA:

Figura 13

Análisis foda ADESGAE CIA. LTDA.

Como explicación al análisis realizado, ADESGAE CÍA TLDA, maneja un escenario muy bueno en Fortalezas, el mismo al ser Operador directo de Terpel Ecuador, maneja un presupuesto de inversiones un poco más amplio, lo que sirve para solventar avances y aperturas de nuevos establecimientos, mantiene apoyo con áreas de gestión integrada a nivel corporativo lo que hace que pueda mantener estándares multinacionales. Del mismo modo ayuda al tener varios puntos o establecimientos en proceso de crecimiento esto ayuda para establecer la fidelización de clientes a nivel Nacional.

Mantiene enfoque de oportunidades muy interesantes porque puede brindar espacios a otros negocios complementarios como por ejemplo hacer alianzas con

otros modelos de negocios como cadenas de farmacias, panaderías, pastelerías, etc. Incentivando la inversión local. Otra oportunidad es que al tener puntos a nivel Nacional su cadena de establecimientos puede crecer en ciudades en donde ya se encuentra alojada la marca Terpel. siendo este un plus, del mismo modo permite nuevos modelos de servicio con el área de Tecnología, lo que ayuda a la innovación digital.

Entre sus debilidades resaltan que pueden tener costos más altos en comparación a cadenas más grandes o con mayor rotación de productos y de marcas conocidas, lo que genera una debilidad en sus ventas, del mismo modo al ser el descendente de la comercializadora, se debe ajustar a los tiempos de respuesta por procesos internos de Terpel Comercial Ecuador.

Sus amenazas recaen en que se puede tomar una operación de algún propietario que mantenga problemas ambientales en su EDS y puede presentar problemas legales; entre otros puntos, puede verse no beneficiado con negocios nuevos al no realizar un estudio de mercado en los lugares de apertura nuevos.

CAPITULO IV: RESULTADOS

4.1 Diagnóstico

Dentro del presente trabajo de investigación, se determinaron puntos importantes de acuerdo con el alcance de la propuesta, los mismos que definimos como hallazgos y son necesarios mitigarlos. Como punto inicial tras la recopilación y levantamiento de información exponemos que el problema apareció debido a la poca inversión de recursos humanos, financieros y posiblemente por la poca facilidad de justificar herramientas de seguridad dentro de los procesos tecnológicos. Esto produce un fuerte desbalance a nivel corporativo y tecnológico.

Determina niveles de seguridad crítica muy altos con falencias considerables dentro de la organización, es fundamental realizar el proceso de implementación de la propuesta para ser proactivos y evitar lamentarse posteriormente ante eventos de ataques cibernéticos. Una vez analizados los procesos actuales se detallan los hallazgos y se los define como los puntos relevantes dentro del diagnóstico de la propuesta:

1.- Analizar las brechas de seguridad en la infraestructura de la compañía, a través del levantamiento de información, análisis forense y pentesting, con aquello cerraremos las brechas de seguridad que existen en la LAN y se procederá a sellar las vulnerabilidades en los sistemas de información de la Organización, ya que no se ha realizado un análisis de vulnerabilidades en la infraestructura local. Actualmente no existe proceso.

2.- Diseñar herramientas de control, accesos, auditoría y de monitoreo con la finalidad de velar y garantizar la operación a través de las conexiones DNS's, control

antivirus en los endpoints con la finalidad de evaluar el comportamiento de las aplicaciones y equipos de la organización. Las mismas responden a Aplicativos (Open DNS Lumu, Antivirus Falcon, y analizador de vulnerabilidades Qualys). Con esto aplicaremos controles de navegación, seguridad en los equipos de usuarios y monitoreo a donde se realizan peticiones salientes. Actualmente mantienen acceso libre a internet y sin aplicativos de antivirus.

3.- Al Proponer actualizaciones y migraciones de las versiones de sistemas operativos en Servidores y PC's. Los estaremos estandarizando, ya que los mismos actualmente mantienen versiones antiguas como (Windows Server 2008, Windows 7 Profesional). Con este plan cumplimos con actualizaciones de seguridad y parches del fabricante para tener el soporte correspondiente dentro de las versiones actualizadas. Actualmente existe el siguiente detalle:

Tabla 1

Listado de Infraestructura para Presupuestar Licenciamiento

Cantidad	Detalle
15	Servidores locales (Windows Servers 2008)
28	Servidores Locales (Windows Server 2019 STD)
95	Puntos de Venta (Windows 10 Pro)
35	Puntos de Venta (Windows 7 Profesional - Windows 8 Home)
34	Equipos de Administradores (Windows 10 Pro)
9	Equipos de Administradores (Windows 7 Profesional)

4.- Con el objetivo de actualizar o revisar políticas de navegación y seguridad perimetral de Firewall, se pretende del mismo modo validar accesos y usuarios VPN, creando roles y perfiles de navegación para los usuarios, así poder evitar accesos a sitios no seguros o descargas y ejecuciones de software malicioso que pueda

comprometer seriamente a la compañía. Actualmente no se maneja un Firewall ni políticas, se define el proceso y la mejora a través de la propuesta.

5.- Al definir procesos de recuperación anti-desastres en los servidores de BD, establecemos las herramientas que necesitaremos para licenciamiento y Servidores adicionales, ya que actualmente se encuentran con un Servidor local y si se presenta algún incidente con alguno de ellos se coloca un Servidor de Backup que se encuentra por casa ciudad, el mismo se levanta como backup, se montan las BD's y todo el ambiente del Sistema de Facturación. Actualmente existe un procedimiento el cual consta del siguiente detalle pero no se encuentra oficializado.

4.2 Propuesta de Mejora

Dentro del marco de la investigación se plantea el esquema de correcciones de los hallazgos en un plan de trabajo, validando y considerando puntos relevantes como (recursos, presupuestos, activos, procesos y procedimientos) que servirán al departamento de Tecnología para organizar de mejor manera los procesos de seguridad dentro de la organización y al mismo tiempo controlar de forma eficiente los equipos de los usuarios finales a través de las siguientes herramientas:

1-. Análisis de Vulnerabilidades.

2.- Diseño y propuesta de implementación de herramientas de controles.

3.- Aplicar actualizaciones y migraciones de versión de Sistemas Operativos

4.- Actualizar seguridad perimetral y aplicar políticas de seguridad

5.- Definición y mejora del plan anti-desastres.

Una vez definidos los puntos en donde se trabajará para la propuesta de mejora, emitiremos la inversión presupuestaria que buscamos por cada uno en

referencia a su costo y tiempo de implementación, con el proveedor o proveedores que se requieran en el proceso presupuestal:

1.- Se procederá a solicitar el requerimiento oficial de análisis de vulnerabilidades a 4 Servidores locales que mantienen el CRM de los sistemas de Información de las EDS y TDC, los mismos que se consideran y se detallan como:

Tabla 2

Listado de Ambientes para Realizar Análisis

No	Servidor
1	Servidor Consolidador de Información
1	Servidor Base de Datos CRM Tienda
1	Servidor Base de Datos CRM Estación
1	Servidor Facturación Electrónica

El objetivo del servicio de Análisis de Vulnerabilidades es identificar, clasificar y priorizar las vulnerabilidades inherentes en los dispositivos o recursos informáticos que pueden constituir un riesgo de seguridad para la infraestructura tecnológica de ADESGAE; además evaluar mediante Ingeniería Social al personal TI. Para realizar esta labor se aplican metodologías y técnicas usadas por especialistas de seguridad desde diferentes perspectivas, intereses, equipos y tecnologías y así evaluar los dispositivos o recursos informáticos presentes en la infraestructura de ADESGAE y en base a los resultados de esta evaluación, ADESGAE pueda aplicar las mejores prácticas de seguridad informática y en caso de ser necesario realizar los correctivos adecuados para cumplir con los pilares fundamentales de la Gestión de la Seguridad de la Información.

El alcance de la propuesta es mantener una visión holística de que tan expuesta está la infraestructura a evaluar, basado en el escaneo de vulnerabilidades y análisis de estas. El servicio está formado por los siguientes componentes de evaluación:

• **Internal Vulnerability Assessment**

Los componentes del servicio poseen diferentes alcances y objetivos, sin embargo, todos están enfocados en contribuir con la mejora continua de los niveles de disponibilidad, integridad y confidencialidad de los activos de información de la organización. Para la ejecución de este proyecto se aplicarán metodologías y técnicas usadas por evaluadores para obtener los siguientes resultados:

- Proveer una visión del nivel de seguridad informática basado en la evaluación realizada.
- Permitir a ADESGAE conocer los factores de riesgo específicos que lo puedan dejar vulnerables a posibles ataques internos y externos, en base al análisis de las vulnerabilidades escaneadas.
- Medir el grado de vulnerabilidad asociado al personal mediante una evaluación de Ingeniería Social.
- En base a los resultados del servicio contar con las recomendaciones generales y específicas que ayuden a la implementación de mecanismos y mejores prácticas de seguridad informática y de la información aportando positivamente en el proceso de mejora continua de ADESGAE y protección de activos de información claves en los procesos de negocio.

Una vez determinados los alcances y los objetivos de la propuesta del análisis de vulnerabilidades se emite el costo que tendría la actividad para la organización ADESGAE.

Tabla 3

Presupuesto de Análisis de Vulnerabilidades Servidores Producción

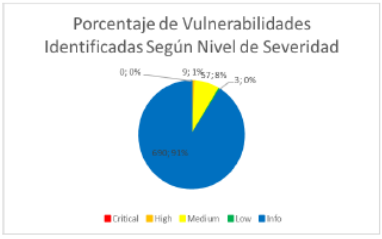
No	Servidor	Costo
1	Servidor Consolidador de Información	$450
1	Servidor Base de Datos CRM Tienda	$450
1	Servidor Base de Datos CRM Estación	$450
1	Servidor Facturación Electrónica	$450
	Total	**$1.800**

La actividad emite un resultado coherente y justificable en severidad media, según el siguiente detalle otorgado y facilitado por el proveedor, en donde se pueden evidenciar brechas de seguridad, pero que se pueden solventar con las correcciones necesarias dentro de la infraestructura tecnológica y en los equipos que mantienen los ambientes de Bases de Datos y sistemas de información. El reporte a profundidad se adjunta en el anexo. (Anexo 01).

Figura 14

Porcentaje de vulnerabilidades y niveles de seguridad

- Número de host analizados: 4.
- Vulnerabilidades altas: 9.



Vulnerabilidades identificadas por sistema

N	IP	Critical	High	Medium	Low	Info
1	192.168.109.21	0	2	14	0	118
2	10.231.111.2	0	2	14	0	306
3	10.231.111.3	0	2	13	3	129
4	10.231.111.4	0	3	16	0	137

2.- Es necesario considerar los detalles relevantes en cuanto a seguridad en equipos de usuarios finales, por este motivo se toma como uno de los puntos importantes reforzar la seguridad y control de las actividades que se realizan en los equipos de cómputo asignados a los usuarios, los mismos que deben mantener aplicaciones que minimicen o monitoreen estos registros o acciones. Para aquello dentro de la propuesta de mejora se ha considerado la validación de diseñar la posible implementación de herramientas de control como (Open DNS, Qualys, Crowstrike Falcon), de los cuales se brinda más información a continuación:

Open DNS (Lumu).- Se proporcionará mediante **Cloud base Security Infrastructure**; a través del monitoreo continuo del uso de internet, por tal motivo el Centro de Operaciones responsable, es pionero en la prestación de protección web, lo que le permite superar los riesgos para la privacidad de los usuario, la seguridad, y el cumplimiento normativo y de esta forma obtener mejores resultados de negocio. Utilizando los procesos, tecnologías y personas que el centro de operaciones definido para la prestación de este servicio, se rompe el paradigma de “protegemos todo el

ciclo de vida de los datos en el vector web", puesto que para ello la prevención de amenazas enfocadas en la internet es una prioridad.

La herramienta entrega una plataforma multicapa de seguridad como un servicio desde la nube, eliminando el coste y la complejidad de los métodos tradicionales de pasarela de protección Web o appliances. Moviendo la seguridad a una nube distribuida a nivel mundial, la puerta de enlace de Internet al usuario es un sistema que incrementa la experiencia dado que aumenta la rápida navegación. Y de esta forma las organizaciones pueden escalar fácilmente la protección a todas las oficinas o usuarios, minimizando la infraestructura a utilizar. Como capa adicional de seguridad del servicio de Navegación segura se cuenta con un nivel de protección en la capa de DNS; a través del monitoreo continuo de las consultas que se realicen a los DNS, esto claro está como propósito principal la detección de malware interno que pone en riesgo la reputación de la empresa. Mediante el uso de herramientas multiplataforma y la correlación de eventos se entrega al cliente un entorno donde puede identificar rápidamente las estaciones de trabajo comprometidas y cuál es su implicación; de igual forma encontrará menos falsos positivos de inundación a DNS por querys.

Tras la implementación de la herramienta, se puede validar los sitios y registros DNS's correspondientes visitados desde los equipos de los usuarios, para poder revisar, monitorear y alertar cualquier circunstancia fuera de lo normal según la consola de Administración del aplicativo:

Figura 15

Actividad en tiempo real de sitios visitados por usuarios

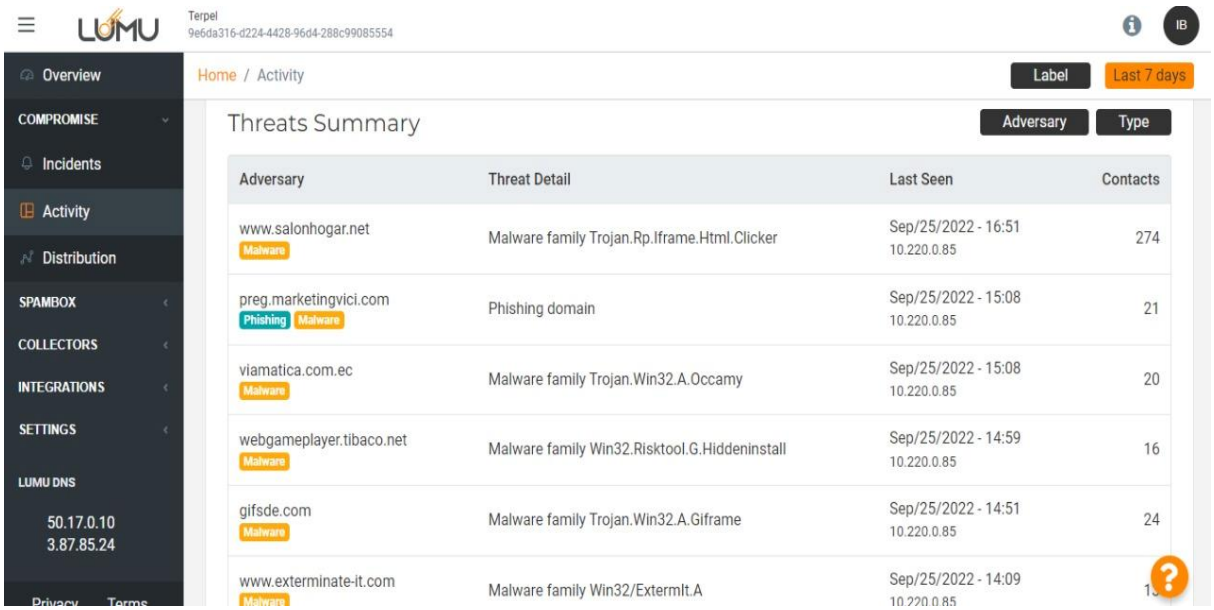
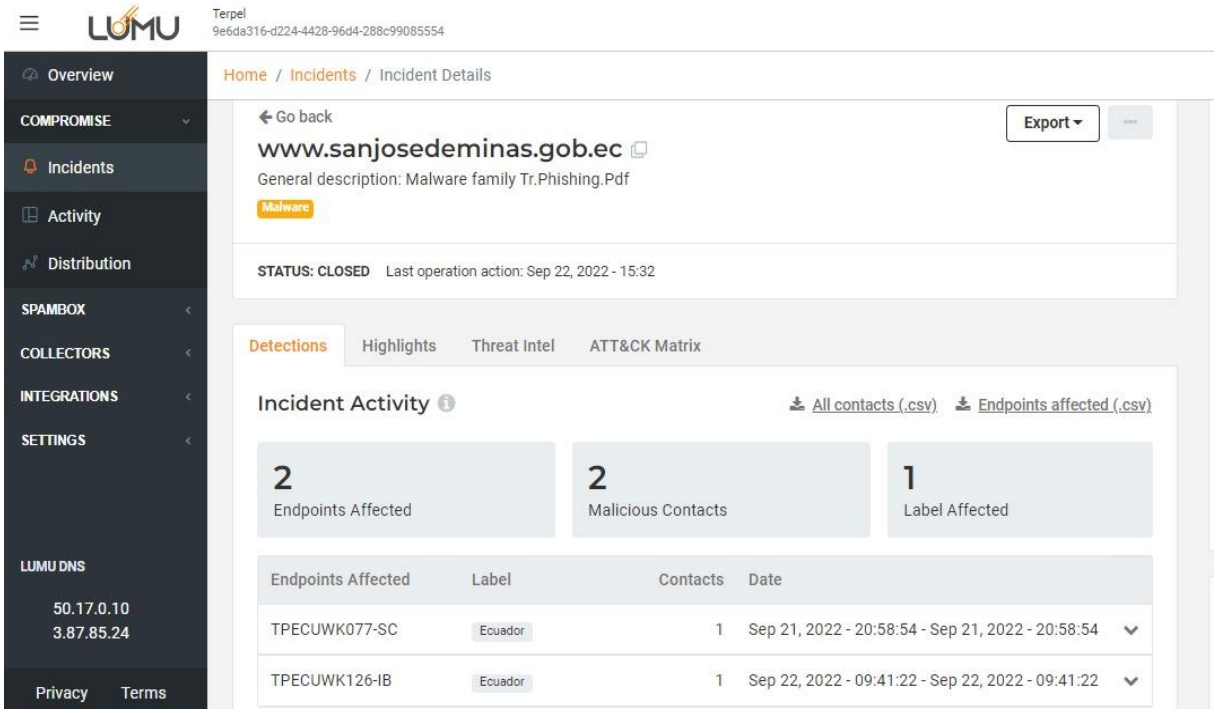


Figura 16

Incidentes registrados de equipos de usuarios



Qualys.- La Plataforma Cloud de Qualys y su conjunto integrado de soluciones ayudan a las empresas a simplificar las operaciones de seguridad y a reducir el costo del cumplimiento; esto ofrece inteligencia de seguridad crítica a la demanda y automatiza todo el espectro de auditoría, cumplimiento y protección de sistemas de TI y de aplicaciones web. Proporciona un ciclo de protección continuo desde un único panel de control, con flujos de trabajo de orquestación integrados y detección de vulnerabilidades en tiempo real, con el fin de priorizar, remediar y auditar en entornos de TI híbridos; es un paso hacia adelante de gigante, que ayudará a las organizaciones de todos los tamaños a fortalecer su postura de seguridad, al ofrecer un flujo de trabajo completo de gestión de vulnerabilidades que:

- Posibilita la gestión de vulnerabilidades y ofrece a los equipos de TI una visibilidad completa y continua de sus activos de TI globales (conocidos y desconocidos).
- Identifica vulnerabilidades en todos los activos en tiempo real.
- Prioriza la remediación mediante aprendizaje automático y conciencia de contexto.
- Proporciona flujos de trabajo de orquestación integrados.
- Permite la remediación mediante un click con rastreo completo para auditorías

Tras la implementación de la herramienta indicada, se puede evidenciar las posibles falencias o vulnerabilidades tanto en software como en aplicativos del propio sistema operativo, para poder revisar, monitorear y alertar cualquier anomalía, se pueden realizar parametrizaciones con TAGS (Grupo de equipos para aplicación de políticas) dentro de la consola de administración con dicho agente de seguridad:

Figura 17

Registros de vulnerabilidades de equipos de usuarios

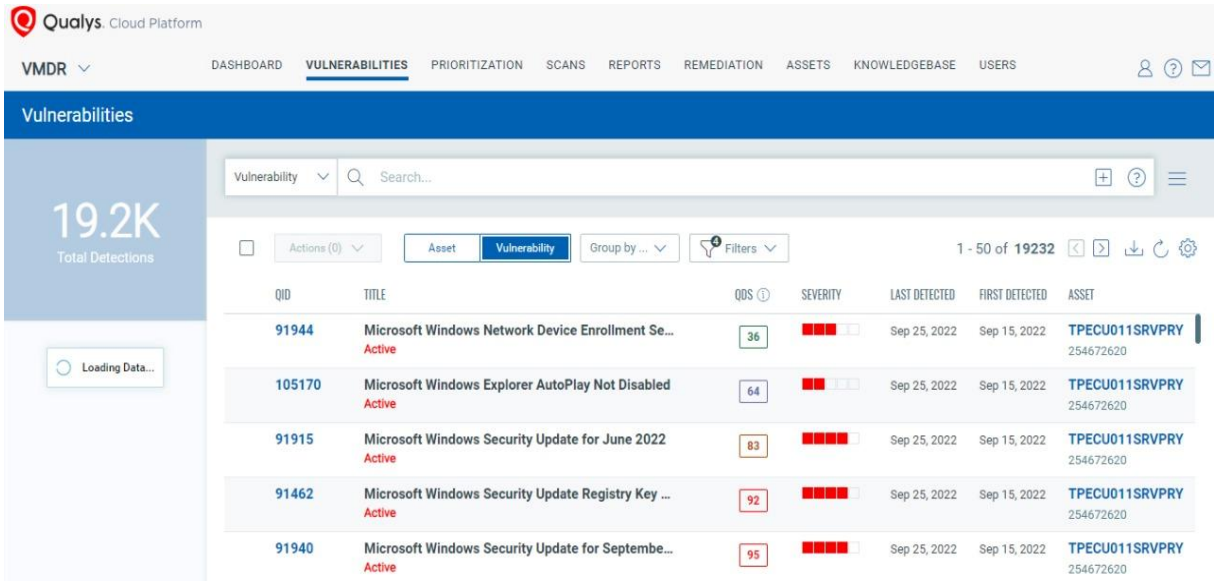
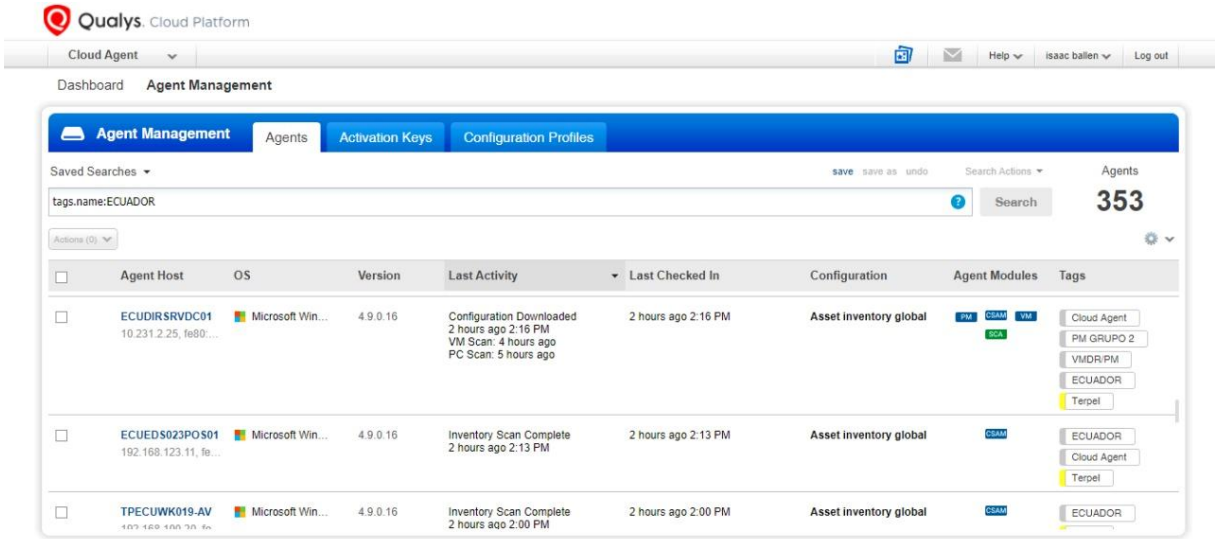


Figura 18

Monitoreo de Agentes activos en equipos de usuarios



Falcon.- Falcon es la plataforma CrowdStrike diseñada específicamente para detener las infracciones a través de un conjunto unificado de tecnologías entregadas en la nube que previenen todo tipo de ataques, incluido el malware y mucho más. Los

atacantes sofisticados de hoy en día van "más allá del malware" para violar las organizaciones, confiando cada vez más en exploits, días cero y métodos difíciles de detectar, como el robo de credenciales y herramientas que ya forman parte del entorno o sistema operativo de la víctima, como PowerShell. CrowdStrike Falcon responde a esos desafíos con una solución poderosa pero liviana que unifica el antivirus de próxima generación (NGAV), la detección y respuesta de punto final (EDR), la inteligencia de amenazas cibernéticas, las capacidades administradas de búsqueda de amenazas y la higiene de seguridad, todo contenido en un pequeño, único, sensor liviano que se administra y entrega en la nube.

Brinda una protección completa y comprobada para defender a su organización contra ataques de malware y sin malware, ya sea que sus puntos finales estén en línea o fuera de línea. Al incorporar identificación de malware conocido, aprendizaje automático para malware desconocido, bloqueo de exploits y técnicas avanzadas de comportamiento de indicador de ataque (IOA), CrowdStrike Falcon permite a las organizaciones reemplazar con confianza sus soluciones AV heredadas existentes, pues permite la integración con Windows System Center, para aquellas organizaciones que necesitan demostrar el cumplimiento de los requisitos normativos correspondientes.

Las ventajas que nos entrega Falcon desde el aplicativo implementado, surgen para determinar aplicaciones, ejecutables o amenazas en los endpoints, ayuda mucho a detectar, alertar y en su efecto poder aislar equipos con sospechas de seguridad.

Figura 19

Monitoreo de detecciones de amenazas en equipos de usuarios

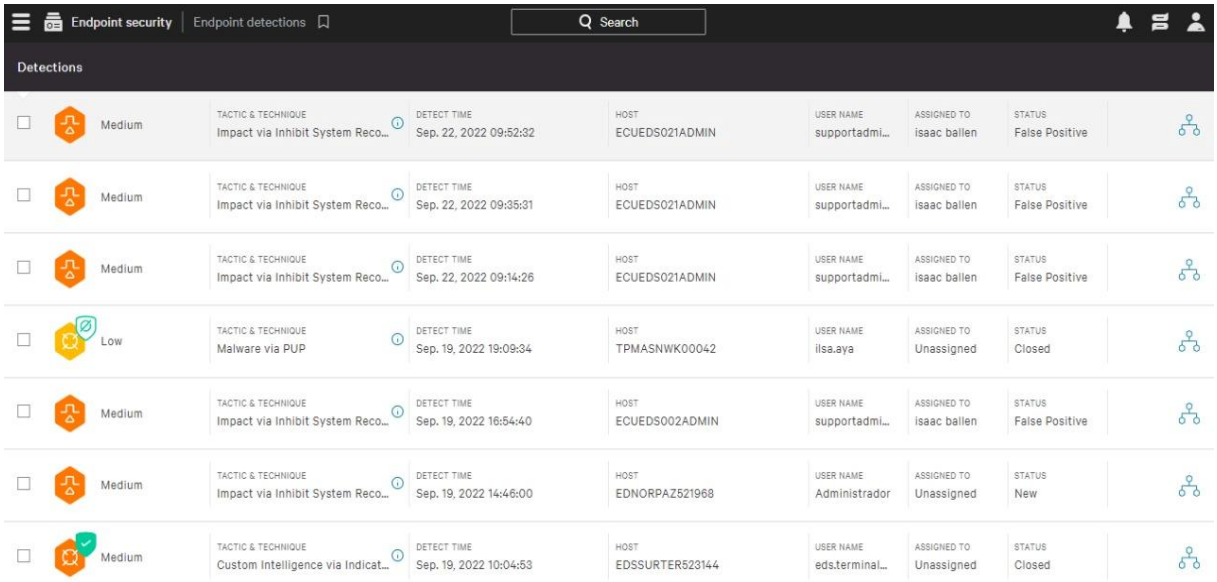
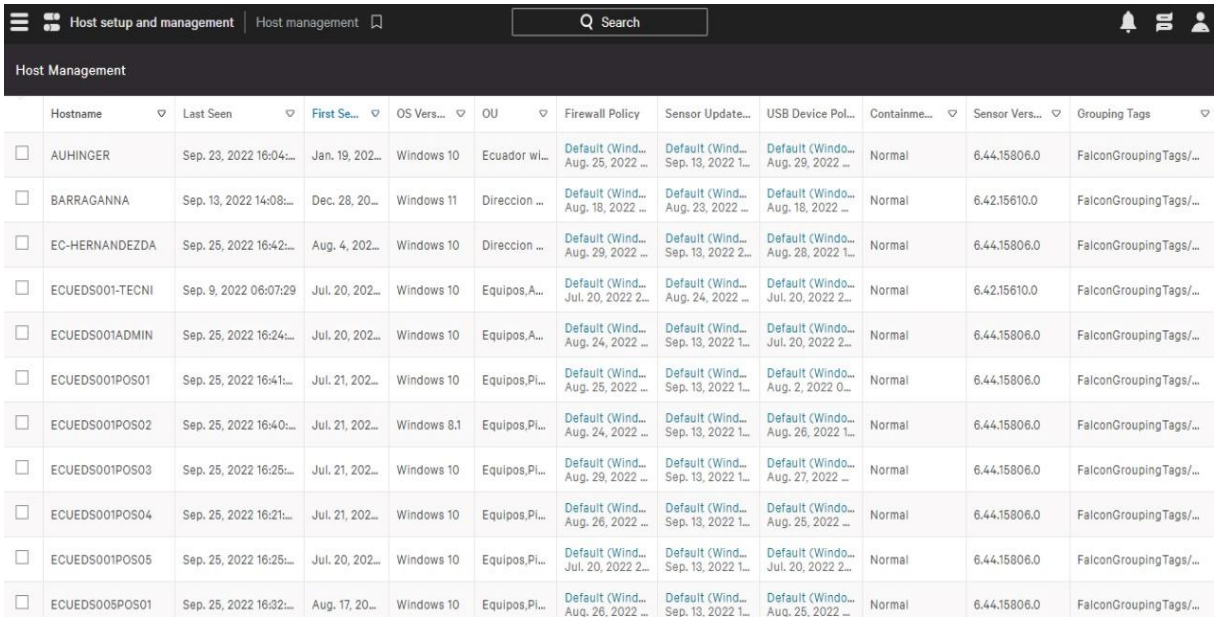


Figura 20

Control de agente instalado en equipos de usuarios



Los costos para considerar dentro de la propuesta de mejora se determinan dentro del siguiente cuadro de costos:

Tabla 4

Presupuesto de Licenciamiento Agentes de Seguridad

Cant	Servidor	Cost Unit	Cost Tot
43	Licenciamiento Open DNS (Servidores)	$12,75	$548,25
130	Licenciamiento Open DNS (Puntos de Venta)	$8,50	$1.105,00
43	Licenciamiento Open DNS (Estaciones de Trabajo)	$8,50	$365,50
43	Licenciamiento Antivirus (Servidores)	$9,90	$425,70
130	Licenciamiento Antivirus (Puntos de Venta)	$6,50	$845,00
43	Licenciamiento Antivirus (Estaciones de Trabajo)	$6,50	$279,50
43	Licenciamiento Qualys (Servidores)	$8,90	$382,70
130	Licenciamiento Qualys (Puntos de Venta)	$7,00	$910,00
43	Licenciamiento Qualys (Estaciones de Trabajo)	$7,00	$301,00
	TOTAL INVERSIÓN		**$5.162,65**

3.- Las actualizaciones automáticas y los parches de seguridad de Windows son actualizaciones acumulativas propias del sistema operativo, enfocadas a solucionar vulnerabilidades del ordenador. Todos los sistemas operativos tienen vulnerabilidades, ya sean nuevas o algunas viejas que acaban de ser reveladas o descubiertas, cuando salen a la luz es importante solucionarlas parcheándolas antes de que alguien las explote. Imagina que se descubre que, debido a un determinado fallo, alguien pudiera entrar en algún ordenador debido a una vulnerabilidad del computador. La manera de solucionarlas es mediante una actualización de versión ó parches, por este detalle Microsoft desarrollaría una solución en cuanto se descubriera este fallo, y la enviaría con un parche de seguridad. Es verdad que la mayoría de parches son actualizaciones acumulativas, pero cuando se trata de un único error muy grave también es posible que envíen el parche de forma independiente. Sea como fuere, este parche siempre llegará mediante Windows Update (Servicio propio de Windows, dentro del sistema operativo), y de ahí que siempre recalquemos la

importancia de tener actualizado el software, porque estos parches llegan como cualquier otra actualización, siempre y cuando se mantenga licenciamiento propio de Microsoft.

Otra forma también es visitar las fuentes oficiales del Fabricantes (Microsoft) ya que acostumbradamente lanzan una única actualización cada mes con todos los nuevos parches de seguridad, para que esto se cumpla es recomendable mantener el Sistema Operativo licenciado y con versión de los últimos años. En cuanto a los problemas de seguridad, pueden ser de varios tipos, pueden ser problemas de incompatibilidades que hayan sido causados por las grandes actualizaciones que Windows recibe dos veces al año, u otros problemas de compatibilidad, con hardware o software de terceros que pueda llevar arrastrando desde versiones anteriores. Muchas organizaciones manejan procesos más robustos colocando servidores WSUS encargados únicamente en realizar las actualizaciones en los equipos de trabajos a través de políticas que permitan mantener actualizados sus sistemas operativos en los ordenadores de la compañía.

Para considerar el punto de mejora, se debe contemplar el licenciamiento Microsoft del sistema operativo de los equipos de cómputo de la organización, los cuales necesitan en este caso (Windows 10 Pro y Windows Server 2019 STD). Tras el análisis se determinó la siguiente necesidad:

Tabla 5

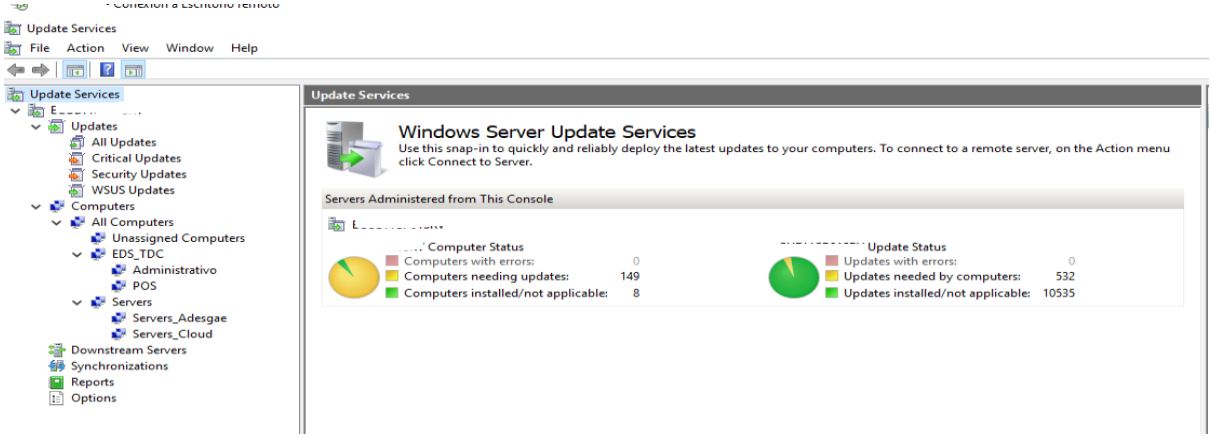
Presupuesto Licenciamiento Actualizaciones de Sistemas Operativos

Cant	Detalle	Costo Unit	Costo Total
15	Servidores locales Renovación a (Windows Server 2019 STD)	750	11250
35	Puntos de Venta Renovación a (Windows 10 Pro)	110	3850
9	Equipos de Administradores (Windows 7 Profesional)	110	990
	TOTAL		**$16.090**

Una vez implementado el proceso de actualizaciones a través del servidor WSUS, se puede validar que los procesos de actualizaciones y parchados se empiezan a realizar en los equipos, se emite una muestra de la infraestructura de actualizaciones dentro de WSUS:

Figura 21

Control de agente instalado en equipos de usuarios



4.- Para la seguridad perimetral y las políticas de navegación, se propone colocar la herramienta de control (Firewall) y los accesos de navegación dentro de la infraestructura a través de políticas o perfiles de accesos de salida a internet a los

equipos de cómputo de la organización. La herramienta Fortigate de Fortinet actualmente ofrece una Gestión Unificada de Amenazas, la cual ejecuta a través de una plataforma que integra dispositivos de seguridad, tanto físicos como virtuales. Estos dispositivos de seguridad realizan funciones de seguridad como firewalls, detección de intrusiones, filtrado web y protección contra malware o correos no deseados. Dentro de esta herramienta podremos tener configuraciones como (Filtrado Web, Políticas de Navegación, publicación de websites y NAT's, conexiones VPN seguras, IPSec VPN, entre otras. Las mismas que servirán para controlar de manera eficiente las actividades de los usuarios al momento de navegar por Internet. La propuesta busca un servicio SAS, de forma administrada por el proveedor para evitar detalles operativos, tal cual apunta el mercado con el modo renta como solución integral al servicio.

Los perfiles de navegación serán aplicados dependiendo de las funciones de los usuarios según sus actividades y funciones dentro de la compañía:

Perfil Básico.- Va destinado a usuarios de primer nivel que sólo necesitan accesos a ciertos sitios ya sean internos o externos y que son de necesidad clave para los procesos operativos o administrativos de sus áreas o departamentos, como por ejemplo (Puntos de Venta, Pasantes, Asistentes).

Perfil Medio.- Perfil de navegación destinado a usuarios con cargos que por sus funciones necesitan acceder a consultas o accesos de varias categorías como bancos, investigativo, gubernamentales, etc.

Perfil VIP.- Perfil con acceso de nivel alto o gerencial, usuarios que mantienen mayor libertad en navegación como streaming, pero con bloqueos a nivel estratégico de seguridad.

Una vez definido el proceso y determinar las categorías que se van a requerir dentro de la herramienta, se puede solicitar el aproximado dentro de los costos que cubren esta necesidad, vale mencionar que se busca una alta disponibilidad para mantener una contingencia en el caso de incidentes operacionales:

Tabla 6

Presupuesto de Implementación de Firewall en Alta Disponibilidad

Cantidad	Servicio	Detalle de requerimiento	Costo Mensual	Costo Anual
1	SEC-NGFW-INTERNET CONTROL	Gestión de la ciberseguridad con Firewall de Siguiente Generación (Modalidad Virtual en Alta Disponibilidad)Incluye: Reglas de FW Incoming, Reglas de FW Outgoing ilimitadas, AV/AS, Prevención de Intrusos, VPN para 100 usuarios remotos, 10 canales VPN site to site, Webfilter personalizado, Reportes Estándar Generado Automáticamente con frecuencia, Respaldo Automático de la configuración.	195	2340

5.- Dentro del proceso de mejora se considera uno de los más importantes, el estudio para el procedimiento del sistema de recuperación anti-desastres, el mismo que conlleva una inversión mucho mayor pero con gran provecho debido a que se podrá mantener un mejor esquema de recuperación en el caso de algún incidente al Servidor principal de la EDS o TDC; siendo este el que podría ocasionar pérdidas considerables en el entorno de los procesos transaccionales de la compañía. Al considerar la mejora se evalúan los costos del licenciamiento de los motores de Base de Datos de los Servidores Locales, los mismos ayudarán a ejecutar sentencias, tareas programadas y sistemas de replicación a otro Servidor local que se encontrará

en el mismo lugar para poder sincronizar la información en espejo y poder mantener la información lo más exacta posible en el momento de algún incidente con el Servidor principal.

Este proceso ayudará a tener un tiempo de respuesta mucho menor y así evitar pérdidas de ventas o cierre de operación temporal hasta poder levantar la contingencia, es un plan de mejora que aparte de poder mantener mayor tiempo de respuesta en los SLA's (Niveles de atención de servicio), ayuda a reaccionar de forma proactiva ante desastres fortuitos a la operación, así se garantiza la continuidad del negocio y la agilidad operativa. Para la inversión de aquello se considera el siguiente presupuesto:

Tabla 7

Presupuesto Licenciamiento Ambientes de Bases de Datos y Replicación

Cantidad	Detalle	Costo Unitario	Costo Total
27	Licenciamiento SQL EXPRESS 2019 STD	1300	35100
	TOTAL $		**35100**

Una vez determinado todo el plan de la propuesta, detallando en cada etapa los costos referenciales y cotizados se expone el presupuesto total de la inversión para la propuesta de mejora, quedando un definitivo según la siguiente tabla expuesta:

Tabla 8

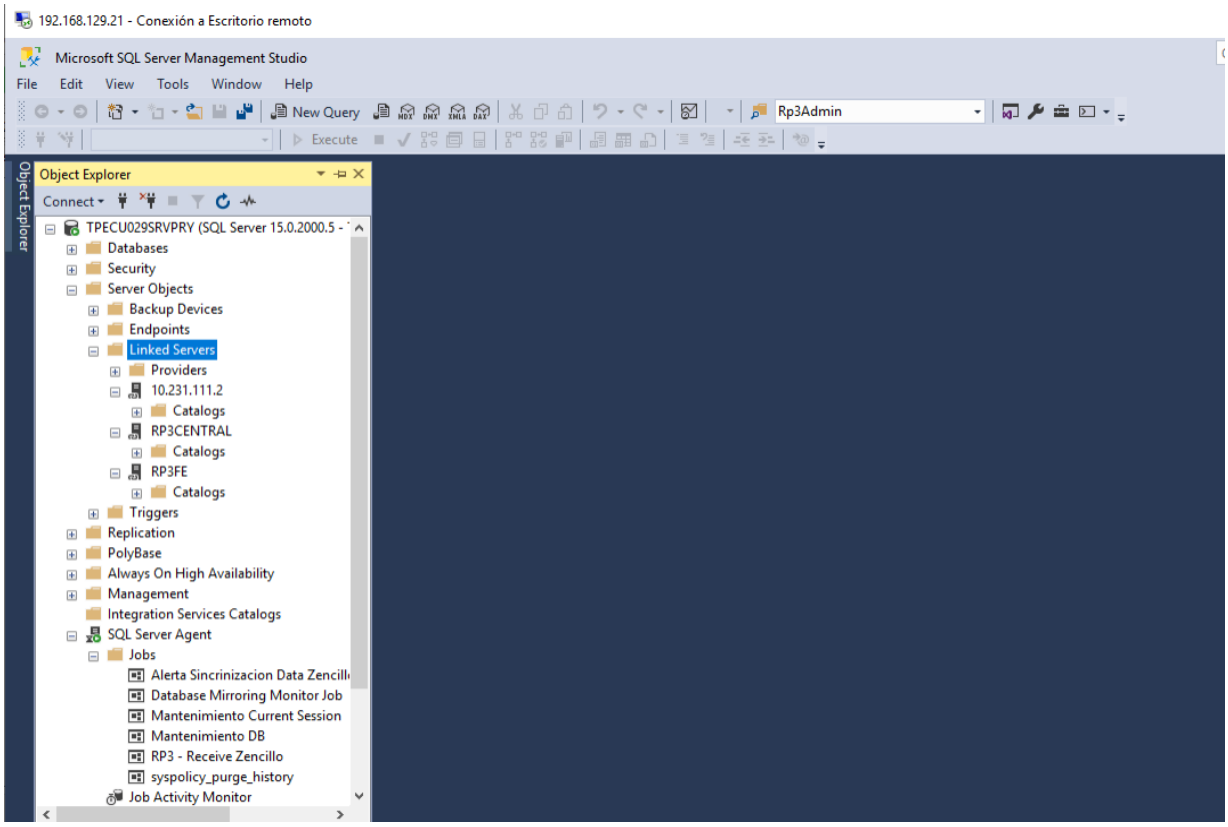
Presupuesto Total Propuesta de Mejora Seguridad Informática, ADESGAE

Cant	Descripción	Costo Unitario	Costo Total
1	Análisis de Vulnerabilidades	1800	1800
1	Costo de Licenciamiento Qualys (Servidores, PC's)	1593,70	1593,70
1	Costo de Licenciamiento Falcon (Servidores, PC's)	1550,20	1550,20
1	Costo de Licenciamiento Open DNS (Servidores, PC's)	2018,75	2018,75
27	Licenciamiento SQL para Servidores de BD	1300	35100
1	Licenciamiento Microsoft Windows	16090	16090
12	Licenciamiento mensual Firewall Gestionado	195	2340
	TOTAL		**60492,65**

Vale mencionar que existen dos inversiones, las perpetuas que corresponden a la adquisición del licenciamiento Microsoft (SQL y Windows), y las que derivan en pagos mensuales/anuales como servicios SAS, los mismos deberán considerarse anualmente como presupuesto para mantener el esquema y arquitectura de infraestructura. Al realizar el procedimiento correspondiente de la infraestructura para la replicación de Bases de Datos en los ambientes de facturación, se aprecia el cambio de los LinkServers realizados para el proceso de alta disponibilidad, el que se mantiene activo en el caso de fallas en el Servidor Principal:

Figura 22

Visualización de réplica activa base de datos de servidor Eds GyR



4.3 Mecanismos de Control

Dentro del esquema de los mecanismos y controles que se consideran en la propuesta de mejora, existen 5 procesos idóneos para la Organización, se evaluaron costos e inversiones aptas para el procedimiento, en ellas rigen el siguiente detalle:

1.- Una vez ejecutado el análisis de vulnerabilidades se deben realizar las correcciones necesarias para mitigar las brechas y poder mantener una arquitectura segura dentro de la organización.

2.- El control de Qualys, Lumu, Falcon, consta de realizar monitoreos diarios y constantes, especificando y ordenando validaciones recurrentes automáticas para notificaciones de hallazgos que requieran corrección en sistemas operativos ó aplicaciones del negocio.

3.- Una vez que se corrijan y mantengan sistemas operativos actualizados, se podrá establecer un proceso automático de procedimientos o procesos de parchado, los mismos que se podrán ejecutar en horarios flexibles para los usuarios o para los servidores que requieren esta actividad. Para así poder cumplir con los objetivos de seguridad organizacional.

4.- Una vez revisados y establecidos los controles de accesos de navegación por roles o perfiles, podemos mitigar los riesgos de accesos no autorizados a páginas que pueden ocasionar problemas serios en seguridad a la organización, los controles declaran que serán revisados y auditados por usuarios al azar, dentro de los períodos de control de los procesos de Auditoría. Esto permitirá mantener co-relación con los accesos a otros sistemas de información de la compañía.

5.- El Plan de control del sistema anti-desastres velará por que se evalúen los respaldos diarios o incrementales en ambientes de pruebas, para asegurar que la réplica se está cumpliendo a cabalidad, que la misma se ejecuta satisfactoriamente y se no existen problemas de sincronización. Con esto podremos asegurar la data de las EDS y TDC. Otro punto clave es minimizar el tiempo de respuesta en la subida de BD del ambiente de replicación, para asegurar y garantizar la continuidad del negocio en el menor tiempo posible.

CAPITULO V: SUGERENCIAS

5.1 Sugerencias

El presente trabajo de investigación tuvo como objetivo cumplir las expectativas a través de las herramientas mencionadas en todo el proceso de la mejora de la seguridad en la compañía ADESGAE CIA LTDA, tras los resultados obtenidos podremos mencionar las siguientes sugerencias o recomendaciones:

Plan de Sugerencias 01	Una vez cerrado el proceso de análisis de vulnerabilidades y etical hacking en la compañía ADESGAE, se recomienda seguir y mantener el siguiente plan post propuesta: 1.- Realizar un análisis de vulnerabilidades antes de colocar en producción cualquier proyecto o sistema de información dentro de la arquitectura de la organización, ya sea un servicio local o un SAS con algún proveedor.
Plan de Sugerencias 02	Al diseñar y dejar implementadas las herramientas de control de DNS's, antivirus y auditoría de aplicativos, se recomienda lo siguiente: 1.- Administrar las consolas mencionadas con el fin de controlar adecuadamente los registros, alertas y hallazgos en los equipos de cómputo de los usuarios finales. Así se garantiza cerrar brechas de seguridad en posibles intentos de robo de información, aplicaciones no deseadas o accesos no autorizados en sitios web.
Plan de Sugerencias 03	Una vez aplicado el proceso de actualizaciones automáticas con la instalación del Servidor WSUS dentro de la organización, se sugiere contemplar el siguiente escenario:

	1.- Velar por la aplicación de actualizaciones de parches de seguridad o actualizaciones de software con una revisión periódica de por lo menos 1 vez a la semana, asegurando que los mismos se encuentren disponibles y se repliquen a todos los equipos de la compañía. Así se garantiza cumplir con los estándares de actualizaciones de los Sistemas Operativos.
Plan de Sugerencias 04	Posteriormente a implementar las políticas y roles de navegación segura, filtrado web y seguridad perimetral, se recomienda lo siguiente: 1.- Controlar constantemente los accesos de navegación de los usuarios nuevos o antiguos, con la finalidad de mantener actualizados sus permisos. 2.- Asegurar que no se apliquen cambios en las configuraciones de sitios publicados o NAT's no permitidos ni autorizados, con la finalidad de no exponer los servicios internos. 3.- Bloquear puertos de salida a IP's públicas determinadas como malintencionadas, y agregarlas en listas negras en las parametrizaciones del Firewall. 4.- Asegurar respaldos diarios a la configuración del firewall, para mantener el plan de contingencia para el servicio de replicación con el otro equipo de alta disponibilidad. 5.- Controlar los accesos VPN de los usuarios, proveedores, asesores, para no tener accesos no debidos a ambientes críticos que puedan comprometer la seguridad de la información.

	6.- Controlar los certificados de confianza y servicios publicados con los protocolos http y https para evitar amenazas externas.
Plan de Sugerencias 05	Una vez definido y establecido el sistema de recuperación anti desastres, se requiere seguir las recomendaciones expuestas a continuación: 1.- Cumplir a cabalidad con la validación de replicación de los Servidores locales, garantizar que la misma se ejecute normalmente. 2.- Ejecutar un plan de conmutación en horarios en donde no se comprometa el negocio o la operación para subir la replicación y garantizar que el proceso trabaja a cabalidad. 3.- Mantener Servidores de backup en stock para evitar un posible escenario en donde los 2 Servidores fallen, teniendo así un protocolo de “Backup del Backup”. 4.- Asegurar el licenciamiento y presupuesto a futuro de los servicios SQL en los ambientes.

Como sugerencia adicional, fuera del contexto de la propuesta de mejora, se brinda una recomendación a criterio personal y es que en las organizaciones actualmente deberían considerar recursos que velen por la ciberseguridad de los sistemas de información, no sólo la seguridad lógica sino la seguridad informática la encriptación de datos, la ejecución de pentesting y cierre de vulnerabilidades en los servicios organizacionales. Estos recursos (Analista de Ciberseguridad) deben ser los encargados de establecer políticas, controles y monitoreos con la finalidad de

garantizar la disponibilidad y veracidad de la información, siendo proactivos ante situaciones que puedan salirse de control.

5.2 Conclusiones

La propuesta de mejora que se establece en el actual trabajo de investigación concluye y finaliza con los siguientes puntos relevantes:

La propuesta de mejora dentro del alcance del objetivo general cumple con mejorar la seguridad de la empresa ADESGAE CÍA LTDA, a través de mecanismos, herramientas y buenas prácticas de control como antivirus, políticas de navegación, agentes de monitoreo de ciberseguridad, análisis forense, etc.

Al analizar las brechas de seguridad, podemos detectar y cerrar las mismas puesto que estas pueden comprometer a la organización, permitiendo a ciberdelincuentes aprovecharse y secuestrar información importante para la compañía, siendo víctimas en escenarios catastróficos, pérdidas monetarias y rompimiento de relaciones comerciales de grandes clientes otorgando así mala reputación en los mercados.

Con las herramientas de monitoreos aplicaremos controles varios como resguardar sitios no seguros, accesos no autorizados en los sistemas de información, navegación segura, auditoría y seguridad en los endpoints, otorgando así protocolos necesarios para reaccionar ante cualquier incidente de seguridad que puedan ocasionar la indisponibilidad de los servicios de información.

Al mantener los Sistemas Operativos actualizados, controlamos los parches y vulnerabilidades en los distintos ambientes de trabajo (Tanto en Servidores como en estaciones de trabajo).

Al definir un plan de recuperación anti-desastres, podemos reaccionar ante cualquier eventualidad ocasionada por algún ciberdelincuente, considerando que se mitigará en el menor tiempo posible para garantizar de manera óptima tiempos de respuesta más rápidos y así poder levantar los ambientes de manera ágil, aportando valor al negocio.

Los ciberdelincuentes tratan de atacar a empresas de pymes altos, lo que se considera a empresas privadas o públicas grandes ser un foco visible a nivel mundial, para aquello es obligación mantener presupuestos anuales para la parte de seguridad y así evitar contratiempos internos.

BIBLIOGRAFÍA

Aguilera, P. (2011). Redes seguras (Seguridad informática). Editex.

Areitio, J. (2008). Seguridad de la información. Redes, informática y sistemas de información. Paraninfo.

Arroto, D., Gayoso, V., & Hernández, L., (2020). Ciberseguridad. CSCI.

ISO/IEC 27000 (2018). Sistemas de Gestión de la Seguridad de la Información.

KASPERSKY CORPORATION (2022). Ciberamenaza en tiempo real. CIBERMAP. Consultado el 11 de Julio del 2022. https://cybermap.kaspersky.com/

Lopez, P. & Valencia, H. (2017). Tratamiento informático de la información. Editex.

Martinez, J. (2015). Planes de Contingencia. Díaz de Santos SA.

Ñaupas, H., Mejía, E., Novoa, E. & Villagomez, A. (2013). Metodología de la investigación. 4ta Edición. Ediciones de la U.

Solarte, F., Enriquez Rosero, E., & Benavides, M. (2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica - ESPOL, 28(5). http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456

Tejada, E. (2015). Auditoría de seguridad informática. IC Editorial.

Vieites, Á. (2013). Auditoría de seguridad informática. Ediciones de la U.