UNIVERSIDAD TECNICA DE BABAHOYO

FACULTAD DE ADMINISTRACION FINANZAS E INFORMATICA

PROCESO DE TITULACION

MAYO/SEPTIEMBRE 2023

EXAMEN COMPLEXIVO DE GRADO O DE FIN DE CARRERA

PRUEBA PRACTICA

PREVIO A LA OBTENCION DEL TITULO DE:

INGENIERA EN SISTEMAS DE INFORMACION

TEMA:

ANÁLISIS Y PROPUESTA SOBRE LA SEGURIDAD DE LA INFORMACIÓN QUE MANEJA EL CENTRO CRISTIANO "CONCILIO LATINOAMERICANO"

ESTUDIANTE:

ABDIAS DAVID JAÑA APOLINARIO

TUTOR:

PEÑAHERRERA LARENAS MILTON FABIAN

ING.

AÑO 2023

INDICE

RESUMEN

En el desarrollo de este caso de estudio, se identificaron varios problemas referente a la seguridad de la información, ya que por encuestas y entrevistas realizadas, tanto a los miembros que se hacen cargo del departamento de TIC y usuarios que manejan y manipulan el sistema web pudieron expresar inconvenientes o experiencias que tienen o presentan con respecto a la seguridad de la información, tales como, la falta de políticas de seguridad, falta de actualizaciones de sistemas operativos, interrupciones o deficiencias del sistema web y por ultimo falencias de respaldos de información ya que una vez borrada o alterada no se puede recuperar, al presentarse estos problemas se vuelve importante tener un enfoque con respecto a la importancia de la información y su resguardo donde se tiene como objetivo "Proponer estrategias de seguridad de la información en el centro cristiano "Concilio Latinoamericano "con el fin de identificar y abordar riesgos y amenazas en la protección de datos" haciendo uso de métodos inductivo-deductivo y técnicas de recolección de datos como entrevistas, encuestas, observación adoptando también la metodología de gestión de riesgo, teniendo como resultado la identificación de riesgos y amenazas, concluyendo los hallazgos encontrados y las opiniones tanto de los encuestados, la entrevista y criterio propio como la tome medidas inmediatas para fortalecer la seguridad de la información que maneja, ya que la falta de incidentes graves hasta el momento no garantiza protección futura, en donde gracias a esto se impartieron recomendaciones de mitigación y mejora para la seguridad de la información.

Palabras Clave: Concilio Latinoamericano, Seguridad de la Información, Riesgos, Amenazas, Activos, Análisis, Recomendaciones.

PLANTEAMIENTO DEL PROBLEMA

Hoy en día uno de los factores más importantes de las organizaciones y empresas en general es la seguridad de la información, ya que los incidentes relacionados con esta, comprometen los activos de las organizaciones poniéndolas en riesgo, si esta información es manipulada por terceros sin autorización.

Al pasar el tiempo, el Concilio Latinoamericano, ha experimentado un crecimiento constante y se ha consolidado como un referente en la comunidad cristiana y por ende la cantidad de los datos e información que maneja la institución, también han aumentado considerablemente.

La información manejada por el establecimiento, incluye registros de miembros, datos financieros, donaciones, actividades y diversos eventos, estos datos o esta información, debe ser tratada con el máximo cuidado y protección, fundamentándose en puntos como el cumplimiento normativo, salvaguardar la reputación del establecimiento, continuidad de las operaciones, prevención de pérdidas financieras y establecer una cultura de seguridad informática, en la cual hacen evidente la necesidad de mejorar la seguridad de la información para proteger los diferentes datos y asegurara la continuidad de las operaciones y preservar la confianza de la comunidad.

Los problemas que se presentan en el Concilio Latinoamericano se enfocan directamente en la forma de resguardar la seguridad de la información, extendiéndose tanto en la parte lógica como física del establecimiento. Dicho esto, se identificó que los equipos del personal laboral, cuenta un sistema operativo de Windows 7, siendo una versión antigua y haciendo más susceptible al equipo contra malware, virus, phishing y ataques de ingeniería social poniendo en riesgo la exposición de datos personales, en las últimas actualizaciones, traen nuevas características y funciones en las cuales contienen parches de seguridad que solucionan vulnerabilidades del sistema operativo haciendo posible la detección y prevención de ataques.

Por otro lado, durante los últimos 12 meses, se ha identificado una problemática recurrente en los servicios del Concilio Latinoamericano, relacionada con la interrupciones y deficiencias en la funcionalidad del sistema web que utilizan, experimentando lentitud al abrir el sistema en momentos específicos de uso. La constante presencia de esta dificultad está afectando negativamente la experiencia de los usuarios y se hace presente la necesidad de una evolución para buscar soluciones y resguardar la información.

También, una de las problemáticas que se revela en el establecimiento, es la ausencia de políticas que promueva cambios regulares de contraseñas para usuarios, así como en la carencia de una estructura de limitación de privilegios basada en roles para el personal, la inexistencia de estos dos puntos importantes, hacen que aumente el riesgo de vulnerabilidades de seguridad con ello resalta o facilita el acceso no autorizado y posibles exposiciones de información sensible. Estas limitaciones en las medidas de seguridad y control plantean la necesidad de implementar un enfoque más riguroso en la gestión de accesos y en la seguridad dentro del Concilio.

También se resalta que existe una falencia de respaldos de información, ya que han ocurrido sucesos en donde han tenido accidentes en eliminar un dato del sistema y por ende se borra desde la base de datos, en donde esta información ya no ha podido ser recuperada afecta negativamente la capacidad del Concilio para tomar decisiones informadas y cumplir con sus responsabilidades, además de exponerlo a sanciones legales y desafíos en la recuperación de datos en caso de incidentes. La necesidad imperante de abordar esta problemática se refleja en la urgencia de establecer un sistema de respaldo robusto y periódico que garantice la disponibilidad y la protección de la información valiosa en todas las circunstancias.

JUSTIFICACION

Hoy en día la seguridad de la información se ha convertido en uno de los pilares fundamentales para la sostenibilidad y el éxito de las organizaciones y empresas, y el Concilio Latinoamericano no es la excepción Con el paso del tiempo, el concilio ha experimentado un notable incremento de datos e información que maneja, abarcando registros de miembros, información financiera, comunicaciones pastorales y diversos eventos. Este crecimiento, ha adquirido un papel central en la comunidad, en donde, la importancia de salvaguardar esta información radica en diversos factores cruciales. En primer lugar, el cumplimiento normativo es imperativo, ya que la institución está sujeta a regulaciones rigurosas en materia de protección de datos personales y seguridad de la información, ya que el incumplimiento de estas normativas podría resultar en sanciones legales y multas. Además, la continuidad de las operaciones se ve amenazada por las interrupciones en la funcionalidad del sistema web, lo que afecta negativamente la experiencia de los usuarios o miembros de la comunidad causando inconvenientes considerables. Por otro lado, la ausencia de políticas de cambio regular de contraseñas y limitación de privilegios aumenta el riesgo de accesos no autorizados, exponiendo así a la institución a posibles vulnerabilidades de seguridad. Esto, a su vez, podría comprometer la confidencialidad e integridad de la información sensible, incluyendo datos de miembros y datos financieros dando paso a perdias de información ya que tampoco se cuenta con respaldos de información siendo un riesgo importante, ya que la pérdida irrecuperable de datos afectaria la capacidad del Concilio para tomar decisiones informadas y cumplir con sus responsabilidades, poniendo en riesgo la reputación y la confianza comunitaria ya que estos son activos intangibles invaluables, y la falta de seguridad de la información podría erosionar la confianza de los miembros y feligreses de la institución.

Al abordar esta problemática, se vuelve una necesidad importante para garantizar la

integridad, confidencialidad y disponibilidad de la información valiosa, así como para cumplir con las regulaciones vigentes, preservar la continuidad de operaciones, prevenir pérdidas financieras, promover una cultura de seguridad informática y proteger la reputación de la comunidad, ya que la inversión en medidas de seguridad adecuadas no es solo una necesidad urgente, sino una responsabilidad hacia todas las partes interesadas del Concilio Latinoamericano para establecer una base sólida para operar en un entorno digital cada vez más complejo y amenazante.

OBJETIVO GENERAL

Proponer estrategias de seguridad de la información en el centro cristiano "Concilio Latinoamericano “con el fin de identificar y abordar riesgos y amenazas en la protección de datos.

OBJETIVO ESPECIFICOS

1. Analizar las posibles amenazas que tiene el centro cristiano “Concilio Latinoamericano”.
2. Evaluar y cuantificar el nivel de riesgo asociado a cada amenaza identificada en el centro cristiano "Concilio Latinoamericano", utilizando una metodología de análisis de riesgos para priorizar las acciones de seguridad y asignar recursos de manera efectiva.
3. Definir políticas de seguridad que garantice la integridad de los datos.

LINEAS DE INVESTIGACION

Línea de investigación

Sistemas de información y comunicación e innovación.

Sublínea de investigación

Redes y tecnología inteligentes de software y hardware.

Como línea principal de investigación tenemos la relación con la seguridad de la información en el Centro Cristiano "Concilio Latinoamericano" puede ser abordada a través de la lente de la línea de investigación siendo de énfasis al análisis, la propuesta y la implementación de medidas de seguridad efectivas pueden contribuir a la protección de la información valiosa y al cumplimiento de los objetivos de la organización en un entorno tecnológico en constante cambio.

La sublínea de investigación en redes y tecnología inteligentes de software y hardware puede proporcionar soluciones y enfoques avanzados para abordar los desafíos de seguridad de la información que enfrenta el Centro Cristiano "Concilio Latinoamericano". La implementación de tecnologías inteligentes puede mejorar la eficiencia y la efectividad de las medidas de seguridad, contribuyendo así a proteger la información valiosa y los activos de la organización.

ARTICULACION DEL TEMA

En el desarrollo de este estudio de caso se procederá a llevar a cabo un análisis exhaustivo de la seguridad de la información del centro cristiano “Concilio Latinoamericano” examinando el proceso que tiene la organización para proteger y resguardar la información que posee, proponiendo medidas para fortalecer y mejorar la seguridad de dicha información.

Tema clave: Seguridad de la información en el “Concilio Latinoamericano”; el enfoque principal es el análisis de las prácticas y políticas actuales relacionadas con la seguridad de la información en el establecimiento, en la cual se investigará la infraestructura tecnológica que se utiliza para almacenar datos y las medidas de protección implementadas para evitar brechas de seguridad y filtración de información.

Tema de vinculación con la sociedad: Protección de datos personales y confidencialidad de información; Este es un aspecto principal e importante que se vincula con la seguridad de la información en el concilio latinoamericano, como antes mencionado hace referencia a la protección de datos personales y la confidencialidad de sus miembros, iglesias, colaboradores y beneficiarios, ya que se analiza, como se almacenan los datos, la seguridad que se tiene al manipular, quienes o quien tiene acceso a estos datos, garantizando el cumplimiento de privacidad y las leyes de protección de datos vigentes.

Tema de prácticas pre profesionales: Capacitación en seguridad de la información; en las practicas pre profesionales se evaluará como el centro cristiano prepara y capacita a su personal en materia de seguridad de la información y se propondrán estrategias para fomentar la seguridad y buenas prácticas en el establecimiento.

MARCO CONCEPTUAL

La obtención de información ilegal, es muy demandado en las organizaciones, basándose en la transferencia, manipulación u obtención ilegal de la información confidencial de una organización, esto puede ser tanto por la parte financiera, contable, de recursos humanos etc. Estos robos pueden incluir contraseñas, códigos de software e incluso algoritmos, información que viaja en la red, manipulación de bases de datos, entre otros.

Centrándonos en esta sección del caso de estudio, se presentarán conceptos teóricos y fundamentos relacionado con el tema de cabecera, los cuales serán de suma importancia para el desarrollo de este estudio, abordando conceptos claves y teorías que sustentan el estudio.

Según el (ESQUEMA NACIONAL DE SEGURIDAD, 2022) , la categoría de la seguridad de un sistema de información modula el equilibrio entre la importancia de la información que maneja, los servicios que presta y el esfuerzo de la seguridad requerida en función de los riesgos a los que está expuesto, bajo el principio de proporcionalidad.

El Esquema Nacional de Seguridad, menciona el valor de la información que los diferentes sistemas manejan, la información varía dependiendo del departamento o modulo que se tiene acceso en los sistemas.

En el Concilio latinoamericano, la información que maneja el departamento de TI, es de suma importancia ya que también se relaciona con la parte financiera, operativa y resguarda la información de los feligreses que pertenecen al centro cristiano, en donde resguardar y proteger esta información es de suma importancia para asegurar la confidencialidad del establecimiento

¿Qué es la seguridad?

La seguridad de manera general, es básicamente el estado de estar protegido contra daños, peligros o amenazas de un entorno.

Para (Benedetti y Renoldi, 2022) La se seguridad puede considerarse como un estado de

ausencia de peligros y de condiciones que puedan provocar daño físico, psicológico o material en los individuos y en la sociedad en general.

Con mención a lo citado se puede decir que la seguridad implica al estado de estar protegido ante cualquier suceso o amenaza en el departamento de TI, el concepto de la seguridad se relaciona explícitamente con la prevención y la mitigación de posibles peligros y riesgos, con un objetivo en especial que sería la garantía de una protección de la información en general.

¿Qué es la seguridad de la información?

Refiriéndose a la seguridad de la información es el acto de proteger los datos de un determinado sistema de una organización o entidad, con el fin de resguardar la información de una manera confidencial, integra y a la vez la disponibilidad de la información, así como garantizar la autenticidad y la privacidad de las personas involucradas que tienen acceso a la información de una entidad.

En la actualidad la información digital es crucial para diversas empresas, organizaciones y particularidad, esta se ha vuelto esencial para prevenir una serie de amenazas.

Para (Vega Briceño, 2021) La seguridad de la información es un concepto que se involucra cada vez más en muchos aspectos de nuestra sociedad hiperconectada, en gran parte como resultado de nuestra adopción casi ubicua de la tecnología de información y comunicación.

Según la (ISO/IEC 27701, 2019) también abreviada como PIMS (Sistema de Gestión de Privacidad de la Información) enfrasca un marco para que los Controladores y Procesadores de Información Personal gestionen la privacidad de los datos.

En otras palabras, PIMS es una enfoque estructurado y organizado para ayudar a las empresas y diversas entidades a manejar y proteger adecuadamente la información personal de las personas, abordando cuestiones relacionadas con la privacidad.

¿Qué es infraestructura tecnológica?

Esta infraestructura puede ser tanto física como virtual en la cual comprende una variedad de elementos que conforman para que una organización funcione de manera eficaz y respaldando las diversas operaciones tecnológicas. Podemos decir que, entre los componentes de una infraestructura está el hardware, software, las redes, sistemas o equipos de almacenamiento de información, como menciona (Segovia Cando y Chicaiza Medina, 2021), La infraestructura o equipamiento informático (servidores, equipos de red, computadores, juntamente con sus herramientas de administración), es uno de los pilares base de cualquier organización a nivel mundial; la seguridad que se aplica a esta, es un factor clave que mantiene el negocio operativo, la imagen y la integridad de las organizaciones.

¿Configuraciones inseguras?

Estas configuraciones hacen referencia a diversas falencias en seguridad de sistemas o aplicaciones que presentan o pueden ser un punto blanco en vulnerabilidades de seguridad en la cual pueden ser explotadas por atacantes para comprometer la integridad o disponibilidad de diversos servicios o comprometer datos de un sistemas, como contraseñas débiles o fáciles de adivinas o compartirlas entre múltiples cuentas, esto aumenta el riesgo de un acceso no deseado, tener permisos y accesos excesivos es otro factor que influye en las configuraciones inseguras ya que al conceder permisos innecesarios a usuarios puede resultar con filtración de datos o modificaciones de la información no autorizadas, ya que, como lo mencionan los autores (Barker c. et al., 2022) La mayoría de los ataques de ransomware son posibles debido a que hay usuarios que utilizan prácticas inseguras, administradores que implementan configuraciones inseguras o desarrolladores que no tienen la suficiente capacitación en seguridad (p. 13).

¿Qué son los ataques DoS y DDoS?

Ataque Dos (Denial of Service)

En teoría un ataque de DoS implica inundar un sistema o red especifica con un tráfico abrumador hasta que ya no pueda manejar solicitudes. Esto se hace mediante una variedad de métodos, como el envío masivo de solicitudes, saturación de red o el uso de recursos intensivo en los servidores.

Para (Mantilla et al., 2023)un ataque DoS como la degradación intencional a los servicios normales de la red. Los ataques más comunes están dirigidos al ancho de banda de la red y a la conectividad. Los ataques DoS más relevantes son: inundación de datos y basados en características del protocolo (p. 32).

Ataques DDoS (Distributed Dania lof Service)

Los ataques DDoS son básicamente una versión más actualizada de los ataques DoS, con este método los atacantes utilizan una red de dispositivos comprometidos, conocidos como "botnets", para generar un tráfico masivo y coordinado hacia un objetivo. Estos dispositivos pueden ser computadoras celulares etc., en la cual cada uno de ellos han sido infectados por malware y están bajo control del atacante, siendo una ventaja para ellos ya que enmascaran su dirección IP.

Según el autor (Gonzalez Manzano et al., 2019)dice que Existen multitud de noticias e investigaciones que relacionan los dispositivos IoT con ataques DDoS, pero el número de investigaciones que evalúan el potencial de los dispositivos IoT para efectuar los ataques DDoS es muy reducido (p. 12).

¿Políticas de acceso?

Según (Vega Velasco, 2018) La política de seguridad requiere no solamente conocer las amenazas a las que están expuestas la información y los recursos de una organización, sino

también establecer el origen de las mismas, que pueden ser internas o externas a la organización.

Según lo citado se enfrasca en la importancia de tener políticas de seguridad en el centro cristiano" concilio latinoamericano" resaltándose dos aspectos claves que son:

- la conciencia de las amenazas; que se basa en la comprensión y reconocimiento de las amenazas y riesgos a los que la información y los recursos del centro están expuestos constantemente, en la cual pueden incluir ataques cibernéticos, robo de datos, violaciones de privacidad que podrían poner en peligro la integridad y disponibilidad de los activos digitales del centro.
- Origen de amenazas; al establecer políticas de seguridad también de refiere a la identificación del origen de las amenazas que pueden ser tanto internas como externas.

Básicamente la implementación de políticas de seguridad se basa en identificar amenazas y su origen para tomar medidas y prevenir incidentes.

Políticas de acceso y autorización

Estas políticas de dividen en los partes que sería la de acceso, esta se refiere a las reglas y directrices que determinan como se permite o se deniega el acceso a recursos del concilio latinoamericano, es decir, estas políticas definen quien puede acceder a esos recursos, en qué momento y bajo que circunstancias, esta política se refiere a preguntas como ¿Quién puede acceder a la información del concilio? Y ¿A qué información puede acceder?

Mientras que las políticas de autorización tienen mayor impacto o se centra en las reglas y controles que dictan que acciones están permitidas una vez que un usuario tiene acceso a la información del concilio latinoamericano.

Como dice (Santana et al., 2019, p. 286)La correcta gestión de la seguridad de la información, busca establecer y mantener programas, controles y políticas, que tengan como

finalidad conservar la confidencialidad, integridad y disponibilidad de la información.

Con referencia a lo citado se recerca la importancia de diseñar y aplicar políticas de acceso y autorización sólidas y responsables para proteger los datos y los sistemas sensibles.

Estas políticas se pueden aplicar en el concilio latinoamericano con contraseñas seguras, dar acceso a roles, permisos y establecer una lista de controles de acceso.

Políticas de uso aceptables

Las políticas de uso aceptable son cruciales para la gestión de la seguridad de la información ayudando a promover un ambiente de trabajo seguro, ético y eficiente, para tener un uso apropiado, cubriendo diversos aspectos como el acceso a recursos y servicios, es decir establecer quienes tienen acceso para interactuar con los sistemas del concilio latinoamericano rigiéndose a diversas condiciones de uso como la confidencialidad, prohibiendo actividades no autorizadas o ilegales, como el uso inadecuado de los recursos o la divulgación de la información confidencial.

Políticas de contraseñas

Esta política se basa en la seguridad del acceso a sistemas en la cual se establecen diversos requisitos para que las contraseñas sean robustas y sea difícil para diversos atacantes tener acceso a las prioridades de los usuarios del concilio latinoamericano, también estableciendo una frecuencia en que las contraseñas deben ser cambiadas y la prohibición de compartirlas para asegurar y resguardar de la información.

Políticas de respuesta a incidentes

Relacionándose con los casos de violación de servicios, es decir los efectos de un incidente en la información, siendo cualquier evento o acción que ponga en riesgo la confidencialidad e integridad de los activos de la información.

Importancia de establecer políticas de seguridad en una organización

Las políticas de seguridad son esenciales para establecer una cultura de seguridad sólida, mitigar riesgos, cumplir con activos de la organización, ayudando a guiar las acciones y decisiones de los empleados y a mantener la información segura de la organización.

Según (Valencia Duque, 2019, p. 23) la informática desarrolla su función sobre todos los elementos técnicos que hacen parte de las TIC, la seguridad de la información actúa sobre la información como activo estratégico para la adecuada toma de decisiones empresariales en las organizaciones modernas estableciendo políticas de seguridad adecuadas.

¿Que son las copias de seguridad de un servidor?

Las copias de seguridad de un servidor son básicamente la duplicación de los datos, siendo un ende importante cuando existe algún problema en la infraestructura de los servidores o cuando existen robos o alteraciones de la información en una organización, esto se crea con el propósito de proteger y respaldar la información más crítica.

Las copias de seguridad de un servidor tienen varios propósitos clave como:

- **Recuperación de datos:** En caso de que ocurra una pérdida de datos, como resultado de un fallo del disco duro, un error del sistema o un ataque de malware, las copias de seguridad permiten restaurar los datos a un estado anterior y recuperar la información perdida.
- **Continuidad del negocio:** Las copias de seguridad son esenciales para garantizar la continuidad de las operaciones en caso de desastres. Si un servidor principal se vuelve inaccesible o inoperable, se puede utilizar una copia de seguridad para recuperar rápidamente los servicios y minimizar el tiempo de inactividad.
- **Prevención contra ransomware:** En el caso de un ataque de ransomware que cifra los datos, las copias de seguridad no afectadas por el ataque pueden utilizarse

para restaurar los datos sin tener que pagar un rescate.

- **Migración y clonación:** Las copias de seguridad pueden ser útiles cuando se necesita migrar a nuevos servidores o realizar pruebas en entornos de desarrollo sin afectar los datos en producción.
- **Recuperación de configuraciones y aplicaciones:** Además de los datos, las copias de seguridad también pueden incluir configuraciones de sistema, aplicaciones y otros elementos necesarios para que el servidor funcione correctamente. Esto facilita la restauración completa de un sistema en su estado original.

Existen diferentes enfoques para realizar copias de seguridad de servidores, como copias de seguridad completas, incrementales y diferenciales. Las copias de seguridad completas copian todos los datos en su totalidad, mientras que las copias incrementales solo respaldan los cambios realizados desde la última copia de seguridad y las copias diferenciales respaldan los cambios desde la última copia completa.

Es importante implementar una estrategia de copias de seguridad sólida que se adapte a las necesidades de la organización, incluido el almacenamiento seguro de las copias de seguridad, la programación regular de las mismas y las pruebas periódicas de recuperación para asegurarse de que los datos puedan ser restaurados con éxito en caso de necesidad.

También cabe mencionar que existen múltiples formas de hacer copias de seguridad como:

Simple backup

Según (Toledo Rodriguez, 2019) Simple Backup está enfocado en realizar copias de seguridad en escritorios. Puede hacer copias de archivos y directorios, y permite emplear expresiones regulares para propósitos de exclusión. Simple Backup utiliza archivos comprimidos,

lo que no es la mejor solución a grandes cantidades de datos pre comprimidos como por ejemplo archivos multimedia; sin embargo, incluye soluciones predefinidas que pueden ser usadas para hacer copias de seguridad a directorios, como **/var, /etc/, /usr/local/**. Simple Backup no está limitado a copias predefinidas, también se pueden hacer copias personalizadas, manuales y programadas (p. 3)

Box backup

Box Backup es una utilidad altamente automatizada diseñada para respaldar datos de manera completa, implementando cifrado y medidas de seguridad. Esta herramienta se basa en dos componentes esenciales: un demonio que opera en el lado del cliente y otro en el lado del servidor, respaldados por una herramienta adicional que permite la restauración de los datos.

Protección de la red

La protección de la red es un conjunto de prácticas, tecnologías y políticas diseñadas para garantizar la seguridad, integridad y disponibilidad de los sistemas, dispositivos y datos dentro de una red. El objetivo principal de la protección de la red es prevenir y mitigar amenazas cibernéticas, ataques maliciosos y brechas de seguridad que puedan afectar el funcionamiento de la red y la información almacenada en ella.

A continuación, se derivan diversas estrategias y componentes clave para la protección de la red:

- **Firewalls:** Los firewalls son dispositivos o programas que monitorean y controlan el tráfico de red entrante y saliente. Pueden filtrar el tráfico no deseado o malicioso y aplicar reglas de seguridad para proteger la red.
- **Sistemas de detección y prevención de intrusiones (IDS/IPS):** Estos sistemas monitorean la actividad de la red en busca de patrones y comportamientos sospechosos. Los IDS detectan intrusiones y alertan a los administradores,

mientras que los IPS pueden tomar medidas activas para bloquear o mitigar ataques en tiempo real.

- **Seguridad de la capa de aplicación:** Protege las aplicaciones web y los servicios expuestos en la red contra ataques como inyección de SQL, cross-site scripting (XSS) y ataques de fuerza bruta.
- **Segmentación de red:** Dividir la red en segmentos separados puede ayudar a limitar el movimiento lateral de posibles atacantes y minimizar el impacto de un ataque en toda la red.
- **Control de acceso:** Implementar autenticación y autorización sólidas para limitar quién puede acceder a los recursos de la red y qué nivel de acceso se les otorga.
- **Cifrado:** Utilizar cifrado para proteger la confidencialidad de los datos en tránsito, lo que significa que incluso si alguien intercepta el tráfico, no podrán leer la información.
- **Gestión de parches:** Mantener los sistemas y aplicaciones actualizados con los últimos parches y actualizaciones de seguridad ayuda a cerrar las vulnerabilidades conocidas.
- **Monitoreo y análisis de tráfico:** Supervisar y analizar el tráfico de red puede ayudar a detectar patrones anómalos o actividades maliciosas en tiempo real.
- **Educación y concienciación:** Capacitar a los usuarios y al personal en prácticas de seguridad cibernética y fomentar la conciencia de las amenazas puede reducir los riesgos asociados con ataques basados en ingeniería social.
- **Respuesta a incidentes:** Tener un plan de respuesta a incidentes establecido puede ayudar a mitigar el impacto de un ataque y permitir una recuperación más

rápida.

La protección de la red es un esfuerzo continuo que requiere una combinación de tecnologías, procesos y educación. Es importante evaluar y actualizar regularmente las medidas de seguridad para mantener la red protegida contra las últimas amenazas y vulnerabilidades.

Gestión de Riesgos

Para (Red Had, 2019) En el caso de la TI, los riesgos se relacionan con la posibilidad de sufrir pérdidas o daños si una amenaza aprovecha un punto vulnerable de seguridad en sus sistemas de hardware o software.

La gestión de riesgos es un proceso integral y continuo que implica identificar, evaluar y mitigar los riesgos que una empresa o entidad enfrenta en su operación, siendo eventos o situaciones que tienen un impacto negativo en los objetivos, metas o activos de la organización. Básicamente al aplicar una gestión de riesgos en un establecimiento, este busca minimizar las probabilidades de que ocurran perdidas o que se exponga la información e integridad de la empresa.

Que son vulnerabilidades

Las vulnerabilidades son debilidades o fallos en sistemas, aplicaciones, redes o procesos que podrían ser explotados por amenazas maliciosas para comprometer la seguridad de la información, causar daños o interrumpir las operaciones normales.

Según (Dured More, 2019) hace referencia a un sin número de amenazas por causas ambientales o tecnológicas que afectas a las organizaciones y sus políticas de privacidad.

¿Qué es Wireshark?

Esta es una herramienta que analiza el tráfico de red siendo una de las más populares y ampliamente utilizadas en el mundo de la seguridad informática y las redes. Ya que analiza los protocolos, donde permite a los administradores de red y profesionales de seguridad examinar el

tráfico de red en tiempo real y analizar datos capturados previamente para identificar problemas de red y detectar actividades maliciosas.

En donde (Angelov, 2021)afirma que este es un analizador de protocolos utilizado para llevar a cabo estudios y solucionar problemas en redes de comunicaciones

¿Qué es Spiceworks?

Es una plataforma de gestión de tecnología de la información (TI) que ofrece una variedad de herramientas y funciones para administrar y monitorear los recursos de TI de una organización. Su objetivo es facilitar la administración de redes, sistemas y activos tecnológicos.

MARCO METADOLOGICO

Tipo de Investigación:

Investigación descriptiva

Esta investigación ayuda a examinar las prácticas de seguridad implementadas en el Concilio Latinoamericano, la gestión de acceso a datos y los protocolos de protección, en la cual, busca proporcionar una visión clara y precisa de la situación actual en cuanto a la seguridad de la información.

Método deductivo

Este método parte de principios generales de seguridad y gestión de datos confidenciales examinando protocolos de acceso, seguridad de datos y medidas de prevención, el método deductivo revelaría las relaciones lógicas entre las prácticas implementadas y los estándares de seguridad aceptados, ayudando a identificaría riesgos y vulnerabilidades con el fin de sugerir recomendaciones para mejorar la protección de información del establecimiento.

Método Inductivo

A través del método inductivo aplicado al análisis de seguridad de la información, permitirá recopilar datos detallados sobre las prácticas y protocolos de seguridad en el Concilio Latinoamericano, permitirían observar patrones, tendencias y casos concretos relacionados con las falencias de la seguridad, en donde permitirá identificar las áreas de riesgo, deficiencias en los sistemas y puntos fuertes en la gestión de datos sensibles, para la extracción de conclusiones generales sobre el estado de la seguridad de la información en la organización.

Población y Muestra

Población

La población objetivo para este estudio está compuesta por 100 miembros activos de la comunidad del **Centro Cristiano "Concilio Latinoamericano":** Estos miembros representan una diversidad de edades, roles y niveles de participación dentro del establecimiento. la selección de esta población tiene como objetivo comprender las practicas, percepciones y necesidades de la seguridad de la información con respecto a sus donaciones, diezmos, ofrendas e información personal, siendo una muestra representativa de la comunidad en cuestión, y su participación en la investigación proporcionará información valiosa para mejorar y fortalecer la gestión de la seguridad de la información en las actividades y comunicaciones del establecimiento.

Muestra

La muestra seleccionada para este estudio se compone de 5 miembros del departamento de TIC del Centro Cristiano, estos miembros fueron elegidos debido a su conocimiento y participación activa en la gestión y manteamiento de los sistemas tecnológicos e información de la iglesia, en donde la información recopilada de esta muestra contribuirá a evaluar la eficacia actual de las medidas de seguridad y a proponer recomendaciones específicas para fortalecer la protección de los activos del establecimiento.

Formula:

Porcentaje de muestra= (Tamaño de la población/Tamaño de la muestra) ×100

En este caso:

Tamaño de la muestra = 5

Tamaño de la población = 100

Sustituyendo en la fórmula:

Porcentaje de muestra= (5/ 100) ×100=5%

Por lo tanto, la muestra representa el 5% de la población total.

Técnicas

Entrevista: La entrevista al personal del departamento de TIC se realiza para obtener su visión experta sobre la seguridad de la información en el Centro Cristino, ya que sus conocimientos permitirán identificar posibles vulnerabilidades y evaluar las prácticas actuales.

Encuesta: La encuesta fue dirigida a los miembros de la iglesia para obtener criterios referentes interrupciones o problemas que hallan tenido en el servicio que ofrece el establecimiento para comprender sus actitudes y practicas relacionadas con sucesos de inactividad del sistema web.

Observación: Esta técnica ayuda a tener una visión mas detallada de los hallazgos u herramientas que tiene el centro cristiano implementadas para la seguridad de la información del establecimiento, es decir por medio de esta técnica se podrá identificar vulnerabilidades y riesgos que se convertirían en amenazas para el establecimiento.

Metodología de gestión de riesgo

Etapas de la gestión de riesgos de la información

1. **Identificación de activos:** consiste en identificas todos los activos de la información y sistemas de tecnología de la organización que deben protegerse, incluyendo datos, aplicaciones, hardware, software, redes infraestructura y cualquier otro elemento relevante.
2. **Identificación de amenazas:** Identificar las posibles amenazas y fuentes de riesgos que podrían afectar los activos de información; estas amenazas pueden incluir ciberataques, malware, acceso no autorizado, desastres naturales, errores humanos.
3. **Evaluación de vulnerabilidades:** identificar las vulnerabilidades o debilidades potenciales en los activos de información y sistemas, es decir; agujeros de seguridad

en el software, configuraciones incorrectas p deficiencias en los procesos.

4. **Análisis de riesgos:** Evaluar la probabilidad de que las amenazas exploten las vulnerabilidades y el impacto potencial si eso sucede y aplicar valores numéricos a la probabilidad y el impacto para determinar la magnitud del riesgo.
5. **Priorización de Riesgos:** Clasificar los riesgos en función de su gravedad y probabilidad, lo que permite priorizar los esfuerzos de mitigación en los riesgos más significativos y probables.
6. **Selección de Estrategias de Mitigación:** Determinar qué enfoques se utilizarán para mitigar los riesgos identificados. Esto podría involucrar la implementación de medidas de seguridad tecnológicas, la formación del personal, la transferencia de riesgos a través de seguros, entre otros.

Para el análisis de riesgos del establecimiento se propone el siguiente esquema para el análisis y evaluación.

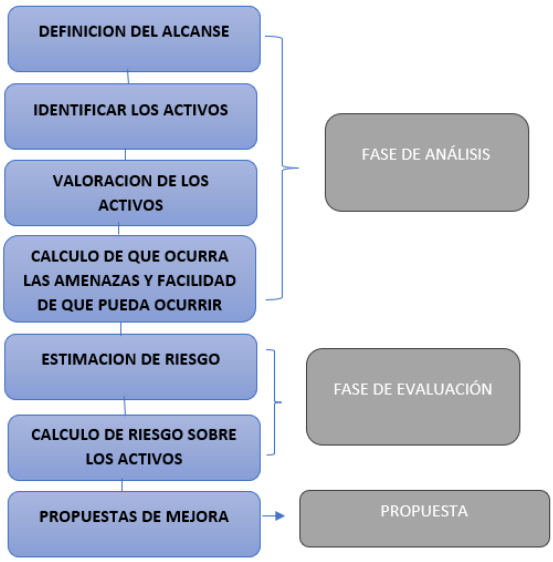


Figura 1: Metodología de análisis de riesgo propuesto.

En donde se procederá ha hacer uso de una escala del 1 al 5 en la cual cada número tendrá un significado para ser valorada las amenazas.

PARAMETROS	DEPENDENCIA FUNCIONALIDAD	INTEGRIDAD, CONFIDENCIALIDAD Y DISPONIBILIDAD
1= Muy baja	Activo con capacidades tecnológicas muy limitadas	La divulgación, modificación y no disponibilidad de este activo afecta de forma insignificante la entrega de servicios.
2= Baja	Activo con capacidades tecnológicas limitadas.	La divulgación, modificación y no disponibilidad de este activo afecta en parte la entrega de servicios.
3= Moderada	Activo con capacidades tecnológicas avanzadas	La divulgación, modificación y no disponibilidad de este activo afecta significativamente la entrega de servicios.
4= Alta	Activo con capacidades tecnológicas muy avanzadas	La divulgación, modificación y no disponibilidad este activo afecta gravemente la entrega de servicios.
5= Muy alta	Activo con capacidades tecnológicas de última generación.	La divulgación, modificación y no disponibilidad de este activo afecta totalmente la entrega de servicios.

Tabla 1: Tabla de escala de valoración Autor: David Jaña

Por consiguiente, se hace una tabla de la escala de probabilidad de ocurrencia y facilidad de explotación

Valor	Probabilidad de ocurrencia	Facilidad de explotación	Riesgo
1	Muy Baja	Insignificante o Nulo	Muy bajo * I/ nulo
2	Baja	Bajo	Bajo*bajo
3	Moderada	Moderado	Moderado*moderado
4	Alta	Alto	Alto*alto
5	Muy Alta	Catastrófico	Muy alto*catastrófico

Tabla 2: Calculo de activos Autor: David Jaña

RESULTADOS

Definición de alcance

El alcance del análisis de seguridad de la información para el Centro Cristiano "Concilio Latinoamericano" comprende a la evaluación detallada de los sistemas informáticos, bases de datos, redes y recursos tecnológicos utilizados en sus operaciones, así como la revisión de las políticas y procedimientos de seguridad establecidos, incluyendo la identificación de activos críticos de información, la evaluación de las vulnerabilidades y amenazas con la revisión de controles de acceso físico y lógico.

Identificación de los activos

Para el análisis de seguridad de la información en el centro cristiano se pudo observar los siguientes activos del establecimiento:

Activos	**Función**
Servidor	Aloja aplicaciones críticas y almacena datos.
Sistemas operativos	Sistema utilizado por los usuarios o miembros de la iglesia
Sistema web	Plataforma web para uso de miembros, feligreses y personal administrativo
Licencias de Software	Permite el uso de las aplicaciones de Microsoft en todas las estaciones de trabajo.
PC de escritorio	Utilizadas por el personal para tareas diarias.
Portátiles	Ofrecen movilidad para el personal de TIC.
Dispositivos Móviles	Proporcionan comunicaciones y acceso remoto.
Impresoras	Imprime documentos y boletines.
Escáneres	Digitaliza documentos y registros.
Dispositivo de Red	**Función**
Router	Dirige el tráfico entre redes locales y externas. Puede asignar direcciones IP y proporcionar seguridad.
Switch	Conmuta datos entre dispositivos en una red local, basándose en direcciones MAC.

Firewall	Filtra y controla el tráfico de red para proteger la seguridad de la red.
Punto de Acceso Inalámbrico	Proporciona conectividad Wi-Fi a dispositivos inalámbricos.
Modem	Convierte señales digitales en analógicas o viceversa para la conectividad de Internet.

Tabla 3: Cantidad estimada de activos del centro cristiano. Autor: David Jaña

Información Sensible	Descripción
Información de Miembros	Datos personales de los miembros de la iglesia, incluyendo nombres, direcciones, números de teléfono, fechas de nacimiento y registros de membresía.
Datos Financieros	Información financiera y registros contables, como donaciones, ingresos, gastos, cuentas bancarias y registros fiscales de la iglesia.
Correspondencia Pastoral	Comunicaciones confidenciales entre el pastor y los miembros de la iglesia, que pueden incluir consejería y asesoramiento pastoral.
Datos de Donantes	Información sobre donantes, incluyendo nombres, direcciones, historial de donaciones y preferencias de donación.
Registro de Asistencia	Registros de asistencia a los servicios religiosos y eventos de la iglesia.
Archivos de Eventos	Documentación y registros de eventos religiosos, incluyendo bodas, bautismos, confirmaciones y otras ceremonias.
Contenido Multimedia	Grabaciones de servicios religiosos, videos, música y otros contenidos multimedia utilizados en las actividades de la iglesia.
Documentos Legales	Contratos, acuerdos legales, actas de reuniones de la junta y otros documentos legales relacionados con la iglesia.
Comunicaciones Internas	Comunicaciones internas de la iglesia, incluyendo correos electrónicos, memorandos y documentos compartidos entre el personal y los líderes de la iglesia.

Tabla 4: Información sensible del centro cristiano. Autor: David Jaña

Las tablas proporcionadas reflejan una variedad de activos que tiene el centro cristiano en donde se deben tomar medidas para proteger la información tanto de sus dispositivos como la aseguración y confidencialidad de los datos que manejan en su aplicación web y fisica.

Valoración de activos

Como se muestra en la tabla 2 se procede a darle valor a los activos en caso de una mala

manipulación de los datos o daños en la información manejada en el establecimiento siendo uno de los aspectos más importantes para el análisis de la seguridad de la información.

Activo	Confidencialidad (1-5)	Integridad (1-5)	Disponibilidad (1-5)	Riesgo Total (1-15)
Servidor	5	5	5	15
Sistemas Operativos	4	4	4	12
Sistema Web	4	4	4	12
Licencias de Software	3	3	3	9
PC de Escritorio	3	3	3	9
Portátiles	3	3	3	9
Dispositivos Móviles	4	4	4	12
Impresoras	2	2	2	6
Escáneres	2	2	2	6
Router	5	5	5	15
Switch	4	4	4	12
Firewall	5	5	5	15
Punto de Acceso Inalámbrico	4	4	4	12
Modem	4	4	4	12
Información de Miembros	5	5	5	15
Datos Financieros	5	5	5	15
Correspondencia Pastoral	4	4	4	12
Datos de Donantes	4	4	4	12
Registro de Asistencia	3	3	3	9
Archivos de Eventos	3	3	3	9
Contenido Multimedia	4	4	4	12
Documentos Legales	5	5	5	15
Comunicaciones	4	4	4	12

Internas				

Tabla 5: Valoración de activos del centro cristiano. *Autor: David Jaña*

En esta tabla se procede a asignar valores de importancia e impacto a cada activo del establecimiento. En esta valoración, cada activo ha sido calificado en una escala del 1 al 5, donde 1 representa un impacto muy bajo y 5 representa un impacto muy alto en caso de explotación de amenazas.

Amenazas y riesgos de los activos

En el Centro Cristiano, se han identificado riegos que se convierten en amenazas de los activos del establecimiento que al ser explotadas afectaran la integridad de sus recursos claves, partiendo desde servidores y sistema informático hasta datos sensibles y documentos pastorales.

Como se muestra en la siguiente tabla, se destacan las amenazas y riesgos del establecimiento.

Activo	**Riesgos**	**Amenazas**
Servidor	- Pérdida de energía - Fallo de hardware - Ataques cibernéticos - Falta de respaldo de información	- Interrupciones de energía eléctrica - Fallos en componentes del servidor - Ataques DDoS, malware, ransomware
Sistemas Operativos	- Vulnerabilidades de software -Desactualización -Contraseñas débiles	- Explotación de vulnerabilidades
Sistema Web	- Vulnerabilidades de software. -Contraseñas débiles de usuarios o roles. -Falta de limitación de privilegios	- Ataques web, inyección de SQL, XSS
Licencias de Software	- Uso no autorizado -Contraseñas débiles	- Copia ilegal de software, piratería

PC de Escritorio	- Pérdida o robo -Contraseñas débiles	- Robo de hardware, pérdida de dispositivos
Portátiles	- Pérdida o robo -Contraseñas débiles	- Robo de hardware, pérdida de dispositivos
Dispositivos Móviles	- Pérdida o robo	- Robo de dispositivos móviles, malware móvil
Impresoras	- Acceso no autorizado	- Acceso no autorizado a la red
Escáneres	- Acceso no autorizado	- Acceso no autorizado a la red
Router	- Configuración incorrecta	- Configuración incorrecta, ataques de red
Switch	- Configuración incorrecta	- Configuración incorrecta, ataques de red
Firewall	- Configuración incorrecta	- Configuración incorrecta, ataques de red
Punto de Acceso Inalámbrico	- Acceso no autorizado	- Acceso no autorizado, ataques de red
Modem	- Acceso no autorizado	- Acceso no autorizado, ataques de red
Información de Miembros	- Acceso no autorizado	- Acceso no autorizado, fuga de datos
Datos Financieros	- Acceso no autorizado -Contraseñas débiles	- Acceso no autorizado, fuga de datos
Correspondencia Pastoral	- Pérdida o robo	- Pérdida de documentos, robo de información
Datos de Donantes	- Acceso no autorizado	- Acceso no autorizado, fuga de datos
Registro de Asistencia	- Acceso no autorizado	- Acceso no autorizado, fuga de datos
Archivos de Eventos	- Acceso no autorizado	- Acceso no autorizado, fuga de datos
Contenido Multimedia	- Acceso no autorizado	- Acceso no autorizado, fuga de datos
Documentos Legales	- Acceso no autorizado	- Acceso no autorizado, fuga de datos
Comunicaciones Internas	- Acceso no autorizado	- Acceso no autorizado, fuga de datos

Tabla 6: La tabla muestra los Riesgos y Amenazas que pueden ser atacadas en el centro cristiano.

Autor: David Jaña

Los riesgos identificados incluyen una variedad de amenazas potenciales, como pérdida

de energía, fallos de hardware, ataques cibernéticos, configuraciones incorrectas, acceso no autorizado y pérdida o robo físico de dispositivos y documentos. Estos riesgos pueden tener un impacto en la confidencialidad, integridad y disponibilidad de los activos, así como en la continuidad de nuestras operaciones y la reputación de nuestra organización.

Estimación de riesgo

En este punto se procede a asignar valores a las probabilidades y consecuencias de un riego en los activos del establecimiento.

Activo	**Riesgo Potencial (Escala de 1 a 5)**	**Descripción del Riesgo**
Servidor	4	Pérdida de energía, fallos de hardware, ataques cibernéticos, Falta de respaldo de información.
Sistemas Operativos	4	Vulnerabilidades de software y posibilidad de explotación, Contraseñas débiles.
Sistema Web	5	Vulnerabilidades de software y riesgos de ataques web contraseñas débiles de usuarios o roles, falta de limitación de privilegios.
Licencias de Software	2	Riesgo de uso no autorizado y piratería de software.
PC de Escritorio	3	Pérdida o robo de hardware y riesgo de acceso no autorizado.
Portátiles	3	Pérdida o robo de hardware y riesgo de acceso no autorizado.
Dispositivos Móviles	4	Pérdida o robo de dispositivos y riesgo de malware móvil.
Impresoras	2	Riesgo de acceso no autorizado a la red y configuración incorrecta.
Escáneres	2	Riesgo de acceso no autorizado a la red y configuración incorrecta.
Router	4	Configuración incorrecta y riesgo de ataques de red.
Switch	3	Configuración incorrecta y riesgo de ataques de red.
Firewall	4	Configuración incorrecta y riesgo de ataques de red.
Punto de Acceso Inalámbrico	4	Riesgo de acceso no autorizado y ataques de red.

Modem	3	Riesgo de acceso no autorizado y ataques de red.
Información de Miembros	5	Riesgo de acceso no autorizado y fuga de datos.
Datos Financieros	5	Riesgo de acceso no autorizado y fuga de datos.
Correspondencia Pastoral	3	Pérdida o robo de documentos y riesgo de acceso no autorizado.
Datos de Donantes	5	Riesgo de acceso no autorizado y fuga de datos.
Registro de Asistencia	3	Riesgo de acceso no autorizado y fuga de datos.
Archivos de Eventos	3	Riesgo de acceso no autorizado y fuga de datos.
Contenido Multimedia	4	Riesgo de acceso no autorizado y fuga de datos.
Documentos Legales	5	Riesgo de acceso no autorizado y fuga de datos.
Comunicaciones Internas	4	Riesgo de acceso no autorizado y fuga de datos.

Tabla 7: Estimación de riesgos sobre los activos. Autor: David Jaña

Esta tabla de estimación de riesgos para los activos del Centro Cristiano proporciona una evaluación detallada de los peligros a los que esta expuesto el establecimiento, en donde al ser analizados, hemos identificado áreas críticas de vulnerabilidad que requieren una atención inmediata y constante para garantizar la seguridad de la información que se maneja.

Cálculo de riesgo sobre los activos

El cálculo del riesgo se realiza con el propósito de evaluar y priorizar las amenazas potenciales para determinados activos en función de su probabilidad de ocurrencia y el impacto que tendrían si llegaran a materializarse para así poder tomar decisiones informadas sobre cómo asignar recursos y esfuerzos para mitigar los riesgos y proteger los activos del establecimiento, ya que cabe mencionar que cada uno de estos activos se involucra con la seguridad de la información.

Activo	Amenazas	Probabilidad de Ocurrencia	Facilidad de Explotación	Riesgo
Servidor	Interrupciones de energía eléctrica	Baja (2)	Media (3)	Baja-Media (5)
	Fallos en componentes del servidor	Media (3)	Alta (4)	Media-Alta (7)
	Ataques DDoS, malware, ransomware	Alta (4)	Alta (4)	Alta (8)
	Falta de respaldos de la información o perdida de datos.	Alta (4)	Muy Alta (4)	Alta (8)
Sistemas Operativos	Explotación de vulnerabilidades Falta de actualización Contraseñas débiles	Media (3)	Alta (4)	Media-Alta (7)
Sistema Web	Ataques web, inyección de SQL, XSS, contraseñas débiles.	Alta (4)	Alta (4)	Alta (8)
Licencias de Software	Copia ilegal de software, piratería	Baja (2)	Media (3)	Baja-Media (5)
PC de Escritorio	Robo de hardware, pérdida de dispositivos	Baja (2)	Media (3)	Baja-Media (5)
Portátiles	Robo de hardware, pérdida de dispositivos	Baja (2)	Media (3)	Baja-Media (5)
Dispositivos Móviles	Robo de dispositivos móviles, malware móvil	Media (3)	Alta (4)	Media-Alta (7)
Impresoras	Acceso no autorizado a la red	Baja (2)	Media (3)	Baja-Media (5)
Escáneres	Acceso no autorizado a la red	Baja (2)	Media (3)	Baja-Media (5)
Router	Configuración incorrecta, ataques de red	Baja (2)	Alta (4)	Baja-Media (6)
Switch	Configuración incorrecta, ataques de red	Baja (2)	Alta (4)	Baja-Media (6)
Firewall	Configuración	Baja (2)	Alta (4)	Baja-Media

	incorrecta, ataques de red			(6)
Punto de Acceso Inalámbrico	Acceso no autorizado, ataques de red	Baja (2)	Alta (4)	Baja-Media (6)
Modem	Acceso no autorizado, ataques de red	Baja (2)	Media (3)	Baja-Media (5)
Información de Miembros	Acceso no autorizado, fuga de datos	Alta (4)	Alta (4)	Alta (8)
Datos Financieros	Acceso no autorizado, fuga de datos	Alta (4)	Alta (4)	Alta (8)
Correspondencia Pastoral	Pérdida de documentos, robo de información	Baja (2)	Media (3)	Baja-Media (5)
Datos de Donantes	Acceso no autorizado, fuga de datos	Alta (4)	Alta (4)	Alta (8)
Registro de Asistencia	Acceso no autorizado, fuga de datos	Alta (4)	Alta (4)	Alta (8)
Archivos de Eventos	Acceso no autorizado, fuga de datos	Alta (4)	Alta (4)	Alta (8)
Contenido Multimedia	Acceso no autorizado, fuga de datos	Alta (4)	Alta (4)	Alta (8)
Documentos Legales	Acceso no autorizado, fuga de datos	Alta (4)	Alta (4)	Alta (8)
Comunicaciones Internas	Acceso no autorizado, fuga de datos	Alta (4)	Alta (4)	Alta (8)

Tabla 8: Calculo de riesgo sobre loa activos. Autor: David Jaña

Esta tabla da resultados en la escala del 1 al 8 para el Concilio Latinoamericano, donde proporciona una evaluación objetiva de las probabilidades de ocurrencia de las amenazas en los activos, en donde se procedió a realizar este cálculo sumando los resultados de las valoraciones de la probabilidad de ocurrencia y la facilidad de explotación. Identificándose de manera efectiva las amenazas más urgentes y los activos más vulnerables, en donde los valores más altos, como 7 u 8, señalan riesgos altos que requieren atención prioritaria y medidas de seguridad más sólidas.

POLÍTICA DE SEGURIDAD QUE SE PUEDEN IMPLEMENTAR

Política de Gestión de Documentos Confidenciales

Objetivo: Esta política tiene como objetivo proteger la confidencialidad e integridad de los documentos sensibles y la información relacionada con la comunidad y actividades del Centro Cristiano.

Ámbito de Aplicación: Esta política se aplica a todos los miembros del personal y voluntarios que tienen acceso a documentos y datos confidenciales.

Responsabilidades:

1. **Personal Responsable:** Todo el personal y voluntarios deben tomar medidas para proteger y gestionar adecuadamente los documentos confidenciales.
2. **Coordinador de Seguridad de la Información:** Designar a un individuo o equipo responsable de supervisar y hacer cumplir esta política.

Procedimientos:

1. **Clasificación de Documentos:** Todos los documentos deben ser clasificados según su nivel de confidencialidad: público, interno o confidencial.
2. **Control de Acceso:** Se deben establecer permisos de acceso a documentos confidenciales. Solo el personal autorizado tendrá acceso a los documentos confidenciales.
3. **Almacenamiento Seguro:** Los documentos confidenciales deben almacenarse en armarios con cerradura o sistemas de archivos digitales seguros.
4. **Transmisión Segura:** Al compartir documentos confidenciales por correo electrónico o cualquier otro medio, se debe utilizar cifrado o métodos seguros.
5. **Eliminación Segura:** La destrucción de documentos confidenciales debe realizarse a través de métodos seguros, como la trituración de papel o la eliminación segura de archivos digitales.
6. **Monitoreo y Auditoría:** Se llevará a cabo un seguimiento y auditoría regular para asegurar el cumplimiento de esta política.

Prevención de Pérdida de Datos (DLP):

- Se implementará una solución de Prevención de Pérdida de Datos (DLP) para supervisar y prevenir la fuga de información confidencial.

Incumplimiento: El incumplimiento de esta política puede resultar en medidas disciplinarias, incluyendo la terminación del empleo o la relación de voluntariado, según la gravedad del incumplimiento.

Revisiones de la Política: Esta política se revisará anualmente y se actualizará según sea necesario para garantizar su eficacia y cumplimiento.

Esta política de gestión de documentos establece directrices claras para proteger la información confidencial del Centro Cristiano y prevenir su divulgación indebida. También enfatiza la importancia de utilizar soluciones de Prevención de Pérdida de Datos (DLP) para fortalecer la seguridad de la información.

Política de Seguridad Física para Dispositivos Móviles

Objetivo: El objetivo de esta política es garantizar la seguridad de los dispositivos móviles utilizados en el Centro Cristiano y la protección de la información almacenada en ellos.

Ámbito de Aplicación: Esta política se aplica a todos los miembros del personal y voluntarios que utilizan dispositivos móviles propiedad del Centro Cristiano o dispositivos personales para acceder a la información y sistemas de la organización.

Responsabilidades:

1. **Usuarios de Dispositivos Móviles:** Todos los usuarios son responsables de seguir las directrices establecidas en esta política.
2. **Coordinador de Seguridad de la Información:** Designar a un individuo o equipo responsable de supervisar y hacer cumplir esta política.

Procedimientos:

1. **Bloqueo Automático:** Todos los dispositivos móviles deben configurarse para bloquearse automáticamente después de un período de inactividad predefinido, no superior a 5 minutos.
2. **Activación de "Buscar mi Dispositivo":** Todos los dispositivos móviles deben tener habilitada la función "Buscar mi Dispositivo" para facilitar su localización y bloqueo remoto en caso de pérdida o robo.
3. **Autenticación Fuerte:** Se requerirá autenticación segura, como contraseñas o huellas dactilares, para desbloquear los dispositivos.
4. **Información Sensible:** Los dispositivos móviles no deben utilizarse para almacenar información sensible, como datos financieros o contraseñas sin la debida protección.
5. **Notificación de Pérdida o Robo:** En caso de pérdida o robo de un dispositivo, los usuarios deben notificar de inmediato al Coordinador de Seguridad de la Información para tomar medidas de bloqueo y seguimiento.
6. **Actualizaciones de Seguridad:** Los dispositivos móviles deben mantenerse actualizados con las últimas actualizaciones de seguridad y parches proporcionados por el fabricante.

Incumplimiento: El incumplimiento de esta política puede resultar en medidas disciplinarias, incluyendo la prohibición de utilizar dispositivos móviles para acceder a la red del Centro Cristiano.

Revisiones de la Política: Esta política se revisará anualmente y se actualizará según sea necesario para garantizar su eficacia y cumplimiento.

Esta política de seguridad física para dispositivos móviles establece medidas para proteger los dispositivos y la información contenida en ellos, garantizando que estén bloqueados cuando no están en uso y que la función "Buscar mi Dispositivo" esté activada para facilitar la recuperación en caso de pérdida o robo.

Política de Contraseñas Seguras

Objetivo: El objetivo de esta política es garantizar la seguridad de las cuentas y la información del Centro Cristiano mediante la implementación de contraseñas fuertes y seguras.

Ámbito de Aplicación: Esta política se aplica a todos los miembros del personal y voluntarios que utilizan sistemas y servicios del Centro Cristiano que requieren autenticación mediante contraseña.

Responsabilidades:

1. **Usuarios:** Todos los usuarios son responsables de seguir las directrices establecidas en esta política y de crear y mantener contraseñas seguras.
2. **Coordinador de Seguridad de la Información:** Designar a un individuo o equipo responsable de supervisar y hacer cumplir esta política.

Procedimientos:

1. **Requisitos de Contraseña:** Las contraseñas deben cumplir con los siguientes requisitos:
    - Contener al menos 8 caracteres.
    - Incluir al menos una letra mayúscula y una minúscula.
    - Contener al menos un número.
    - Incluir al menos un carácter especial (¡por ejemplo, !, @, #, $, %, etc.).
    - No utilizar contraseñas obvias, como "password" o "123456".
2. **Cambio de Contraseñas:** Los usuarios deben cambiar sus contraseñas cada 90 días y no reutilizar contraseñas anteriores.
3. **Almacenamiento de Contraseñas:** Las contraseñas no deben almacenarse en lugares visibles o accesibles por otros, como notas adhesivas en el escritorio.
4. **Autenticación Multifactor (MFA):** Se promoverá el uso de la autenticación de dos factores (2FA) siempre que sea posible para añadir una capa adicional de seguridad.

Incumplimiento: El incumplimiento de esta política puede resultar en la desactivación de la cuenta del usuario hasta que se establezca una contraseña segura.

Revisiones de la Política: Esta política se revisará anualmente y se actualizará según sea necesario para garantizar su eficacia y cumplimiento.

Esta política de contraseñas seguras establece directrices claras para la creación y el mantenimiento de contraseñas robustas, garantizando que las cuentas y la información del Centro Cristiano estén protegidas contra accesos no autorizados.

DISCUSION DE RESULTADOS

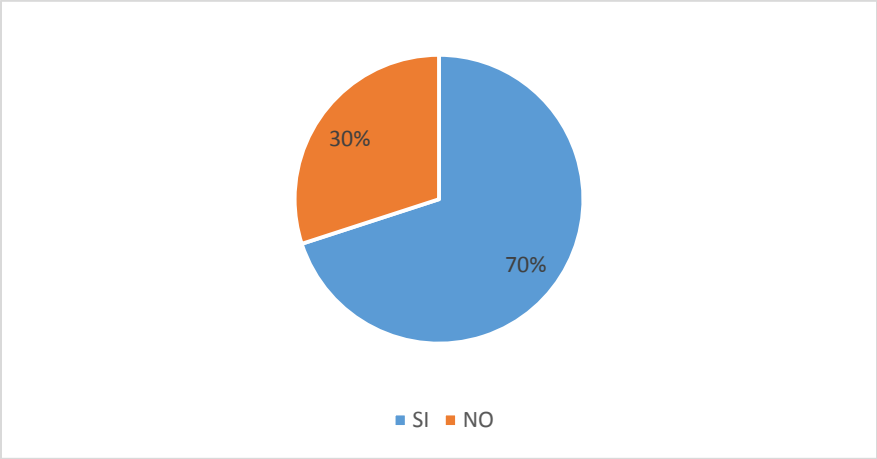
Encuestas dirigidas al personal: Con respecto a las encuestas realizadas al personal que labora en el concilio latinoamericano se expresaron criterios de inconsistencia de seguridad en el establecimiento tanto en la parte lógica como física, existiendo falencias de políticas de seguridad claras y estables para que la información sea más resguardada o reforzada teniendo una valoración negativa con respecto a este ámbito.

Entrevista con el encargado del establecimiento: Al entrevistar al encargado del departamento de TIC, se pudo notar que existen falencias con respecto a tener un enfoque integral de la seguridad de la información, en la cual se puede beneficiar implementando políticas de acceso más sólidas para mejorar la protección de los datos confidenciales de la organización, para que no ocurran incidentes graves en la manipulación de la información que maneja, ya que a pesar que tenga departamentos pequeños y pocos dispositivos, esta institución maneja mucha información de las diferentes iglesias y de la comunidad a la que pertenece.

Criterio propio: Con los resultados de las herramientas implementadas como Wireshark, Spiceworks y con ayuda de la técnica de la observación se pudo se determina que en el análisis realizado en el centro cristiano revelo brechas en la seguridad de la información del establecimiento, en la cual se deben tomar medidas para solventar estos agujeros, ya que representan un alto riego en los activos, donde se hace necesario que la organización tenga un enfoque holístico de seguridad de la información que incluya políticas de seguridad, medidas técnicas y capacitación para el personal , para poder disminuir los riesgos y amenazas que se presentan.

1. ¿Utilizas dispositivos electrónicos personales (como computadoras, teléfonos móviles, tabletas) para actividades relacionadas con la iglesia?

	FRECUENCIA	%
SI	70	70%
NO	30	30%
		100%

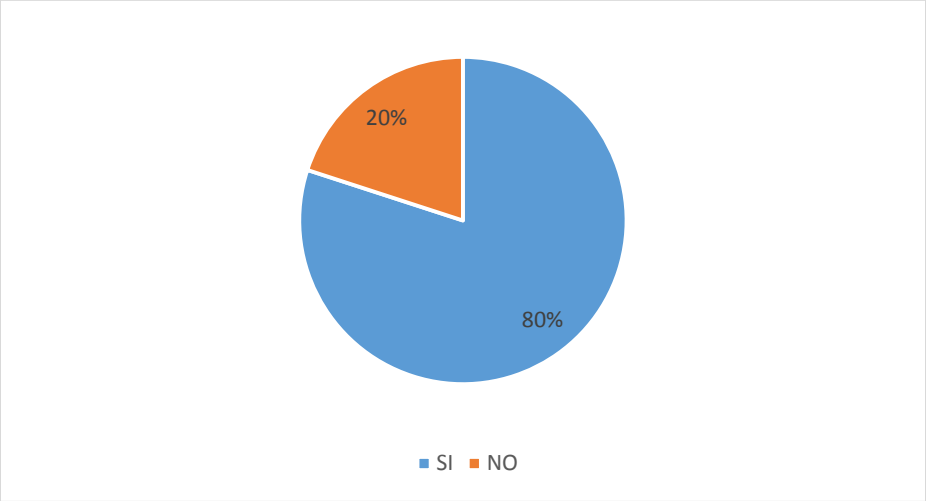


ANALISIS

La mayoría de los encuestados (70%) utilizan dispositivos electrónicos personales para actividades relacionadas con la iglesia. Esto sugiere que la tecnología desempeña un papel importante en la participación de los miembros de la iglesia en sus actividades.

2. ¿Ha experimentado alguna interrupción en los servicios del Concilio Latinoamericano como lentitud al abrir el sistema en determinados tiempos de uso en los últimos 12 meses?

	FRECUENCIA	%
SI	80	80%
NO	20	20%
		100%

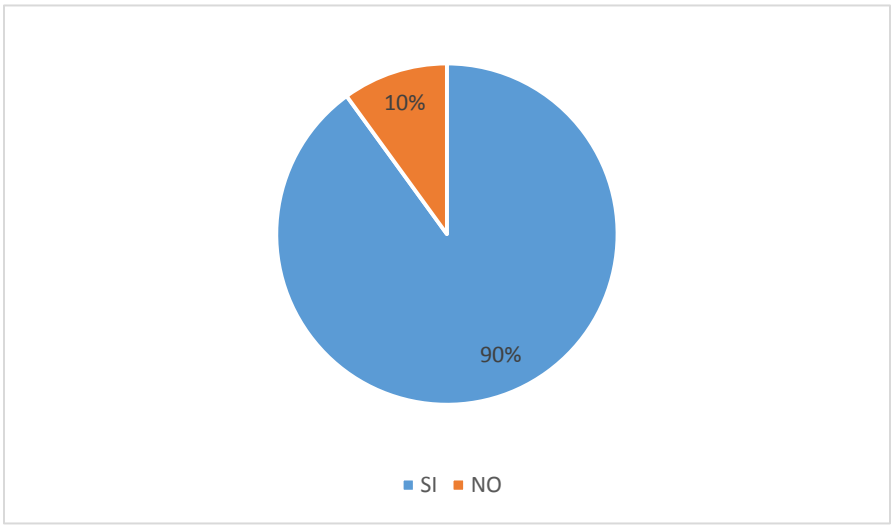


ANALISIS

Un número significativo de encuestados 80% informa haber experimentado interrupciones en los servicios del Concilio Latinoamericano en los últimos 12 meses. Esto indica que existe una preocupación sobre la calidad y la disponibilidad de los servicios tecnológicos proporcionados por la organización.

3. ¿Crees que es importante que la iglesia comunique y eduque a los miembros sobre prácticas seguras de manejo de la información?

INDICADOR	FRECUENCIA	%
SI	90	90%
NO	10	10%
TOTAL		100%

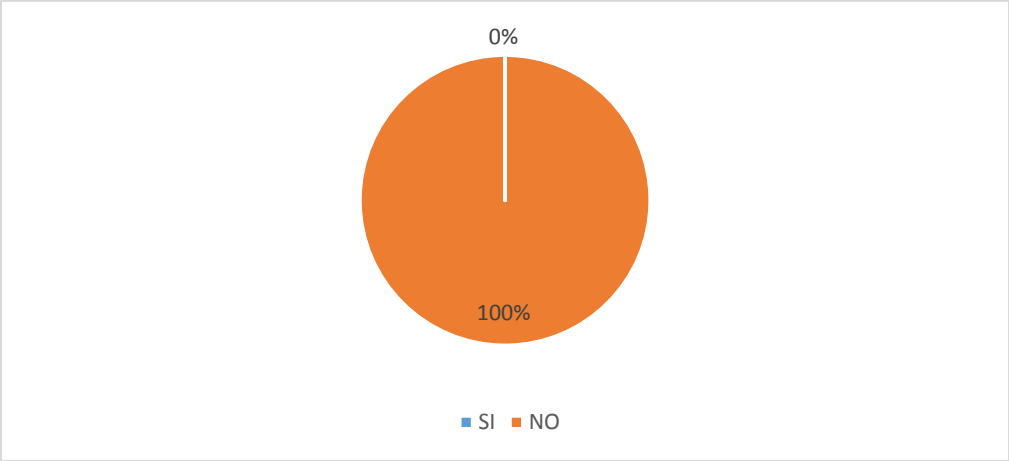


ANALISIS

La gran mayoría de los encuestados (90%) considera importante que la iglesia comunique y eduque a los miembros sobre prácticas seguras de manejo de la información. Esto muestra una fuerte conciencia de la importancia de la seguridad de la información en la comunidad eclesiástica

4. ¿Crees que se están tomando las medidas adecuadas para proteger la información de la iglesia y sus miembros?

	FRECUENCIA	%
SI	0	0%
NO	100	100%
TOTAL		100%



ANALISIS

Aquí se presenta una preocupación significativa, ya que el 100% de los encuestados no cree que se estén tomando medidas adecuadas para proteger la información de la iglesia y sus miembros. Esto indica una falta de confianza en la seguridad de los datos dentro de la iglesia y sugiere la necesidad de mejorar las políticas y prácticas de seguridad de la información.

5. ¿Te sientes seguro/a de que la información que compartes con la iglesia se maneja de manera confidencial y segura?

INTERVALO	FRECUENCIA	%

SI	0	0%
NO	100	100%
TOTAL		100%

ANALISIS

El 100% de los encuestados no se siente seguro/a de que la información que comparte con la iglesia se maneje de manera confidencial y segura. Esto es una señal de una falta significativa de confianza en la gestión de la información por parte de la iglesia y subraya la importancia de abordar esta preocupación de manera urgente.

ENTREVISTA

1. ¿**Cómo se aseguran de que los datos sensibles no sean accesibles por personal no autorizado?**

   En base a la seguridad de la información no tenemos políticas que implementen o restrinjan información del concilio, hasta el día de hoy no hemos tenido problemas a ese nivel, pero para el acceso a al sitio web se cuenta con contraseñas.

2. **¿Se les brinda información sobre cómo pueden reportar posibles vulnerabilidades o incidentes de seguridad?**

   No, tenemos ninguna manera de reportar este incidente, ya que somos miembros activos de la iglesia, pero parcialmente.

3. **¿Sabe que son los ataques de denegación de servicios?**

   Sí, estoy familiarizado con lo que son los ataques de denegación de servicios, son para interrumpir o hacer inaccesible un servicio en línea, como un sitio web o una red, al abrumarlo con una cantidad abrumadora de tráfico falso o solicitudes.

4. **¿Qué herramientas o tecnologías se implementan para garantizar la seguridad de la información?**

   En algunas ocasiones, hemos utilizado un firewall básico para controlar el tráfico de red. Sin embargo, hemos experimentado limitaciones en su capacidad para detectar amenazas más avanzadas

5. **¿Cuál es el proceso de respaldo y recuperación de datos en caso de un desastre o**

pérdida de información?

Nuestro proceso de respaldo actual implica la copia de archivos en unidades externas de almacenamiento de forma periódica. Sin embargo, reconocemos que esta práctica puede resultar insuficiente en situaciones de desastre o pérdida de información a gran escala

6. **¿Existen políticas específicas de seguridad de la información en el Centro Cristiano?**

   No, en este momento no contamos con políticas específicas de seguridad de la información establecidas en el Centro Cristiano "Concilio Latinoamericano". Reconocemos la importancia de implementar estas políticas para garantizar la protección adecuada de la información.

CONCLUSIÓN

Las respuestas de las encuestas indican una gran necesidad de mejorar la seguridad de la información en el Concilio Latinoamericano ya que los miembros manifiestan frecuentes interrupciones de los servicios en línea y la falta de confianza de los miembros en las medidas de seguridad existentes plantean desafíos.

Además, también se evidencia que hay brechas entre la conciencia de la importancia de la seguridad de la información y la percepción de que se están tomando medidas adecuadas resalta la urgencia de abordar estos problemas.

Por otro lado, los resultados de la entrevista revelan una serie de preocupaciones en cuanto a la seguridad de la información en la institución. ya que resalta áreas de vulnerabilidad evidentes. Además, la falta de herramientas avanzadas de seguridad, como un firewall efectivo, plantea riesgos potenciales y por ende el proceso de respaldo y recuperación de datos también es insuficiente en caso de desastres o pérdida de información a gran escala, en otras palabras, hace necesario implementar medidas más sólidas de seguridad de la información y establecer políticas claras para proteger los datos sensibles.

Para finalizar como resultado del estudio al analizar la seguridad de la información realizado en el Centro Cristiano "Concilio Latinoamericano" ha arrojado una visión detallada de los activos involucrados, así como de las amenazas y riesgos que estos enfrentan.

Estos activos se han sometido a una valoración cuidadosa en términos de confidencialidad, integridad y disponibilidad, utilizando una escala del 1 al 5, también, se ha calculado el riesgo potencial en función de la probabilidad de ocurrencia y el impacto que tendrían las amenazas en cada uno de los activos, en donde, este análisis destaca la necesidad de implementar políticas de seguridad de la información, así como medidas de seguridad técnicas y organizativas para salvaguardar los activos del Centro Cristiano "Concilio Latinoamericano".

La gestión de riesgos se convierte en un aspecto fundamental para proteger la información y garantizar la continuidad de las operaciones de la institución en un entorno cada vez más desafiante desde el punto de vista de la seguridad informática.

RECOMENDACIONES

Basadas en los hallazgos presentados en el caso de estudio, se proponen las siguientes recomendaciones para fortalecer la seguridad de la información en el centro cristiano "Concilio Latinoamericano":

- Establecer políticas y procedimientos sólidos de seguridad de la información que aborden la gestión de contraseñas, el acceso autorizado, la retención de datos y la clasificación de información sensible. Estas políticas deben ser comunicadas y capacitadas para todo el personal y miembros relevantes de la iglesia.
- Mantener actualizados los sistemas operativos, aplicaciones y software utilizado en la organización para mitigar vulnerabilidades conocidas. Esto incluye la implementación de parches de seguridad y actualizaciones regulares.
- Establecer una estructura de limitación de privilegios basada en roles para el personal, lo que garantiza que cada usuario tenga acceso solo a la información necesaria para realizar sus funciones. Además, promover cambios regulares de contraseñas y el uso de contraseñas fuertes.
- Configurar y monitorear adecuadamente dispositivos de red como routers, switches e implementar firewalls para prevenir accesos no autorizados y ataques. Esto incluye la revisión regular de las configuraciones de seguridad de la red.
- Implementar un sistema de respaldo robusto y periódico que garantice la disponibilidad y protección de la información valiosa, y por ende realizar pruebas de recuperación para verificar la eficacia de los respaldos.
- Implementar sistemas de monitoreo y detección de amenazas para identificar actividades sospechosas o intentos de intrusión como, sistema de detección de intrusiones en red, este monitorea el tráfico de red en busca de patrones de actividad sospechosa o maliciosa y

alerta sobre intrusiones. sistema de detección de intrusiones en el host ejecutándose en dispositivos individuales (servidores o estaciones de trabajo) para detectar actividades inusuales a nivel del sistema operativo y aplicaciones o sistema de análisis de comportamiento de usuarios (UEBA): Examina el comportamiento de usuarios y sistemas en busca de desviaciones de las normas normales que podrían indicar actividades maliciosas.

- Mejorar la seguridad física de los dispositivos y equipos críticos, como servidores y dispositivos de red, para prevenir robos y daños físicos.
- Desarrollar un plan de respuesta a incidentes que incluya procedimientos detallados para manejar situaciones de seguridad, notificar a las partes relevantes y tomar medidas correctivas.
- Realizar auditorías de seguridad regulares para evaluar la efectividad de las políticas y procedimientos de seguridad de la información y garantizar el cumplimiento de las normativas aplicables.
- Proporcionar capacitación continua en seguridad de la información a todo el personal y miembros de la iglesia, asegurando que estén al tanto de las últimas amenazas y medidas de seguridad.
- Instalar sistemas UPS que permiten que los servidores y sistemas críticos sigan funcionando durante cortes eléctricos para que los servicios en línea no se vean interrumpidos.
- Realización de mantenimiento preventivo regular en los servidores, como limpieza interna y reemplazo de ventiladores desgastados, para evitar fallos inesperados.
- Utilización de un servicio de mitigación de DDoS que detecta y bloquea automáticamente el tráfico malicioso durante un ataque para mantener la disponibilidad del sitio web.

- Utilización de un firewall de aplicaciones web (WAF) que inspecciona y filtra el tráfico web para proteger contra ataques como inyección de SQL y XSS.
- Adquisición de licencias legítimas de software de productividad en lugar de utilizar versiones pirateadas o copias ilegales.
- Implementación de políticas de seguridad física que requieren que los dispositivos se bloqueen cuando no están en uso y la activación de la función "Buscar mi dispositivo" en dispositivos móviles.
- Implementación de políticas de gestión de documentos que establecen quién tiene acceso a documentos sensibles y la utilización de soluciones de prevención de pérdida de datos (DLP) para evitar que la información confidencial se comparta indebidamente.

BIBLIOGRAFÍA

Angelov, M. I. (2021). *Análisis de paquetes con Wireshark.* Retrieved 13 de 09 de 2023, from https://riunet.upv.es/bitstream/handle/10251/174236/Mitkov%20-%20Analisis%20de%20paquetes%20con%20Wireshark%20estudio%20de%20vulnerabilidades.pdf?sequence=1&isAllowed=y

Barker c., W., Fisher, W., Scarfone, K., y Souppaya, M. (Febrero de 2022). *Gestión de riesgo de ransomware.* Retrieved 14 de 08 de 2023, from Un perfil de marco de ciberseguridad: https://nvlpubs.nist.gov/nistpubs/ir/2022/NIST.IR.8374.spa.pdf

Benedetti, A., y Renoldi, B. (2022). *Seguridad*. Retrieved 7 de 8 de 2023, from https://www.teseopress.com/palabrasclavefronteras/chapter/seguridad/#:~:text=La%20seguridad%20puede%20considerarse%20como,Libre%20y%20exento%20de%20riesgo%E2%80%9D.

Dured More, A. D. (2019). *EVALUACIÓN DE TÉCNICAS DE ETHICAL HACKING PARA EL DIAGNÓSTICO DE VULNERABILIDADES DE LA SEGURIDAD INFORMATICA EN UNA EMPRESA PRESTADORA DE SERVICIOS.* Retrieved 28 de 08 de 2023, from https://repositorio.uss.edu.pe/bitstream/handle/20.500.12802/7359/Durand%20More%2c%20Andrés%20David.pdf?sequence=1&isAllowed=y

ESQUEMA NACIONAL DE SEGURIDAD. (3 de Mayo de 2022). *LEGISLACIÓN CONSOLIDADA*. Retrieved 28 de 07 de 2023, from https://www.boe.es/buscar/pdf/2022/BOE-A-2022-7191-consolidado.pdf

Gonzalez Manzano, L., Bautista Rosell, J., y Covadonga Gijon. (Octubre de 2019). *Ataques DDoS con IoT, Análisis y Prevención de Riesgos.* Retrieved 14 de 08 de 2023, from https://e-archivo.uc3m.es/bitstream/handle/10016/29630/TFG_Javier_Bautista_Rosell.pdf?sequence=1&isAllowed=y

ISO/IEC 27701. (2019). *Organizacion de certificacion global*. Retrieved 7 de 8 de 2023, from https://www.nqa.com/es-es/certification/standards/iso-27701#:~:text=La%20ISO%2FIEC%2027701%3A2019,requisitos%20de%20privacidad%20de%20datos.

Mantilla, C., Borona, L., Valdivieso, A. L., y Benalcazar , M. (Feb de 2023). *Arquitectura de Medición del Impacto de Ataques DoS en QoS/QoE de Servicios Multimedia en Redes SDN.* Retrieved 14 de 08 de 2023, from https://www.proquest.com/openview/73b9743edad126b9e8b6af18dca57952/1?pq-origsite=gscholar&cbl=1006393

Red Had. (10 de 2019). *Gestion de Riesgos*. Retrieved 28 de 08 de 2023, from https://www.redhat.com/es/topics/management/what-is-risk-management

Sanchez, T. (23 de Nov de 2021). *Linkedin*. Retrieved 14 de 08 de 2023, from La importancia de la gestión de parches y la actualización de las TI para recudir los riesgos de seguridad:

https://es.linkedin.com/pulse/la-importancia-de-gesti%C3%B3n-parches-y-actualizaci%C3%B3n-las-toni-sanchez

Santana, C., F, W., Pico Pionce, y Efrain. L. (23 de Octubre de 2019). *Apuntes teoricos introductorios sobre la seguridad de la infromacion.* Retrieved 7 de 8 de 2023, from https://dialnet.unirioja.es/servlet/articulo?codigo=6174477

Segovia Cando, R. M., y Chicaiza Medina, P. R. (2021). Prevención en ciberseguridad enfocada a los procesos de infraestructura tecnológica. *10*(1), 17-41. Retrieved 14 de 08 de 2023, from Prevencion en ciberseguridad enfocada a los procesos de infraestructura tecnologica: https://dialnet.unirioja.es/servlet/articulo?codigo=7888164

Toledo Rodriguez, M. (24 de Junio de 2019). *Módulo para la gestión de copias de seguridad en Nova 360.* Retrieved 14 de 08 de 2023, from https://repositorio.uci.cu/bitstream/123456789/10098/1/TD_09445_19.pdf

Valencia Duque, F. J. (2019). *Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000.* Retrieved 7 de 8 de 2023, from https://pdfs.semanticscholar.org/ff97/978e09c5bc3f1ca826017e9f34490d4e5c19.pdf

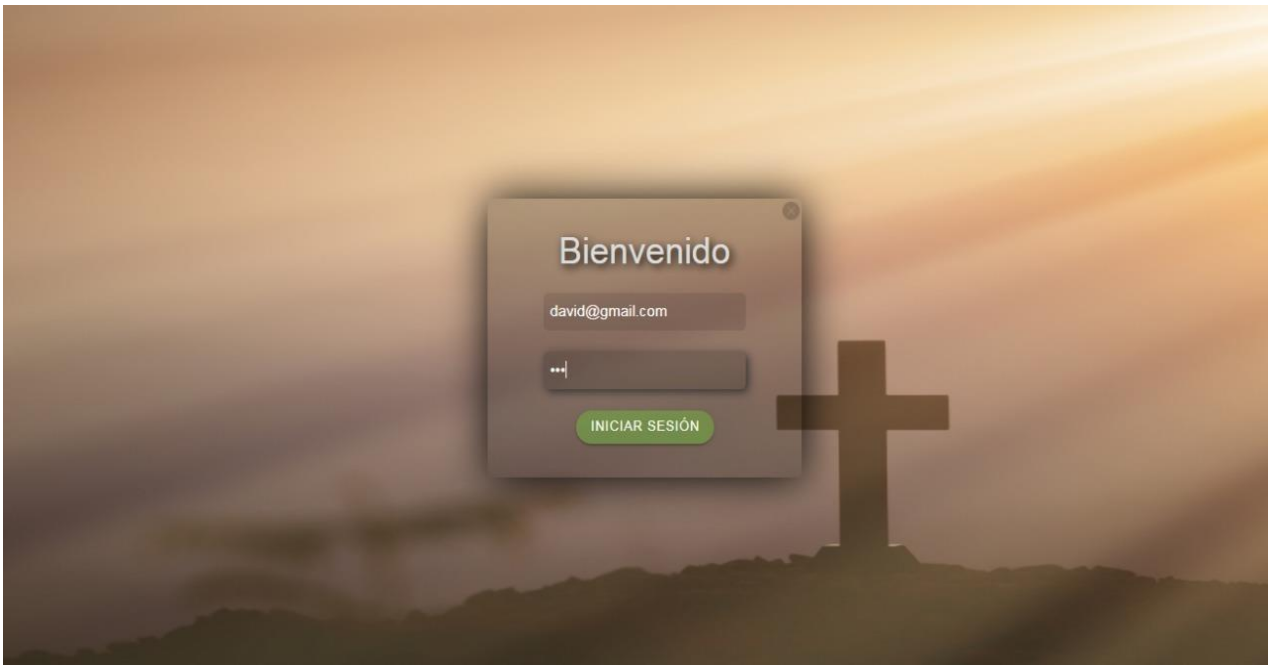
Vega Briceño, E. (03 de 2021). *Seguridad de la infromacion.* Retrieved 7 de 8 de 2023, from https://www.3ciencias.com/wp-content/uploads/2021/03/LIBRO-SEGURIDAD-INFORMACIO%CC%81N.pdf

Vega Velasco, W. (2018). *Politicas de seguridad*. Retrieved 7 de 08 de 2023, from http://www.scielo.org.bo/pdf/rfer/v2n2/v2n2a08.pdf

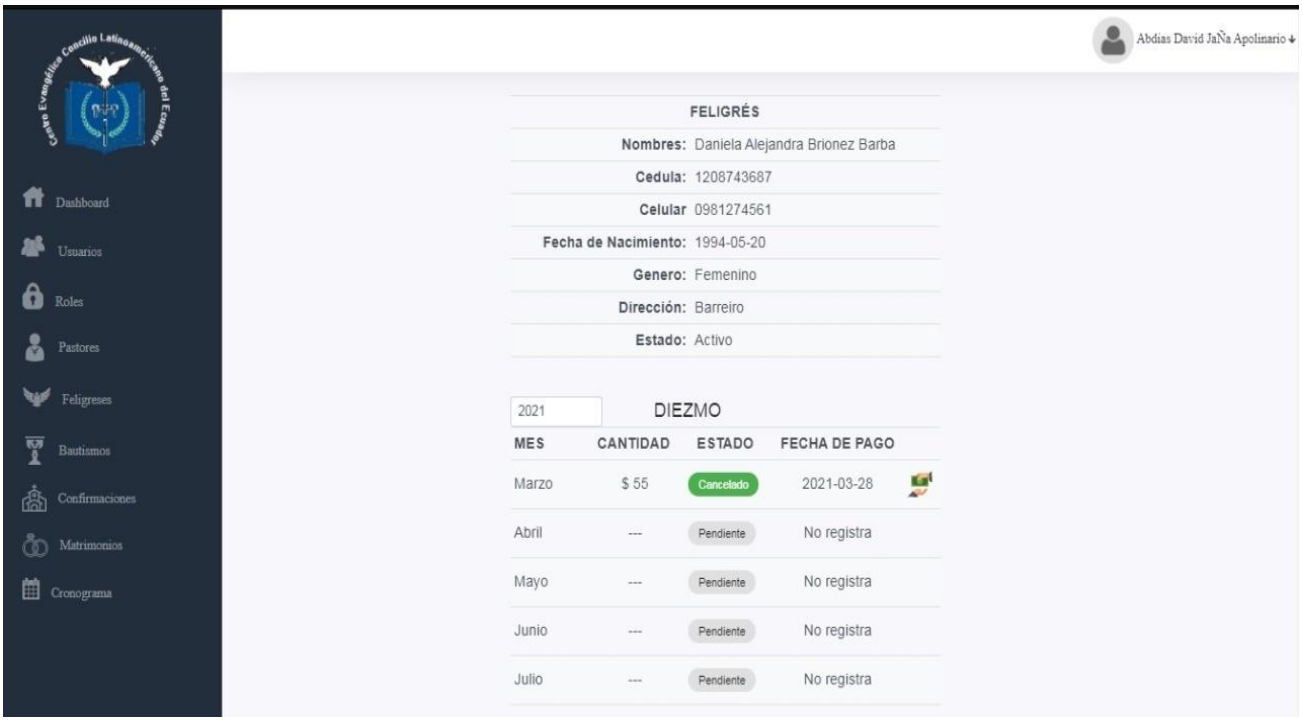
ANEXOS


Anexo 1: Entrevista, encargado principal del departamento TIC.


Anexo 2: Servidores del departamento de TIC.



Anexo 3: capturas del sistema web del establecimiento.



Anexo 4: parámetros y controles Financieros

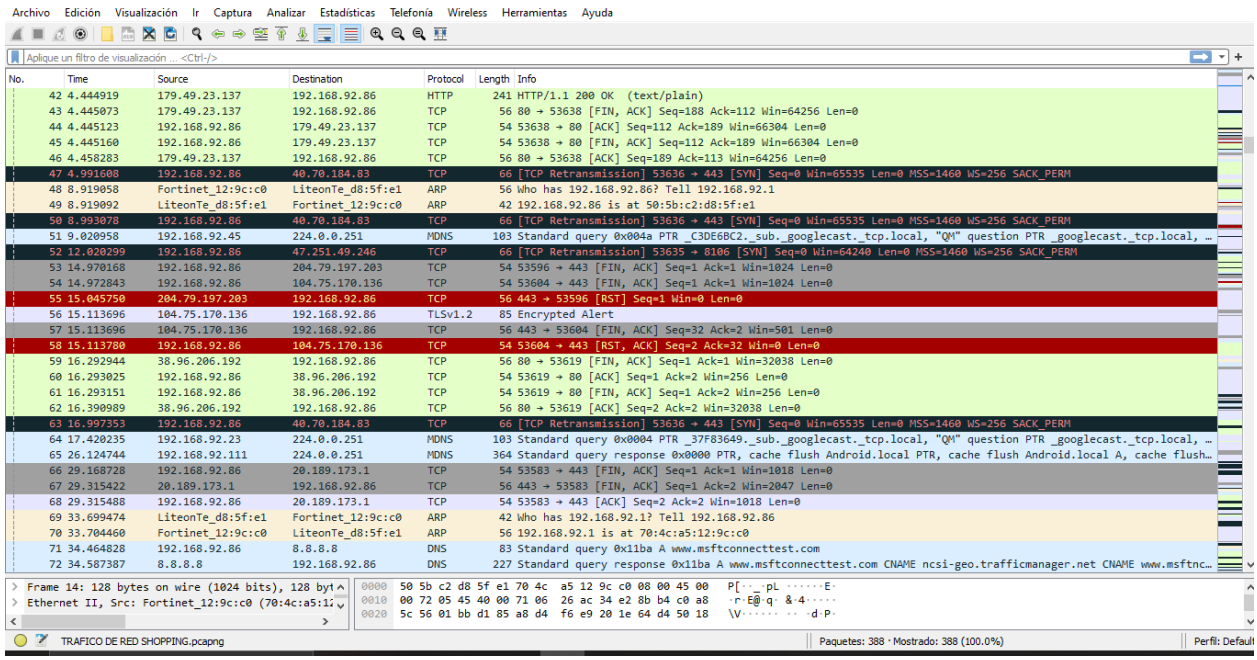
CENTRO EVANGELICO CONCILIO LATINOAMERICANO DEL ECUADOR
EMAIL: conciliolecuador@gmail.com
Telefax: 052732244 ext.-114

FELIGRES:

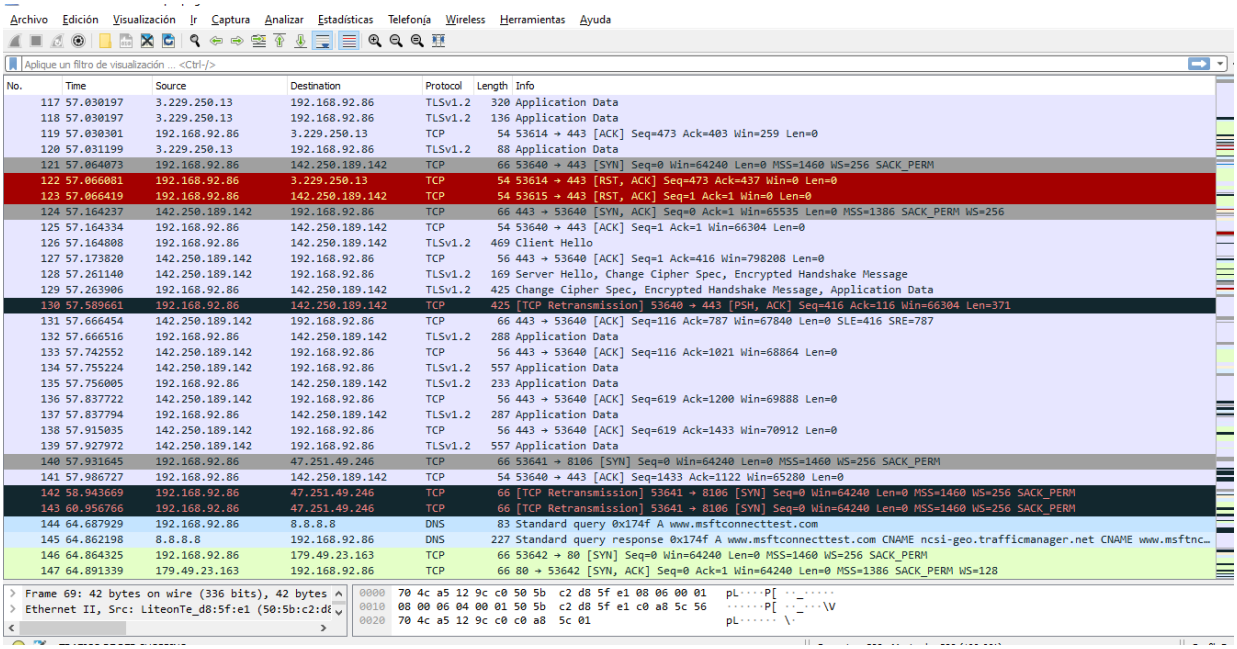
Nombres: Lisbeth Dayana Baños Galeas
Cedula: 1209873423
Celular: 0981277467
Genero: Femenino
fecha de Nacimiento: 04/02/1987

DIEZMO DEL AÑO 2021				
#	Mes	Cantidad	Fecha de Pago	Estado
1	Abril	50	01/04/2021	Cancelado
2	Mayo	----	No registra	Pendiente
3	Junio	----	No registra	Pendiente
4	Julio	----	No registra	Pendiente
5	Agosto	----	No registra	Pendiente
6	Septiembre	----	No registra	Pendiente
7	Octubre	----	No registra	Pendiente
8	Noviembre	----	No registra	Pendiente
9	Diciembre	----	No registra	Pendiente

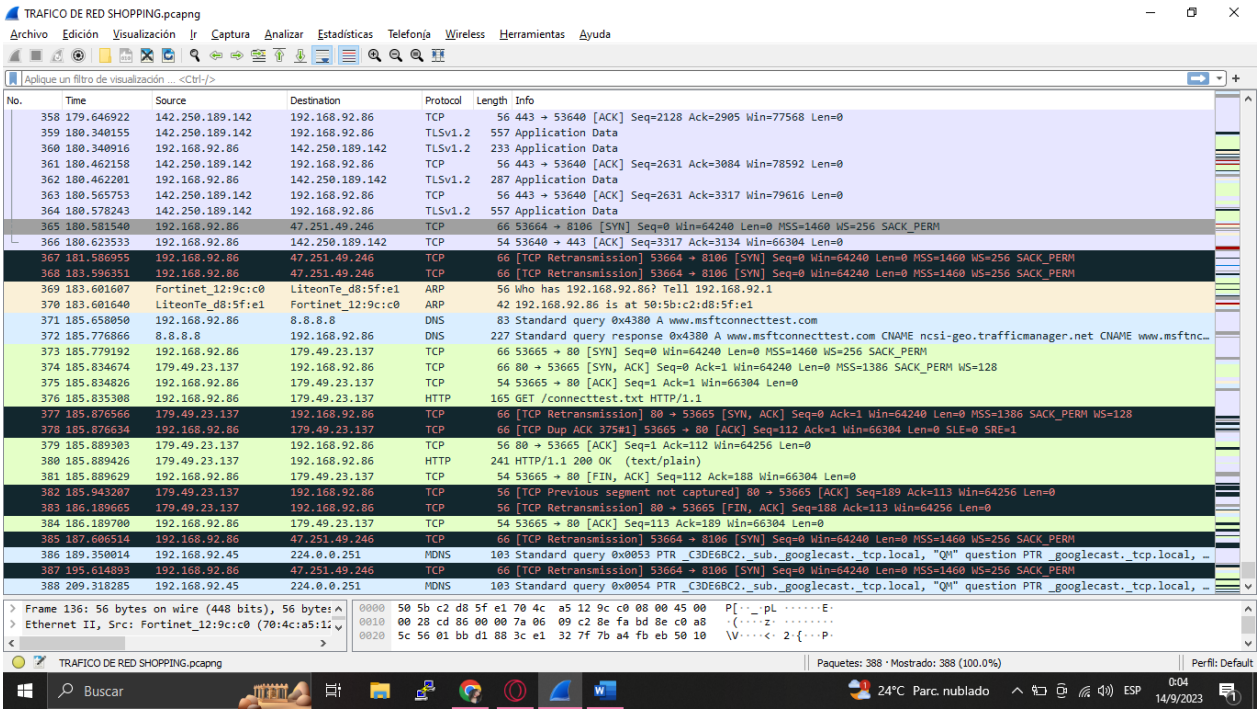
Anexo 5: reportes financieros.



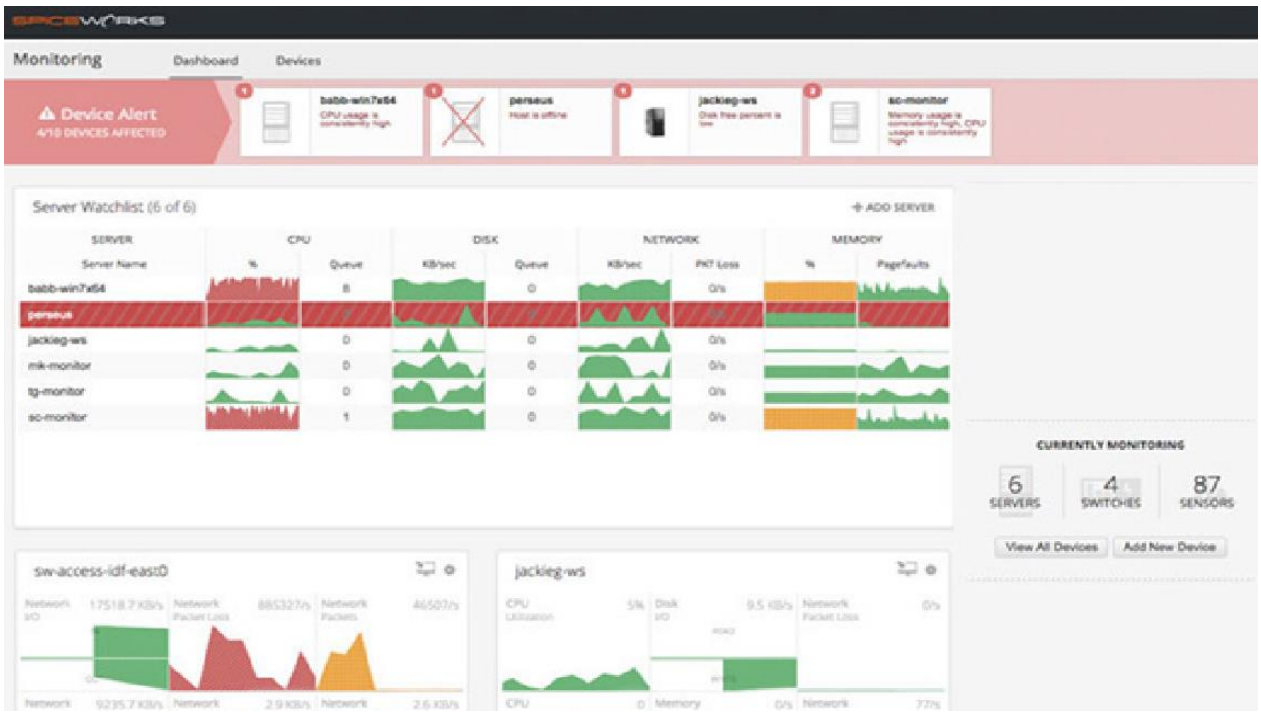
Anexo 6: Captura del trafico de red con la herramienta Wireshark y posibles riesgos.



Anexo 7: Captura wireshark.



Anexo 8: Captura wireshark.



Anexo 9: Monitoreo de los equipos.