Universidad Católica de Honduras

“Nuestra Señora Reina de la Paz”

Propuesta Análisis y Evaluación de Riesgo - Entregable Final

World Vision/Programa Integrado Lenca

Equipo 3

Asignatura: Seguridad Informática y Gestión de Riesgo (IF360)

Sección: 1501

Catedrático: Ing. Blanca Patricia Medina Hernandez

28 de Julio 2022

Integrantes

Nombre	No. de Cuenta
Andrea Saroginny Montalvo Castro	0801-2000-21834
Yessy Danira Tinoco Vasquez	1305-2002-00353
Hacknel Alexis Reyes	1001–2001-00363
Oscar Josué Mejía Serén	1001-2002-00094

Índice

Objetivos

Objetivo General

- Desarrollar un análisis de seguridad informática en la institución “World Vision/Programa Integrado Lenca”, identificando dentro de sus actividades cotidianas, aquellas que requieren la utilización de sistemas o elementos informáticos de forma directa o indirecta, así como los riesgos a los que están expuestos, con el fin de mejorar la seguridad y la integridad de los datos implementando la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT).

Objetivos Específicos

- Planificar un estudio de seguridad informática para la institución World Vision/Programa Integrado Lenca.
- Identificar el equipo y otros activos informáticos con los que cuenta la institución actualmente.
- Realizar la valoración de los activos informáticos de la institución.
- Identificar las amenazas a las que la institución se expone mediante sus actividades con elementos informáticos.
- Describir las consecuencias que las amenazas pueden representar para la información que se maneja.
- Brindar opciones de mejora o soluciones ante las amenazas que se detectaron, así como detallar las prácticas que pueden impulsar a la institución a tener un mejor entorno de seguridad informática.
- Realizar cada etapa de este proyecto implementando las directrices establecidas por la metodología MAGERIT.

Planteamiento del Problema

Los sistemas informáticos son una realidad con la cual las personas interactuamos de forma cotidiana. Las instituciones obtienen beneficios notables en el desarrollo de sus actividades con el uso e implementación de este tipo de sistemas o elementos computacionales. Tiempo atrás, este tipo de tecnologías no estaban tan presentes en nuestras sociedades como lo son hoy en día. Debido a esto, la seguridad informática no era un tema del cual habría que preocuparse. Sin embargo, así como la adopción de la tecnología ha crecido de forma rápida, las distintas amenazas o factores de riesgo también lo han hecho. Actualmente, se desarrollan miles de problemas informáticos que pueden afectar negativamente a cualquier entidad

Cuando se presenta un incidente que afecta a los sistemas o elementos informáticos, pueden desarrollarse eventos que, dependiendo de la naturaleza del suceso, podrían generar pérdidas graves de datos o información, filtración, robo o publicación de detalles confidenciales, interrupción indefinida de los servicios informáticos, daños físicos a los equipos, entre muchas otras consecuencias. Algunas de estas, pueden afectar negativamente a la economía de la institución, así como a su imagen ante la sociedad.

World Vision/Programa Integrado Lenca, al ser una empresa que maneja grandes cantidades de información y que la misma es fundamental para el desarrollo óptimo de sus actividades cotidianas, debe contar con un entorno informático seguro, donde cualquier amenaza o riesgo sea controlado, garantizando así la confiabilidad, disponibilidad e integridad de la información. Existe una gran cantidad de prácticas o metodologías que tienen como objetivo mitigar o eliminar completamente aquellas vulnerabilidades y amenazas a las cuales está expuesto el equipo de cómputo. La importancia de mantener la seguridad informática en óptimas condiciones puede servir de mucho a la institución a corto y largo plazo ante las amenazas conocidas, como las desconocidas.

Justificación

Cada día, nuevas vulnerabilidades son descubiertas en los sistemas informáticos o software en general que se utiliza para el desarrollo de actividades cotidianas. De la misma manera, personas cuyo objetivo es infiltrarse en las organizaciones para robar información sensible, idean y desarrollan nuevas y sofisticadas técnicas para lograr su cometido. La lucha contra este tipo de agentes debe ser algo a tomar muy en cuenta en cualquier organización. Es aquí donde resalta la importancia de desarrollar un entorno seguro para todas las actividades empresariales que involucren factores informáticos.

La información que circula a diario en los medios informáticos dentro de la empresa a estudiar es de suma importancia, por lo que mantenerla íntegra, disponible y confiable es un aspecto fundamental. De no suceder lo anterior, muchas actividades que requieren de los datos pueden verse seriamente afectadas, generando consecuencias aún más grandes que puedan afectar incluso a otras entidades de forma indirecta.

Desarrollar las actividades productivas de la institución en un entorno informático seguro, agrega valor extra a lo que se ofrece al público o las personas relacionadas con las actividades, así como a los procesos internos de la misma. Esto genera a su vez, una mejor imagen a los involucrados, como a la institución en general.

Marco Conceptual

Seguridad informática

Seguridad informática también llamada “ciberseguridad” es cualquier medida que impida la ejecución de operaciones no autorizadas sobre un sistema o red informática, cuyos efectos puedan conllevar a daños sobre la información, comprometer su confidencialidad, autenticidad o integridad, disminuir el rendimiento de los equipos o bloquear el acceso de usuarios autorizados.

Análisis de Riesgos

Un análisis de riesgo es la apreciación detallada de todo lo que pueda implicar peligro para la empresa. Es decir de cualquier detalle que pueda causar un inconveniente sea financiero o funcional. Una metodología de análisis de riesgos es un procedimiento mediante el cual se realiza un análisis de riesgo para conocer sus causas y consecuencias. Es organizar toda la información necesaria que sirva de lumbrera para saber si la situación es conveniente o no para la empresa.

Amenazas

Una amenaza se puede definir entonces como un evento que puede afectar los activos de información y están relacionadas con el recurso humano, eventos naturales o fallas técnicas. Algunos ejemplos pueden ser ataques informáticos externos, errores u omisiones del personal de la empresa, infecciones con malware, terremotos, tormentas eléctricas o sobrecargas en el fluido eléctrico.

Medidas de seguridad o salvaguardas

Una medida de seguridad o salvaguarda es cualquier medio empleado para eliminar o reducir un riesgo. Su objetivo es reducir las vulnerabilidades de los activos, la probabilidad de ocurrencia de las amenazas y/o el nivel de impacto en la organización.

Riesgos

Los riesgos son la probabilidad de que una amenaza se materialice sobre una vulnerabilidad del sistema informático, causando un determinado impacto en la organización. El nivel de riesgo depende del análisis previo de vulnerabilidades del sistema, de las amenazas y del posible impacto que estas puedan tener en el funcionamiento de la organización.

SGSI

El sistema de seguridad de la información o SGSI (Information Security Management System) tiene como objetivo evaluar todos los riesgos asociados con los datos e información que se manejan en una empresa. El SGSI es un elemento fundamental de la norma internacional ISO 27001 (Sistemas de Gestión de la Seguridad de la Información), que persigue asegurar la integridad y confidencialidad de los datos y los sistemas encargados de procesarlos.

Las empresas que obtienen el certificado ISO 27001 se diferencian por su tratamiento seguro y preciso de todos los datos que manejan y garantizan que se utiliza un sistema de seguridad de la información, que es un estándar a nivel internacional para proteger la privacidad e integridad de la información.

Metodología MAGERIT

En este sentido fue desarrollado MAGERIT una metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, que ofrece un

método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones para de esta forma implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados. Además de esto, cuenta con todo un documento que reúne técnicas y ejemplos de cómo realizar el análisis de riesgos.

Puntualmente MAGERIT se basa en analizar el impacto que puede tener para la empresa la violación de la seguridad, buscando identificar las amenazas que pueden llegar a afectar la compañía y las vulnerabilidades que pueden ser utilizadas por estas amenazas, logrando así tener una identificación clara de las medidas preventivas y correctivas más apropiadas.

ISO/IEC 31010

ISO / IEC 31010 es una norma relativa a la gestión de riesgos codificada por la Organización Internacional de Normalización y la Comisión Electrotécnica Internacional (IEC). La norma ISO 31010 es compatible con la norma ISO 31000. Proporciona información sobre la selección y aplicación de técnicas de evaluación de riesgos.

Es parte de los elementos centrales de la gestión de riesgos definidos en ISO 31000, que son:

- Comunicación y consulta.
- Establecer el contexto.
- Evaluación de riesgos (identificación de riesgos, análisis de riesgos, evaluación de riesgos).
- Tratamiento de riesgo.
- Seguimiento y examen.

ISM3

ISM3 es un modelo de madurez para seguridad con cinco niveles que facilita la mejora y alineación entre las necesidades del negocio y los de la gestión de la seguridad dirigido a organizaciones de cualquier tipo y tamaño.

Características

- Enlazar la seguridad con los objetivos del negocio. Hay un profundo conocimiento de las metas del negocio y su dependencia a los elementos tecnológicos.
- Incluir métricas, adopción evolutiva y mejora continua. Partiendo de la premisa de que lo que no se mide no se puede mejorar.
- Flexibilidad, al adaptarse a distintas capacidades de inversión. (Open Source queda perfecto). La idea es poder hacer inversiones programadas. Existen muchísimas soluciones de Seguridad OpenSource que requieren muy poca inversión (OSSIM, Graylog, Wazuh, PfSense, Cortex, entre otros), las cuales en Gudix Security Consulting estamos dispuestos a apoyar en todo el proceso.
- Crear un ecosistema alrededor de ISM3 (COBIT, ISO2700 etc.). Permite establecer la base para posteriormente aspirar a una certificación ISO2700 o alinearnos con COBIT

Marco Teórico

Información General sobre la Institución

Nombre de la Institución:

Visión Mundial / Programa Integrado Lenca - Oficina Regional de Occidente.

Fundador de World Vision International:

Bob Pierce

Dirección:

Hotel Huella Lenca, desvío hacia Gracias Lempira, Aldea El Pericón, Yamaranguila, Intibucá.

Contacto:

gesler_seren@wvi.org

+504 98678952

Rubro de la Institución:

Desarrollo y Ayuda Comunitaria

Proyectos de la Institución:

- Transformación Comunitaria
- Respuesta ante el cambio climático
- Educación y Empleabilidad Juvenil
- Niñez y Juventud libre de violencia

Misión de la Institución:

World Vision Honduras es una confraternidad internacional de cristianos cuya misión es seguir a nuestro Señor y Salvador Jesucristo trabajando con los pobres y oprimidos para promover la transformación humana, buscar la justicia y dar testimonio de la buena noticia del Reino de Dios.

Historia:

Por casi 46 años, World Vision Honduras ha estado comprometido con la protección y el cuidado de los niños, niñas y a aquellos que más lo necesiten. Desde su llegada en 1974 como respuesta humanitaria a los desastres provocados por el huracán Fifi hasta la crisis por COVID-19 que en la actualidad afecta a nivel global, World Vision Honduras ha ido donde otros no lo harían. Incluso en los lugares donde es más difícil ser un niño, Dios está allí; y nosotros también deberíamos estarlo. Por lo tanto, nuestra misión continúa.

Resumen Institucional

World Vision es una organización no gubernamental que trabaja por el desarrollo de las comunidades, a través de proyectos y patrocinio de niños. Existe una oficina central en Tegucigalpa, de la cual se derivan 4 oficinas regionales en distintas ubicaciones del país. En cada región también existen oficinas más pequeñas distribuidas por los distintos municipios de la zona.

El Programa Integrado Lenca, es el encargado del acompañamiento a las oficinas más pequeñas.

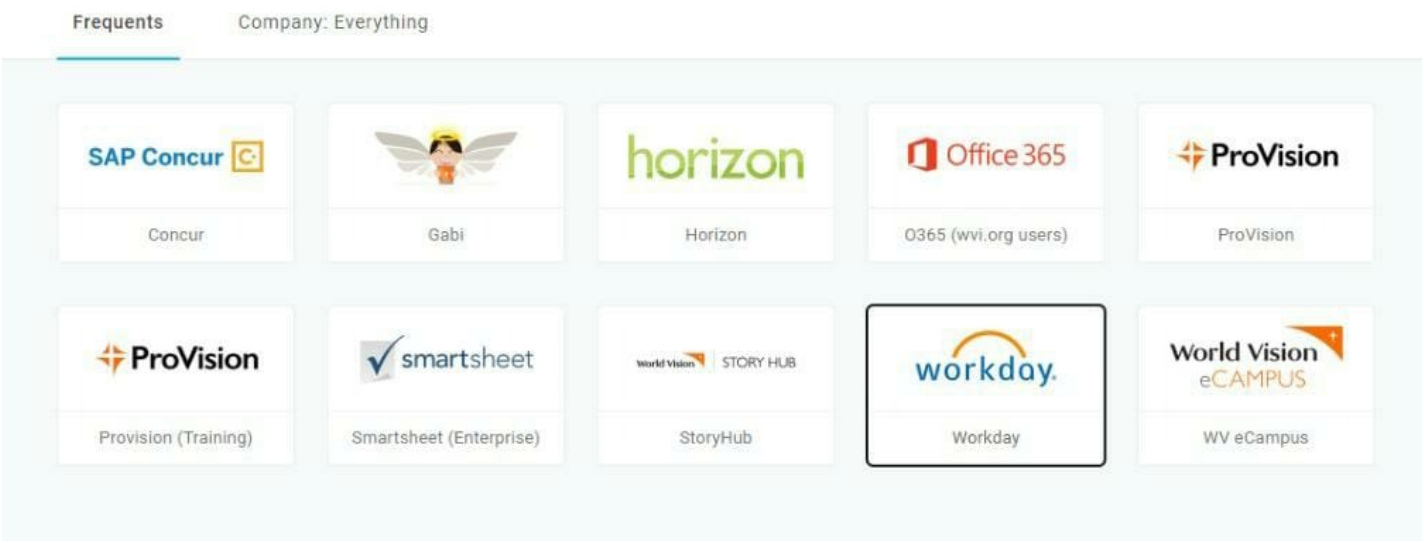
Los distintos sistemas con los que cuenta la institución, se manejan a través de Servidores Remotos, estos se encuentran físicamente en Malasia, específicamente en la ciudad de Kuala Lumpur.

Cuando una persona ingresa a trabajar en la institución, se permite el acceso a OneLogin, este permite acceder a las distintas aplicaciones, que se usan para liquidaciones, gastos, información de los niños, correo electrónico, además permite ver al usuario su perfil profesional detallado dentro de la institución. Cada empleado cuenta con una computadora portátil y un smartphone para realizar sus labores.

Sistemas Institucionales

- Sistema Contable
- Sistema Administrativo de Datos de los Niños
- Sistema Administrativo de Empleados
- Sistema para el Correo Electrónico
- KoboCollects (No está asociado a OneLogin)

Principales Sistemas/Software



Accesos del Departamento de Operaciones

Gerente: Tiene acceso a todos los sistemas, pero únicamente para visualizar reportes en el sistema Horizon. En WorkDay, el puede solicitar plazas, aprobar ascensos, permisos, solicitudes de compra, entre otros. (Sistemas de Alta Gerencia)

T.I: Tiene acceso a una plataforma para administración de los problemas de soporte, puede visualizar los empleados nuevos, las solicitudes de correo. También maneja los dispositivos de red de la institución. (Gestión de Dispositivos de T.I.)

CESP: Tienen acceso a la información de los niños, se encargan de revisar la información proporcionada por los compañeros que se encuentran en campo.

Accesos del Departamento de Finanzas

Tienen acceso a todo lo correspondiente a actividad monetaria, además aquí se manejan los inventarios y los activos con los que cuenta la institución.

Organigrama de la Institución

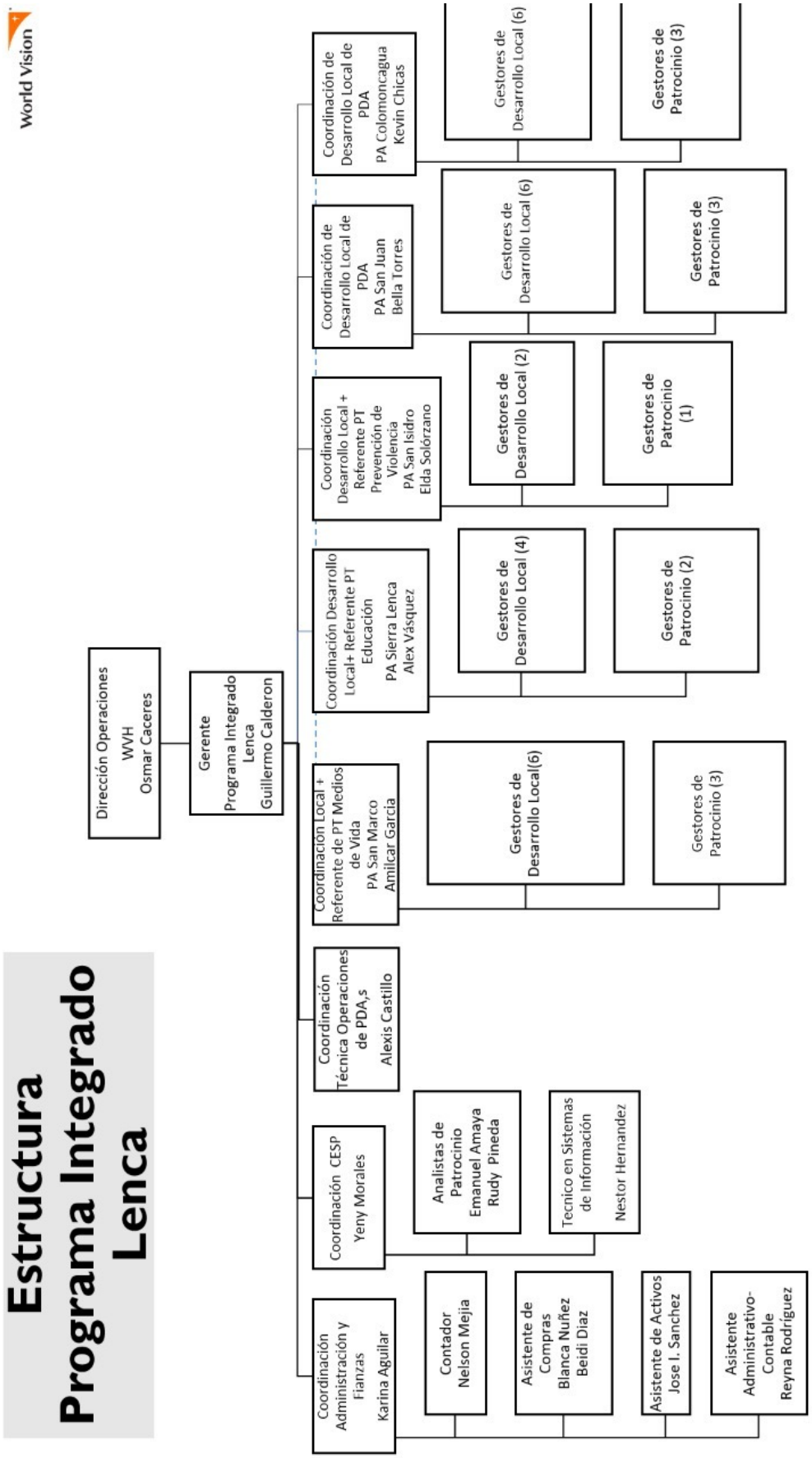
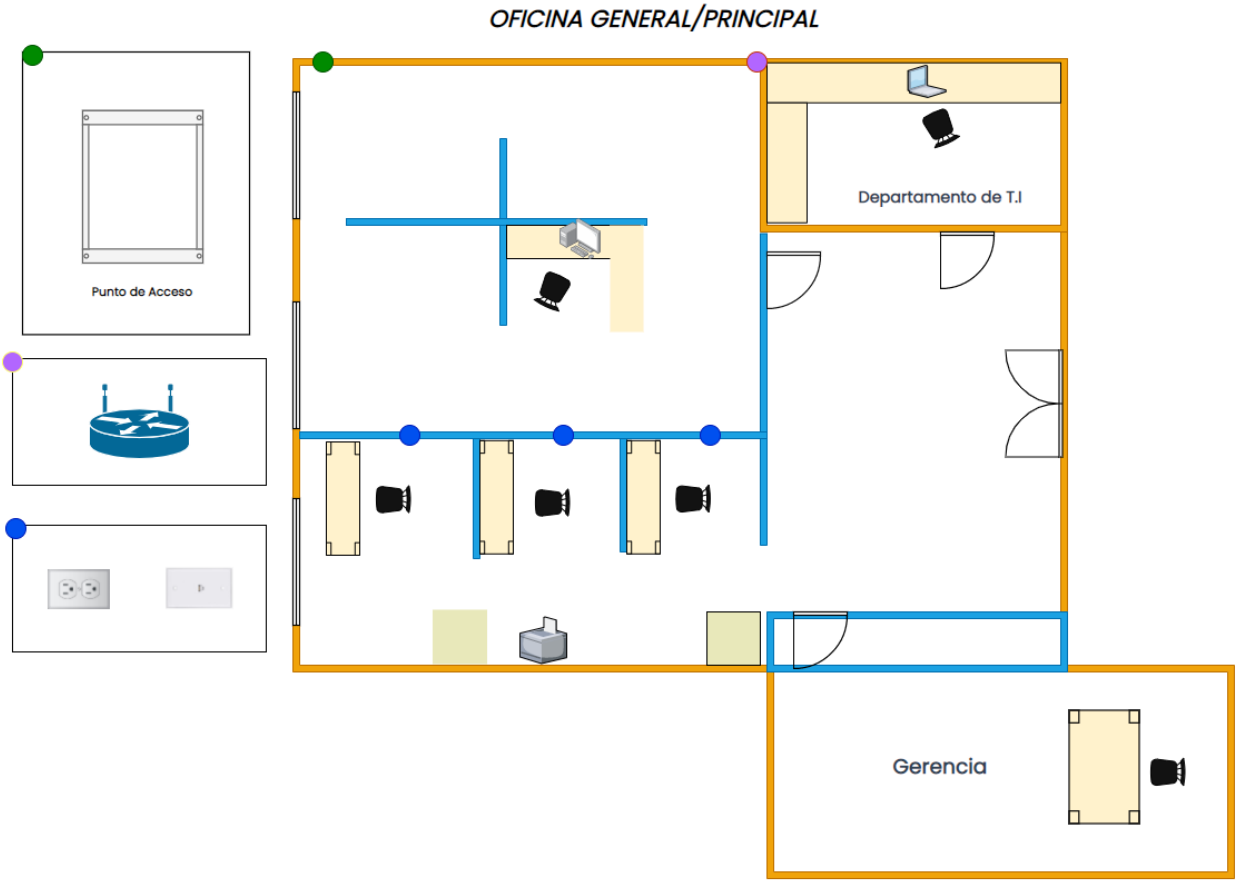
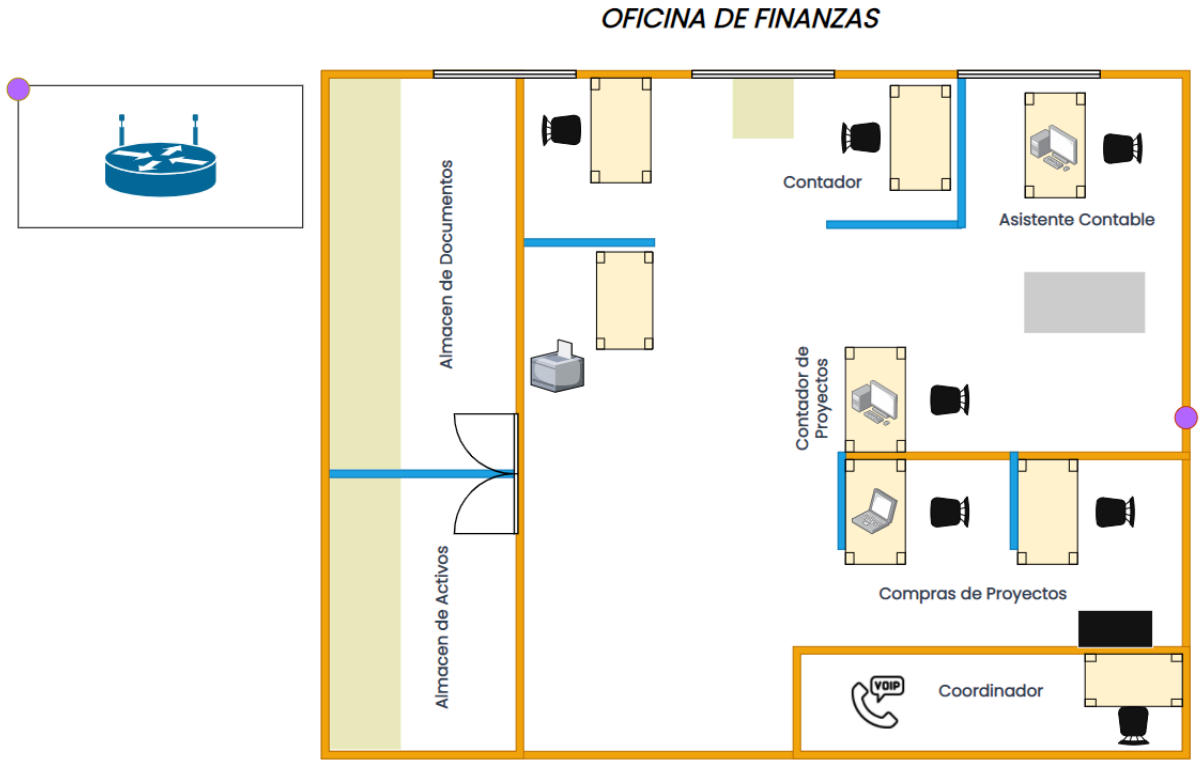
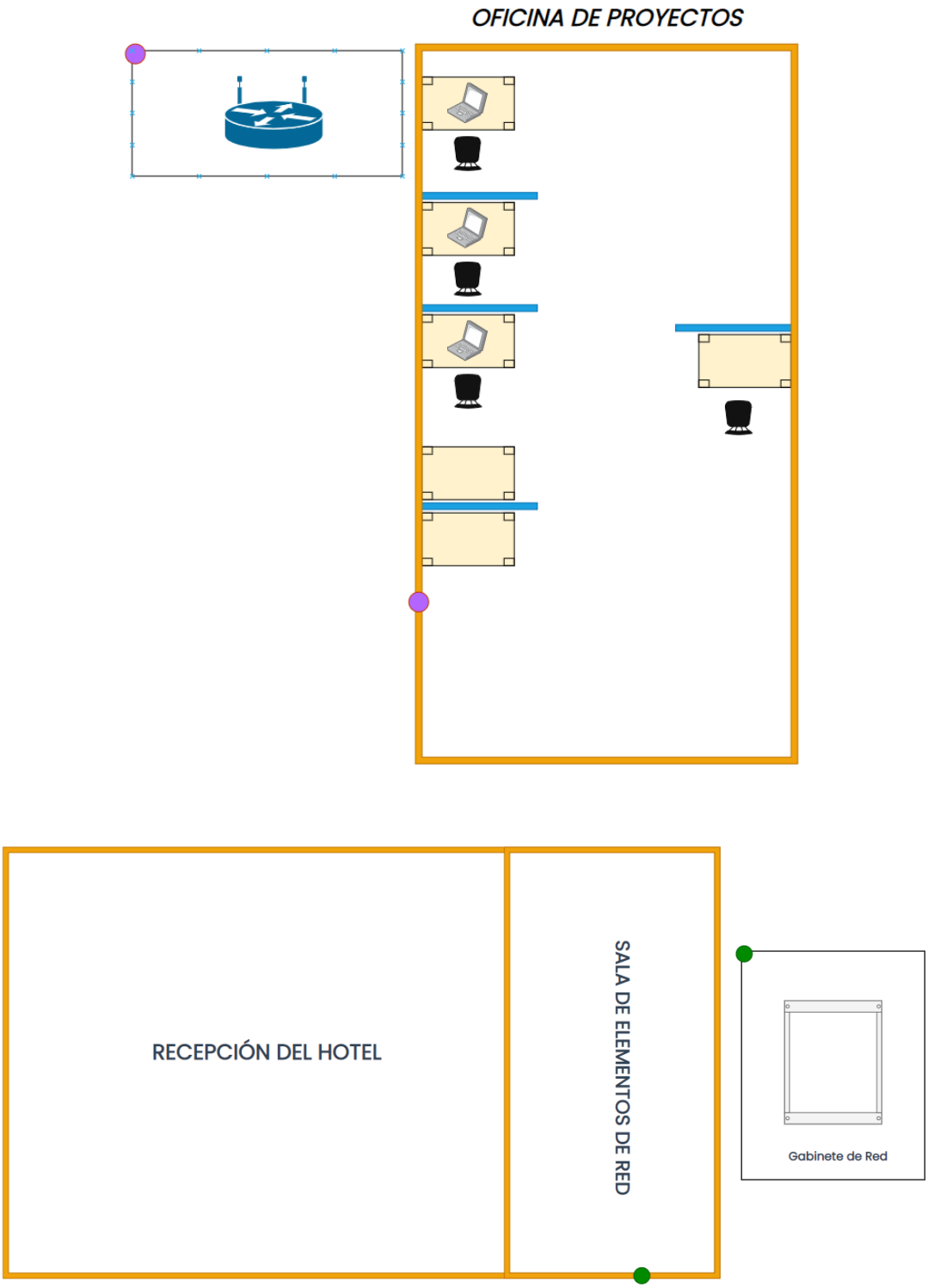


Diagrama de Distribución







Es importante mencionar que no todos los activos se encuentran dentro del establecimiento, puesto que, World Vision mantiene una parte del personal en trabajo de campo constantemente, por lo que dichas personas portan dispositivos como Computadoras portátiles y teléfonos inteligentes para realizar el envío de datos de manera remota.

1. Planificación

1.1 Planeación de la seguridad informática en la organización

Un plan informático es un conjunto de medios administrativos, técnicos y personales que garantizan niveles de seguridad y mitigación de riesgos en los bienes. De tal manera que se busca determinar cuáles son las necesidades de protección en el hardware, software, equipo humano y equipo técnico que hacen posible el funcionamiento de la organización World Vision en las oficinas del Programa Integrado Lenca.

Una vez realizada la identificación de activos prioritarios, se evalúan las posibles amenazas, riesgos y vulnerabilidades existentes para poder planificar, analizar los escenarios y estimaciones de riesgos respecto al estado actual de la seguridad para poder contar con un plan de acción de manera que facilite solucionar un problema.

Se establece un orden de riesgos, amenazas o vulnerabilidades por gravedad y frecuencia de incidencias de los activos ordenados por su prioridad teniendo en cuenta el nivel de uso, coste para solventar el problema, nivel de vulnerabilidad, el tipo de ataque, posibles consecuencias, entre otros.

Para finalizar, se busca la seguridad o protección adecuada para cada posible situación de amenazas o riesgos. Con el plan de seguridad informática en la organización las posibilidades de que se produzcan ciberataques, pérdidas de información, daños en los equipos, accesos no autorizados al sistema o servidores y demás se reducen porque habrá una acción de prevención y solución ante la incidencia.

1.2 Alcance del análisis y evaluación de riesgos del sistema informático

Se plantea evaluar el nivel de seguridad y protección de los equipos y otros activos informáticos que son responsables del funcionamiento de la organización World Vision en las oficinas del Programa Integrado Lenca, ubicado en Yamaranguila, municipio del departamento de Intibucá, Honduras. Se implementará la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT) para determinar los riesgos, amenazas y vulnerabilidades a los que están expuestos, con el fin de mejorar la seguridad e integridad de los datos con los que cuenta la institución.

1.3 Objetivos del análisis

- Identificar los activos más importantes de la organización
- Prevenir, detectar y mitigar las amenazas existentes
- Realizar un plan de acción contra amenazas, vulnerabilidades y riesgos
- Analizar y evaluar las vulnerabilidades
- Determinar las necesidades de seguridad que tiene World Vision/Programa Integrado Lenca
- Minimizar los riesgos, amenazas y vulnerabilidades que se encuentran en la organización.

2. Análisis de Riesgos

2.1 Descripción de los activos o recursos informáticos de la organización

Descripción de activos

Activo	Descripción
Computadoras	Dispositivos personales conectados a la red de la organización para realizar las tareas de su área. Cada empleado cuenta con una laptop para hacer sus labores en la plataforma web de la organización accediendo a las aplicaciones respectivas, cada empleado cuenta con una computadora personal para facilitar el trabajo remoto cuando no están en la oficina. Además cuentan con dos torres desktop
Impresoras multifuncionales	Dispositivos que se conectan a la red de dispositivos Meraki y brindan acceso local para las funciones de impresión y escaneo de documentos.
Gabinete de Red Troncal	Se encuentra el equipo de red principal donde llega la red troncal de fibra óptica proporcionada por la empresa Tigo, contiene los siguientes equipos.
Gabinete de Red Administrativo	Encargado de distribuir la red cableada e inalámbrica en las instalaciones mediante un switch.
Puntos de Acceso Inalámbricos	Brindan acceso inalámbrico a todos los dispositivos que lo requieran de manera segura y controlada.
Telefonos IP	Se cuentan con 2 teléfonos IP, uno en la oficina del gerente administrativo y otro en la oficina de la gerente de finanzas.
Conexiones de Energía y red local Ethernet	Todos los escritorios cuentan con conexión a la red eléctrica vía enchufe estándar de 110v junto con conexiones a la red ethernet vía conectores RJ45.
Smartphones personales	Cada empleado cuenta con un smartphone personal que incluye un plan de internet, llamadas y mensajes proporcionado por la empresa Claro Honduras.

Características de los activos

Computadoras (Windows 10)	4x HP EliteBook 735 G5 Ryzen CPU 8GB.
	1x HP EliteBook 735 G6 Ryzen Pro CPU 8GB.
	2x HP ProDesk 600 G1 SFF Core i5 4th CPU 8GB.
	4x HP ProBook 440 G6 Core i5 8th CPU 8GB.
	2x HP Modelo no especificado.
	2x HP ProBook 450 G6 Core i5 8th CPU 8GB.
	1x HP EliteBook 820 G3 Core i5 6th CPU 8GB.
	1x HP ProBook 640 G2 Core i5 6th 8GB.
	3x Lenovo E14 Gen 2 Core i5 11th 8GB.
	1x Lenovo 20U2S2S600 Ryzen 5 Pro 8GB.
	2x Dell Optiplex 7090 Core i5 11th 8GB.
Impresoras Multifuncionales	1x Impresor multifuncional profesional Canon MF 411. 1x Impresor multifuncional profesional Canon MF 410.
Gabinete de Red Troncal	1x Cisco Meraki MX64 (router y firewall). 1x Switch Operable Dell. 1x UPS.
Gabinete de Red Administrativo	1x Switch Dell.
Puntos de Acceso Inalámbricos	1x Cisco Meraki MR26 ubicado en la oficina administrativa. 1x Cisco Meraki MR42 ubicado en la oficina de finanzas.

	1x Cisco Meraki MR52 ubicado en el salón de capacitaciones. 1x Ubiquiti Wifi AP ubicado en la oficina de proyectos.
Teléfonos IP	Teléfonos IP de marca y modelo desconocido.
Conexiones de Energía y red local Ethernet	Conexión eléctrica estándar tipo B. Conexión de red RJ45.
Smartphones personales	Las especificaciones varían según el modelo elegido por cada empleado.

2.2 Valoración y confidencialidad de los activos o recursos

Clasificación de confidencialidad

Principio de seguridad	Clasificación	Definición
Confidencialidad	Público (1)	Este activo es considerado de carácter público y puede ser divulgado a cualquier persona o entidad interna o externa a la organización.
	Interna (2)	Este activo es utilizado por los funcionarios autorizados de la empresa para la ejecución de sus labores, y no puede ser conocida por terceros sin autorización del responsable del activo de información o directivas de la organización.
	Confidencial (3)	Este activo se considera altamente sensible y es utilizada por solo un grupo limitado de funcionarios o áreas para la ejecución de labores y no puede ser conocida por otros funcionarios de la organización o terceros externos sin autorización especial del responsable de la información o directivas de la organización.

Integridad	No sensitiva (1)	La pérdida o modificación no autorizada de este activo podría causar un daño leve o nulo para la organización.
	Sensitiva (2)	La pérdida o modificación de este activo podría causar un daño que genera perjuicios importantes que afecten a la organización, pero puede ser absorbido o asumido por este.
	Altamente sensitiva (3)	La pérdida o modificación de este activo podría causar un daño grave que genere perjuicios que afecten significativamente a la organización y que difícilmente podrían ser asumidos por ésta.
Disponibilidad	No critico (1)	El activo puede no estar disponible por un periodo de tiempo extendido, sin afectar la operación de la organización.
	Importante (2)	La no disponibilidad de este activo afectaría operaciones y servicios de los funcionarios.
	Misión crítica (3)	La no disponibilidad de este activo afectaría significativamente las operaciones, servicios de la organización y el acceso a la información.

2.2.1 Valoración y confidencialidad de activos

Activos	Valoración de activos		Valoración de confidencialidad			
Activo	**Valor**	**Descripción**	**C**	**I**	**D**	**Valor final**
Computadoras	10	Esencial para el desempeño de la institución	3	2	3	3
Impresoras multifuncionales	5	Importancia menor para la institución	2	1	1	2
Gabinete de Red Troncal	10	Esencial para el desempeño de la institución	2	2	3	3
Gabinete de Red Administrativo	10	Esencial para el desempeño de la institución	2	2	3	3
Puntos de Acceso Inalámbricos	10	Esencial para el desempeño de la institución	2	1	1	2
Telefonos IP	3	Importancia menor para la institución	3	1	1	3
Smartphones Personales	10	Esencial para el desempeño de la institución	3	2	3	3
Conexiones de Energía y red local Ethernet	10	Esencial para el desempeño de la institución	2	2	3	3

2.3 Identificación de amenazas y probabilidades

Una amenaza es un evento que puede afectar los activos de información y están relacionadas con el recurso humano, eventos naturales o fallas técnicas. Algunos ejemplos pueden ser ataques informáticos externos, errores u omisiones del personal de la empresa, infecciones con malware, terremotos, tormentas eléctricas o sobrecargas en el fluido eléctrico.

2.3.1 Tabla de estimación de probabilidad

Valor	Descripción
1	Es muy improbable que la amenaza ocurra o haya ocurrido
2	La amenaza podría ocurrir una o dos veces a lo largo del tiempo de actividad de la Institución
3	La amenaza se materializa a lo mínimo una vez cada uno o dos año
4	La amenaza se materializa a lo mínimo una vez cada tres o seis meses
5	La amenaza se materializa a lo mínimo una vez cada mes

2.3.2 Listado de amenazas

Código	Amenaza	Descripción	P	Razón de clasificación
A1	Daños por incendio	Daños que son generados por la incorrecta instalación o manipulación del hardware de los activos produciendo chispas o cortocircuitos que generen fuego. También considerable por incendios aledaños en el área de la organización.	**1**	Han ocurrido algunos casos de fuego en zonas de bosque aledañas, pero no en zonas cercanas.
A2	Daños por suministros de energía inestable	Daños producidos por las fluctuaciones de tensión eléctrica del suministro de energía pública.	**5**	En las oficinas es común presentar bajas de tensión eléctrica durante horas pico.
A3	Daños por humedad en	Daños producidos por goteras y filtraciones de agua dentro de las instalaciones.	**1**	Existe la posibilidad que al

	las habitaciones			ser una zona de alta pluviosidad el techo o las paredes se desgasten.
A4	Daños por desastres naturales	Daños graves producidos por tormentas eléctricas, granizadas e inundaciones.	**2**	Han ocurrido tormentas eléctricas y lluvias fuertes que han producido fallas y falta de servicios en la organización.
A5	Robo de Activos	Daños producidos por acceso no autorizado a las instalaciones de la organización o hurto por parte de los propios trabajadores de la organización.	**1**	No se han producido este tipo de incidentes, pero existe la posibilidad de que se produzcan.
A6	Acceso no autorizado	Daños producidos por el acceso de personal no autorizado a instalaciones restringidas de la organización o acceso no autorizado a los sistemas informáticos de la organización.	**1**	No se han producido este tipo de incidentes, pero existe la posibilidad de que se produzcan.
A7	Ciberataques(Virus, troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	Daños producidos por cualquier tipo de ciberataque a la organización que ponga en peligro la integridad de los sistemas.	**3**	Ha ocurrido una ocasión en donde la seguridad financiera de los empleados se vio vulnerada por un ataque de phishing.
A8	Ataques de denegación de servicio	Daños producidos por la interrupción de cualquiera de los servicios informáticos de la organización producidos por un atacante interno o externo intencionalmente.	**1**	No se han producido este tipo de incidentes, pero existe la posibilidad de que se produzcan.
A9	Daños de hardware	Daños producidos por la mala manipulación o circunstancias no controlables que produzcan una mala función en un equipo de la organización.	**2**	En algunos casos se suelen reportar problemas en los equipos de uso general en la

				oficina como impresoras y los personales como computadoras.
A10	Daños de software	Daños producidos por la mala manipulación o circunstancias no controlables que produzcan una mala función en un elemento de software de la organización.	**2**	Las computadoras personales de los empleados algunas veces han tenido problemas con los programas utilizados.
A11	Problemas de configuración	Daños producidos por la incorrecta configuración del software o equipos con que cuenta la organización que producen cortes inmediatos o futuros en el desarrollo de las actividades de la organización.	**1**	Los dispositivos suelen estar configurados de manera correcta porque son configurados por el encargado en el área de TI, pero podría suceder en el futuro.
A12	Activos defectuosos	Daños producidos por productos defectuosos entregados por los proveedores.	**1**	No se han producido este tipo de incidentes, pero existe la posibilidad de que se produzcan.
A13	Documentación impresa no reclamada	Daños producidos por posible exposición de información confidencial dejada en las bandejas de impresión de las impresoras multifuncionales.	**1**	No suele haber información confidencial oculta que los empleados de la organización no puedan ver, pero puede ocurrir en el futuro.
A14	Daños por inseguridad de red de impresoras	Daños producidos por la exposición de los archivos no protegidos en los servidores de colas de impresión.	**1**	No suele haber información confidencial oculta que los empleados de la organización no puedan ver, pero puede ocurrir en el futuro.

A15	Puertos de red abiertos	Daños producidos por el acceso no autorizado vía los puertos de red de los routers de la organización.	**1**	No se han producido este tipo de incidentes, pero existe la posibilidad de que se produzcan.
A16	Problemas o fallos de red	Daños que se producen por el funcionamiento deficiente de los routers, switches o proveedores del servicio de red local y para acceso a internet.	**2**	Se han producido caídas en los servicios de acceso a internet.
A17	Sobrecargas en el activo de red	Daños producidos por el uso indebido de los recursos de red utilizándolos para fines incorrectos o no autorizados produciendo cortes e interferencias en el servicio.	**1**	No se han producido este tipo de incidentes, pero existe la posibilidad de que se produzcan.
A18	Tener el gabinete de red sin identificación para el mantenimiento o por fallas en un cable	Daños producidos por el retraso en el mantenimiento o reparación de los servicios de red producido por la insuficiente identificación de los componentes internos de un gabinete de red.	**1**	No se han producido este tipo de incidentes porque los cables ya están rotulados, pero existe la posibilidad de que se produzcan.
A19	Intercepción de datos	Daños producidos por la utilización de malware malintencionado para interceptar datos que se transfieren entre los dispositivos de la organización.	**1**	No se han producido este tipo de incidentes, pero existe la posibilidad de que se produzcan.
A20	Instalar aplicaciones de terceros no autorizadas	Daños a los equipos consecuencia de la instalación de aplicaciones de terceros no autorizadas en las computadoras de los empleados.	**1**	Las computadoras tienen limitadas las aplicaciones que pueden instalarse, sin embargo existe la posibilidad que se produzcan.

2.4 Amenazas clasificadas por su tipo y su nivel de probabilidad

Las amenazas se clasificaron por un código que los identifica dependiendo de los activos que se encuentran en la Institución. Las amenazas se realizaron de manera descrita y con sus posibles soluciones de riesgo, también está definido un nivel de probabilidad que esta amenaza ocurra ciertas cantidades de veces en un tiempo determinado. En el nivel de probabilidad 1 significa que es poco probable y 5 que la probabilidad amenace muy frecuentemente.

2.4.1 Niveles de Clasificación de Probabilidad de las Amenazas

Nivel	Descripción
1	Es muy improbable que la amenaza ocurra o haya ocurrido
2	La amenaza podría ocurrir una o dos veces a lo largo del tiempo de actividad de la Institución
3	La amenaza se materializa a lo mínimo una vez cada uno o dos año
4	La amenaza se materializa a lo mínimo una vez cada tres o seis meses
5	La amenaza se materializa a lo mínimo una vez cada mes

2.4.2 Tabla de Estimación de Probabilidad

Activo	Descripción de Amenaza			Nivel de Probabilidad
	Código	Amenaza	Solución	
Todos los activos de la empresa	A1	Daños por incendio	Implementar detectores de incendios automáticos y extintores que no usan agua	**1**
	A2	Daños por suministros de energía inestable	Utilizar controladores de voltaje	**5**
	A3	Daños por humedad en las habitaciones	Cubrir las goteras para evitar filtraciones de agua	**1**
	A4	Daños por desastres naturales	Protección contra rayos, alojamiento de sistemas informáticos en lugares altos para evitar inundaciones	**2**

	A5	Robo de activos	Acceso restringido al personal no autorizado.	**1**
	A6	Acceso no autorizado	Utilizar métodos de autenticación para ingresar a las instalaciones restringidas de la organización o acceso no autorizado a los sistemas informáticos	**1**
	A12	Activos defectuosos	Adquirir los activos en negocios confiables y revisarlos previamente a su compra	**1**
Computadora	A7	Ciberataques(Virus, troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	Implementar un software antivirus y capacitar al personal sobre seguridad informática	**3**
	A8	Ataques de denegación de servicio	Usar sistemas de detección y prevención de intrusiones.	**2**
	A9	Daños de hardware	Mejorar la protección del activo y su ubicación	**2**
	A10	Daños de software	Capacitar al personal para hacer un mejor uso del activo	**2**
	A11	Problemas de configuración	Probar los activos después de su configuración	**1**
Impresoras multifuncionales	A9	Daños de hardware	Mejorar la protección del activo y su ubicación	**2**
	A11	Problemas de configuración	Probar los activos después de su configuración	**2**
	A13	Documentación impresa no reclamada	El personal autorizado retire la documentación y la coloque en un lugar seguro dependiendo de la confidencialidad de la información	**1**
	A14	Daños por inseguridad de red de impresoras de impresoras	Proteger la información sensible en la cola del servidor	**1**
	A15	Puertos de red abiertos	Todos los datos transmitidos	**1**

			sean encriptados	
Gabinete de Red Troncal	A16	Problemas o fallos de red	Verificar que los puntos de red estén conectados, tampoco saturar la cantidad de descargas en las computadoras	**2**
	A17	Sobrecargas en el activo	No utilizar la red en asuntos que son innecesarias y pesados para evitar que el activo sufra una caída	**1**
	A18	Tener el gabinete de red sin identificación para el mantenimiento por fallas en un cable	Verificar que los puntos de red estén conectados y usar un generador de tonos sino desconectar cada cable uno por uno hasta identificar en dónde está el fallo	**1**
Gabinete de Red Administrativo	A16	Problemas o fallos de red	Verificar que los puntos de red estén conectados, tampoco saturar la cantidad de descargas en las computadoras	**1**
	A17	Sobrecargas en el activo de red	No utilizar la red en asuntos que son innecesarias y pesados para evitar que el activo sufra una caída	**1**
	A18	Tener el gabinete de red sin identificación para el mantenimiento por fallas en un cable	Verificar que los puntos de red estén conectados y usar un generador de tonos sino desconectar cada cable uno por uno hasta identificar en dónde está el fallo	**1**
Puntos de Acceso Inalámbricos	A6	Acceso no autorizado	Para evitar instalación de puntos no autorizados, se debe configurar WLC con políticas de puntos de acceso y utilizar un software de monitoreo	**1**
	A7	Ciberataques(Virus, troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	Tener una vigilancia en el monitoreo de actividades en la red y que los usuarios estén autenticados.	**2**
	A8	Ataques de denegación	Usar sistemas de detección y	**2**

		de servicio	prevención de intrusiones.	
	A11	Problemas de configuración	Probar los activos después de su configuración	**1**
	A19	Intercepción de datos	Los datos deben estar encriptados	**1**
Teléfonos IP	A7	Ciberataques	Capacitar al personal sobre seguridad informática	**1**
	A9	Daños de hardware	Mejorar la protección del activo y su ubicación	**2**
	A10	Daños de software	Capacitar al personal para hacer un mejor uso del activo	**2**
	A11	Problemas de configuración	Probar los activos después de su configuración	**1**
Smartphones Personales	A7	Ciberataques(Virus, troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	Implementar un software antivirus y capacitar al personal sobre seguridad informática	**2**
	A9	Daños de hardware	Mejorar la protección del activo y su ubicación	**2**
	A10	Daños de software	Capacitar al personal para hacer un mejor uso del activo	**2**
	A20	Instalar aplicaciones de terceros no autorizadas	Restringir a los empleados descargas de aplicaciones no deseadas, no compartir datos sensibles por apps de terceros, monitorear las apps, asegurarse que todos los datos compartidos que son confidenciales sean encriptados	**2**
Conexiones de Energía y red local Ethernet	A7	Ciberataques(Virus, troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	Implementar un software antivirus y capacitar al personal sobre seguridad informática	**1**
	A19	Intercepción de datos	Los datos deben estar encriptados	**1**

2.5 Matriz de Impacto Potencial

En este apartado, se estima el impacto a nivel de actividades institucionales que tendría la materialización de las amenazas en cada activo.

Para realizar esta clasificación, se utilizará una escala de 3 niveles que describen de manera general la magnitud de cada amenaza en caso de que suceda, siendo 1 el nivel con menor impacto y el nivel 3 representa efectos graves para las actividades productivas de la institución.

2.5.1 Niveles de Clasificación del Impacto de las Amenazas

Nivel	Descripción
1	No hay consecuencias relevantes para la institución.
2	Bajo impacto o efecto sobre la institución.
3	Consecuencias significativas para la institución.
4	Consecuencias graves para la institución y sus actividades.
5	Consecuencias catastróficas para la institución y sus actividades.

2.5.2 Tabla de Impacto Potencial

Activo	Amenazas		Impacto
	Cod.	Descripción	
Todos los activos de la empresa	A1	Daños por incendio	**5**
	A2	Daños por suministros de energía inestable	**5**
	A3	Daños por humedad en las habitaciones	**2**
	A4	Daños por desastres naturales	**3**
	A5	Robo de activos	**2**
	A6	Acceso no autorizado	**2**

	A12	Activos defectuosos	**2**
Computadoras	A7	Ciberataques(Virus, troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	**5**
	A8	Ataques de denegación de servicio	**3**
	A9	Daños de hardware	**2**
	A10	Daños de software	**2**
	A11	Problemas de configuración	**1**
Impresoras multifuncionales	A9	Daños de hardware	**1**
	A11	Problemas de configuración	**1**
	A13	Documentación impresa no reclamada	**1**
	A14	Daños por inseguridad de red de impresoras de impresoras	**3**
	A15	Puertos de red abiertos	**3**
Gabinete de Red Troncal	A16	Problemas o fallos de red	**5**
	A17	Sobrecargas en el activo	**2**
	A18	Tener el gabinete de red sin identificación para el mantenimiento por fallas en un cable	**1**
Gabinete de Red Administrativo	A16	Problemas o fallos de red	**5**
	A17	Sobrecargas en el activo de red	**2**
	A18	Tener el gabinete de red sin identificación para el mantenimiento por fallas en un cable	**1**
Puntos de Acceso Inalámbricos	A6	Acceso no autorizado	**3**
	A7	Ciberataques(Virus, troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	**4**
	A8	Ataques de denegación de servicio	**3**
	A11	Problemas de configuración	**2**
	A19	Intercepción de datos	**3**

Teléfonos IP	A7	Ciberataques	**2**
	A9	Daños de hardware	**1**
	A10	Daños de software	**1**
	A11	Problemas de configuración	**1**
Smartphones Personales	A7	Ciberataques(Virus, troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	**5**
	A9	Daños de hardware	**2**
	A10	Daños de software	**2**
	A20	Instalar aplicaciones de terceros no autorizadas	**1**
Conexiones de Energía y red local Ethernet	A7	Ciberataques(Virus, troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	**5**
	A19	Intercepción de datos	**2**

2.6 Riesgo Potencial

2.6.1 Matriz de Riesgo Potencial

Una vez establecidos los criterios de impacto y probabilidad para cada amenaza identificada, calculamos el nivel de riesgo potencial, el cual es el resultado de multiplicar el nivel de impacto por el nivel de probabilidad.

El resultado de lo anterior debe clasificarse en base a la matriz potencial de riesgos, en la cual se definieron los siguientes rangos:

		Impacto				
		Muy Bajo	**Bajo**	**Medio**	**Alto**	**Muy Alto**
Probabilidad	**Valor**	**1**	**2**	**3**	**4**	**5**
Muy Alta	**5**	**5**	**10**	**15**	**20**	**25**
Alta	**4**	**4**	**8**	**12**	**16**	**20**
Media	**3**	**3**	**6**	**9**	**12**	**15**
Baja	**2**	**2**	**5**	**6**	**8**	**10**
Muy Baja	**1**	**1**	**2**	**3**	**4**	**5**

Indicador	Clasificación del Riesgo	Rango
	Mínimo	**1-3**
	Considerable	**4-8**
	Importante	**9-12**
	Grave	**15-25**

2.6.2 Valoración de las Amenazas en base a Probabilidad e Impacto

Activo	Amenazas		I	N.P	R.P	Indicador
	Cod.	Descripción				
Todos los activos de la empresa	A1	Daños por incendio	5	1	**5**	Considerable
	A2	Daños por suministros de energía inestable	5	4	**20**	Grave
	A3	Daños por humedad en las habitaciones	2	3	**6**	Considerable
	A4	Daños por desastres naturales	3	2	**6**	Considerable
	A5	Robo de activos	2	3	**6**	Considerable
	A6	Acceso no autorizado	2	2	**4**	Considerable
	A12	Activos defectuosos	2	3	**6**	Considerable
Computadoras	A7	Ciberataques(Virus, troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	5	3	**15**	Grave
	A8	Ataques de denegación de servicio	3	2	**6**	Considerable
	A9	Daños de hardware	2	3	**6**	Considerable
	A10	Daños de software	2	3	**6**	Considerable
	A11	Problemas de configuración	1	3	**3**	Mínimo
Impresoras multifuncionales	A9	Daños de hardware	1	2	**2**	Mínimo
	A11	Problemas de configuración	1	3	**3**	Mínimo
	A13	Documentación impresa no reclamada	1	4	**4**	Considerable
	A14	Daños por inseguridad de red de impresoras de impresoras	3	1	**3**	Mínimo
	A15	Puertos de red abiertos	3	1	**3**	Mínimo
Gabinete de Red Troncal	A16	Problemas o fallos de red	5	3	**15**	Grave
	A17	Sobrecargas en el activo	2	3	**6**	Considerable
	A18	Tener el gabinete de red sin identificación	1	2	**2**	Mínimo

		para el mantenimiento por fallas en un cable				
Gabinete de Red Administrativo	A16	Problemas o fallos de red	5	2	**10**	Importante
	A17	Sobrecargas en el activo de red	2	3	**6**	Considerable
	A18	Tener el gabinete de red sin identificación para el mantenimiento por fallas en un cable	1	2	**2**	Mínimo
Puntos de Acceso Inalámbricos	A6	Acceso no autorizado	3	2	**6**	Considerable
	A7	Ciberataques(Virus, troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	4	3	**12**	Importante
	A8	Ataques de denegación de servicio	3	2	**6**	Considerable
	A11	Problemas de configuración	2	3	**6**	Considerable
	A19	Intercepción de datos	3	2	**6**	Considerable
Teléfonos IP	A7	Ciberataques	2	1	**2**	Mínima
	A9	Daños de hardware	1	3	**3**	Mínima
	A10	Daños de software	1	3	**3**	Mínima
	A11	Problemas de configuración	1	3	**3**	Mínima
Smartphones Personales	A7	Ciberataques(Virus, troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	5	3	**15**	Grave
	A9	Daños de hardware	2	4	**8**	Considerable
	A10	Daños de software	2	2	**4**	Considerable
	A20	Instalar aplicaciones de terceros no autorizadas	1	4	**4**	Considerable
Conexiones de Energía y red local Ethernet	A7	Ciberataques(Virus, troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	5	2	**10**	Considerable
	A19	Intercepción de datos	2	2	**4**	Considerable

2.7 Número de amenazas por zona de riesgo y tipo de activo

En esta tabla se han seccionando por los riesgos y activos, primero se muestran todos los riesgos mínimos seccionado por los activos y cada uno de los activos con sus riesgos, a posteriori colocar la cantidad de riesgos que hay en cada activo, y así en cada uno de los 4 riesgos.

2.7.1 Número de amenazas por zona de riesgo y tipo de activo

Riesgos Mínimos		
Activo	**Riesgo**	**Total**
Computadoras	Problemas de configuración	1
Impresoras multifuncionales	Daños de hardware	4
	Problemas de configuración	
	Daños por inseguridad de red de impresoras de impresoras	
	Puertos de red abiertos	
Gabinete de Red Troncal	Tener el gabinete de red sin identificación para el mantenimiento por fallas en un cable	1
Gabinete de Red Administrativo	Tener el gabinete de red sin identificación para el mantenimiento por fallas en un cable	1
Teléfonos IP	Ciberataques	4
	Daños de hardware	
	Daños de software	
	Problemas de configuración	
Total de riesgos **mínimos**		11
Riesgos considerables		
Todos los activos de la empresa	Daños por incendio	6
	Daños por humedad en las habitaciones	
	Daños por desastres naturales	
	Robo de activos	

	Acceso no autorizado	
	Activos defectuosos	
Computadoras	Ataques de denegación de servicio	3
	Daños de hardware	
	Daños de software	
Impresoras multifuncionales	Documentación impresa no reclamada	1
Gabinete de Red Troncal	Sobrecargas en el activo	1
Gabinete de Red Administrativo	Sobrecargas en el activo de red	1
Puntos de Acceso Inalámbricos	Acceso no autorizado	4
	Ataques de denegación de servicio	
	Problemas de configuración	
	Intercepción de datos	
Smartphones Personales	Daños de hardware	3
	Daños de software	
	Instalar aplicaciones de terceros no autorizadas	
Conexiones de Energía y red local Ethernet	Ciberataques(Virus, troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	2
	Intercepción de datos	
Total de riesgos **considerables**		21
Riesgos importantes		
Gabinete de Red Administrativo	Problemas o fallos de red	1
Puntos de Acceso Inalámbricos	Ciberataques(Virus, troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	1
Total de riesgos **importantes**		8
Riesgos graves		

Todos los activos de la empresa	Daños por suministros de energía inestable	1
Computadoras	Ciberataques(Virus, troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	1
Gabinete de Red Troncal	Problemas o fallos de red	1
Smartphones Personales	Ciberataques(Virus, troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	1
Total de riesgos **graves**		4

2.9 Salvaguardas o controles existentes

Una vez especificados los riesgos potenciales de los activos, se prosigue en definir las salvaguardas o controles existentes en la Institución para poder proteger o prevenir amenazas en los activos, comenzando por especificar el tipo de activo, seguido de su posible amenaza, luego se mencionan los salvaguardas que pueden ser útiles para combatir o prevenir dicha amenaza, por consiguiente se determina el tipo de control, se especifica si la Institución cuenta con unas de las mitigaciones que se mencionan y su nivel de efectividad.

2.9.1 Tabla de estimación de nivel de efectividad del control

Valor	**Descripción**
1	Existe la probabilidad que falle el salvaguardas o no existe un control contra esta amenaza

2	El salvaguardias es eficaz de manera parcial porque no se ha probado, pero podría funcionar para combatir amenazas
3	El salvaguardias es comprobado que es óptimo y eficaz por lo que garantiza el funcionamiento para combatir amenazas

2.9.2 Tabla de nivel de efectividad del salvaguarda existente

Activos	Amenazas	Salvaguardas	Tipo de Salvaguardas	La Institución cuenta con el Salvaguarda	Nivel de Efectividad del Salvaguardas
Todos los activos de la empresa	Daños por incendio	Implementar detectores de incendios automáticos y extintores que no usan agua	Reducción del impacto	Sí	**2**
	Daños por suministros de energía inestable	Utilizar controladores de voltaje	Prevención	No	**1**
	Daños por humedad en las habitaciones	Cubrir las goteras para evitar filtraciones de agua	Prevención	Sí	**3**
	Daños por desastres naturales	Protección contra rayos, alojamiento de sistemas informáticos en lugares altos para evitar inundaciones	Reducción del daño	No	**1**
	Robo de activos	Acceso restringido al personal no autorizado.	Prevención	Sí	**3**
	Acceso no autorizado	Utilizar métodos de autenticación para ingresar a las instalaciones restringidas de la organización o acceso no autorizado a los sistemas informáticos	Prevención	No	**1**
	Activos defectuosos	Adquirir los activos en negocios confiables y	Prevención	Sí	**3**

		revisarlos previamente a su compra			
Computadora	Ciberataques (Virus, troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	Implementar un software antivirus y capacitar al personal sobre seguridad informática	Prevención	Sí	**2**
	Ataques de denegación de servicio	Usar sistemas de detección y prevención de intrusiones.	Prevención	Sí	**2**
	Daños de hardware	Mejorar la protección del activo y su ubicación	Reducción del daño	Sí	**2**
	Daños de software	Capacitar al personal para hacer un mejor uso del activo	Prevención	Sí	**2**
	Problemas de configuración	Probar los activos despues de su configuración	Prevención	Sí	**3**
Impresoras multifuncionales	Daños de hardware	Mejorar la protección del activo y su ubicación	Reducción del daño	Sí	**2**
	Problemas de configuración	Probar los activos despues de su configuración	Prevención	Sí	**2**
	Documentación impresa no reclamada	El personal autorizado retire la documentación y la coloque en un lugar seguro dependiendo de la confidencialidad de la información	Reducción del daño	Sí	**2**
	Daños por inseguridad de red de impresoras	Proteger la información sensible en la cola del servidor	Prevención	Sí	**2**

	Puertos de red abiertos	Todos los datos transmitidos sean encriptados	Prevención	Sí	**2**
Gabinete de Red Troncal	Problemas o fallos de red	Verificar que los puntos de red estén conectados, tampoco saturar la cantidad de descargas en las computadoras	Prevención	Sí	**2**
	Sobrecargas en el activo	No utilizar la red en asuntos que son innecesarias y pesados para evitar que el activo sufra una caída	Prevención	Sí	**2**
	Tener el gabinete de red sin identificación para el mantenimiento por fallas en un cable	Verificar que los puntos de red estén conectados y usar un generador de tonos sino desconectar cada cable uno por uno hasta identificar en dónde está el fallo	Prevención	Sí	**2**
Gabinete de Red Administrativo	Problemas o fallos de red	Verificar que los puntos de red estén conectados, tampoco saturar la cantidad de descargas en las computadoras	Prevención	Sí	**2**
	Sobrecargas en el activo	No utilizar la red en asuntos que son innecesarias y pesados para evitar que el activo sufra una caída	Prevención	Sí	**2**
	Tener el gabinete de red sin identificación para el mantenimiento por fallas en un cable	Verificar que los puntos de red estén conectados y usar un generador de tonos sino desconectar cada cable uno por uno hasta identificar en dónde está el fallo	Prevención	Sí	**2**
Puntos de	Acceso no	Para evitar instalación	Monitoreo	No	**1**

Acceso Inalámbricos	autorizado	de puntos de accesos no autorizados, se debe configurar WLC con políticas de puntos de acceso y utilizar un software de monitoreo			
	Ciberataques (Virus, troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	Tener una vigilancia en el monitoreo de actividades en la red y que los usuarios estén autenticados.	Prevención	Sí	**2**
	Ataques de denegación de servicio	Usar sistemas de detección y prevención de intrusiones.	Prevención	Sí	**2**
	Problemas de configuración	Probar los activos después de su configuración	Prevención	Sí	**3**
	Intercepción de datos	Los datos deben estar encriptados	Prevención	Sí	**2**
Teléfonos IP	Ciberataques	Capacitar al personal sobre seguridad informática	Prevención	Sí	**2**
	Daños de hardware	Mejorar la protección del activo y su ubicación	Reducción del daño	Sí	**2**
	Daños de software	Capacitar al personal para hacer un mejor uso del activo	Prevención	Sí	**2**
	Problemas de configuración	Probar los activos después de su configuración	Prevención	Sí	**3**
Smartphones Personales	Ciberataques (Virus, troyanos, gusanos, spyware,	Implementar un software antivirus y capacitar al personal sobre seguridad informática	Prevención	Sí	**2**

	phishing, rootkit, keyloggers, MTM)				
	Daños de hardware	Mejorar la protección del activo y su ubicación	Reducción del daño	Sí	**2**
	Daños de software	Capacitar al personal para hacer un mejor uso del activo	Reducción del daño	Sí	**2**
	Instalar aplicaciones de terceros no autorizadas	Restringir a los empleados descargas de aplicaciones no deseadas, no compartir datos sensibles por apps de terceros, monitorear las apps, asegurarse que todos los datos compartidos que son confidenciales sean encriptados	Monitoreo	Sí	**2**
Conexiones de Energía y red local Ethernet	Ciberataques (Virus, troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	Implementar un software antivirus y capacitar al personal sobre seguridad informática	Reducción del daño	Sí	**2**
	Intercepción de datos	Los datos deben estar encriptados	Reducción del daño	Sí	**2**

3. Gestión de Riesgos

3.1 Impacto Residual

El impacto residual es el daño sobre el activo debido a la materialización de la amenaza a pesar del actuar de las salvaguardas que intentan mitigarla.

En esta tabla, se toman los valores de las tablas anteriores, dentro de los cuales encontramos las amenazas, sus salvaguardas, la eficacia y el impacto potencial que se asignó a las mismas.
Para calcular el valor del impacto residual, es necesario dividir el impacto potencial entre la eficacia de la salvaguarda.

Activos	Amenazas	Salvaguardas	Tipo	¿Implementado?	Eficacia	Impacto	Impacto Residual
Todos los activos de la empresa	Daños por incendio	Implementar detectores de incendios automáticos y extintores que no usan agua	Reducción del impacto	Sí	2	5	**2.5**
	Daños por suministros de energía inestable	Utilizar controladores de voltaje	Prevención	No	1	5	**5**
	Daños por humedad en las habitaciones	Cubrir las goteras para evitar filtraciones de agua	Prevención	Sí	3	2	**0.67**
	Daños por desastres naturales	Protección contra rayos, alojamiento de sistemas informáticos en lugares altos para evitar inundaciones	Reducción del daño	No	1	3	**3**
	Robo de activos	Acceso restringido al personal no	Prevención	Sí	3	2	**0.67**

		autorizado.					
	Acceso no autorizado	Utilizar métodos de autenticación para ingresar a las instalaciones restringidas de la organización o acceso no autorizado a los sistemas informáticos	Prevención	No	1	2	**2**
	Activos defectuosos	Adquirir los activos en negocios confiables y revisarlos previamente a su compra	Prevención	Sí	3	2	**0.67**
Computadora	Ciberataques(Virus, troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	Implementar un software antivirus y capacitar al personal sobre seguridad informática	Prevención	Sí	2	5	**2.5**
	Ataques de denegación de servicio	Usar sistemas de detección y prevención de intrusiones.	Prevención	Sí	2	3	**1.5**
	Daños de hardware	Mejorar la protección del activo y su ubicación	Reducción del daño	Sí	2	2	**1**
	Daños de software	Capacitar al personal para hacer un mejor uso del activo	Prevención	Sí	2	2	**1**
	Problemas de configuración	Probar los activos después de su configuración	Prevención	Sí	3	1	**0.33**

Impresoras multifuncionales	Daños de hardware	Mejorar la protección del activo y su ubicación	Reducción del daño	Sí	2	1	**0.5**
	Problemas de configuración	Probar los activos después de su configuración	Prevención	Sí	2	1	**0.5**
	Documentación impresa no reclamada	El personal autorizado retire la documentación y la coloque en un lugar seguro dependiendo de la confidencialidad de la información	Reducción del daño	Sí	2	1	**0.5**
	Daños por inseguridad de red de impresoras	Proteger la información sensible en la cola del servidor	Prevención	Sí	2	3	**1.5**
	Puertos de red abiertos	Todos los datos transmitidos sean encriptados	Prevención	Sí	2	3	**1.5**
Gabinete de Red Troncal	Problemas o fallos de red	Verificar que los puntos de red estén conectados, tampoco saturar la cantidad de descargas en las computadoras	Prevención	Sí	2	5	**2.5**
	Sobrecargas en el activo	No utilizar la red en asuntos que son innecesarias y pesados para evitar que el activo sufra una caída	Prevención	Sí	2	2	**1**
	Tener el gabinete de red sin identificación para el mantenimiento por fallas en un	Verificar que los puntos de red estén conectados y usar un generador de tonos sino desconectar cada cable uno por uno	Prevención	Sí	2	1	**0.5**

	cable	hasta identificar en dónde está el fallo					
Gabinete de Red Administrativo	Problemas o fallos de red	Verificar que los puntos de red estén conectados, tampoco saturar la cantidad de descargas en las computadoras	Prevención	Sí	2	5	**2.5**
	Sobrecargas en el activo	No utilizar la red en asuntos que son innecesarias y pesados para evitar que el activo sufra una caída	Prevención	Sí	2	2	**1**
	Tener el gabinete de red sin identificación para el mantenimiento por fallas en un cable	Verificar que los puntos de red estén conectados y usar un generador de tonos sino desconectar cada cable uno por uno hasta identificar en dónde está el fallo	Prevención	Sí	2	1	**0.5**
Puntos de Acceso Inalámbricos	Acceso no autorizado	Para evitar instalación de puntos de accesos no autorizados, se debe configurar WLC con políticas de puntos de acceso y utilizar un software de monitoreo	Monitoreo	No	1	3	**3**
	Ciberataques(Virus, troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	Tener una vigilancia en el monitoreo de actividades en la red y que los usuarios estén autenticados.	Prevención	Sí	2	4	**2**

	Ataques de denegación de servicio	Usar sistemas de detección y prevención de intrusiones.	Prevención	Sí	2	3	**1.5**
	Problemas de configuración	Probar los activos después de su configuración	Prevención	Sí	3	2	**0.67**
	Intercepción de datos	Los datos deben estar encriptados	Prevención	Sí	2	3	**1.5**
Teléfonos IP	Ciberataques	Capacitar al personal sobre seguridad informática	Prevención	Sí	2	2	**1**
	Daños de hardware	Mejorar la protección del activo y su ubicación	Reducción del daño	Sí	2	1	**2**
	Daños de software	Capacitar al personal para hacer un mejor uso del activo	Prevención	Sí	2	1	**2**
	Problemas de configuración	Probar los activos después de su configuración	Prevención	Sí	3	1	**0.33**
Smartphones Personales	Ciberataques(Virus, troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	Implementar un software antivirus y capacitar al personal sobre seguridad informática	Prevención	Sí	2	5	**2.5**
	Daños de hardware	Mejorar la protección del activo y su ubicación	Reducción del daño	Sí	2	2	**1**
	Daños de software	Capacitar al personal para hacer un mejor uso del activo	Reducción del daño	Sí	2	2	**1**

	Instalar aplicaciones de terceros no autorizadas	Restringir a los empleados descargas de aplicaciones no deseadas, no compartir datos sensibles por apps de terceros, monitorear las apps, asegurarse que todos los datos compartidos que son confidenciales sean encriptados	Monitoreo	Sí	2	1	**0.5**
Conexiones de Energía y red local Ethernet	Ciberataques(Virus, troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	Implementar un software antivirus y capacitar al personal sobre seguridad informática	Reducción del daño	Sí	2	5	**2.5**
	Intercepción de datos	Los datos deben estar encriptados	Reducción del daño	Sí	2	2	**1**

3.2 Tabla de Impacto Residual y Riesgo Residual

En la siguiente tabla, se clasifica cada amenaza según el riesgo residual. Se toman como base los valores de Impacto residual obtenidos en la sección anterior, así como la probabilidad de que cada amenaza se materialice.

Para calcular el riesgo residual, se multiplica la probabilidad por el impacto residual, y dicho valor se clasifica según los detalles de la sección 2.6.1.

Activos	Amenazas	Salvaguardas	Tipo	Impacto Residual	Probabilidad	Riesgo Residual	Zona de Riesgo Residual
Todos los activos de la empresa	Daños por incendio	Implementar detectores de incendios automáticos y extintores que no usan agua	Reducción del impacto	2.5	1	**2.5**	Mínimo
	Daños por suministros de energía inestable	Utilizar controladores de voltaje	Prevención	5	5	**25**	Grave
	Daños por humedad en las habitaciones	Cubrir las goteras para evitar filtraciones de agua	Prevención	0.67	1	**0.67**	Mínimo
	Daños por desastres naturales	Protección contra rayos, alojamiento de sistemas informáticos en lugares altos para evitar inundaciones	Reducción del daño	3	2	**6**	Considerable
	Robo de activos	Acceso restringido al personal no autorizado.	Prevención	0.67	1	**0.67**	Mínimo
	Acceso no	Utilizar métodos	Prevenci	2	1	**2**	Mínimo

	autorizado	de autenticación para ingresar a las instalaciones restringidas de la organización o acceso no autorizado a los sistemas informáticos	ón				
	Activos defectuosos	Adquirir los activos en negocios confiables y revisarlos previamente a su compra	Prevenci ón	0.67	1	**0.67**	Mínimo
Computa dora	Ciberataques(Viru s, troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	Implementar un software antivirus y capacitar al personal sobre seguridad informática	Prevenci ón	2.5	3	**7.5**	Considerable
	Ataques de denegación de servicio	Usar sistemas de detección y prevención de intrusiones.	Prevenci ón	1.5	2	**3**	Mínimo
	Daños de hardware	Mejorar la protección del activo y su ubicación	Reducci ón del daño	1	2	**2**	Mínimo
	Daños de software	Capacitar al personal para hacer un mejor uso del activo	Prevenci ón	1	2	**2**	Mínimo
	Problemas de configuración	Probar los activos después de su configuración	Prevenci ón	0.33	1	**0.33**	Mínimo
Impresora s multifunc	Daños de hardware	Mejorar la protección del activo y su ubicación	Reducci ón del daño	0.5	2	**1**	Mínimo

ionales	Problemas de configuración	Probar los activos después de su configuración	Prevención	0.5	2	**1**	Mínimo
	Documentación impresa no reclamada	El personal autorizado retire la documentación y la coloque en un lugar seguro dependiendo de la confidencialidad de la información	Reducción del daño	0.5	1	**0.5**	Mínimo
	Daños por inseguridad de red de impresoras	Proteger la información sensible en la cola del servidor	Prevención	15	1	**1.5**	Mínimo
	Puertos de red abiertos	Todos los datos transmitidos sean encriptados	Prevención	1.5	1	**1.5**	Mínimo
Gabinete de Red Troncal	Problemas o fallos de red	Verificar que los puntos de red estén conectados, tampoco saturar la cantidad de descargas en las computadoras	Prevención	2.5	2	**5**	Considerable
	Sobrecargas en el activo	No utilizar la red en asuntos que son innecesarias y pesados para evitar que el activo sufra una caída	Prevención	1	1	**1**	Mínimo
	Tener el gabinete de red sin identificación para el mantenimiento por fallas en un cable	Verificar que los puntos de red estén conectados y usar un generador de tonos sino desconectar cada cable uno por uno hasta identificar en	Prevención	0.5	1	**0.5**	Mínimo

		dónde está el fallo					
Gabinete de Red Administrativo	Problemas o fallos de red	Verificar que los puntos de red estén conectados, tampoco saturar la cantidad de descargas en las computadoras	Prevención	2.5	1	**2.5**	Mínimo
	Sobrecargas en el activo	No utilizar la red en asuntos que son innecesarias y pesados para evitar que el activo sufra una caída	Prevención	1	1	**1**	Mínimo
	Tener el gabinete de red sin identificación para el mantenimiento por fallas en un cable	Verificar que los puntos de red estén conectados y usar un generador de tonos sino desconectar cada cable uno por uno hasta identificar en dónde está el fallo	Prevención	0.5	1	**0.5**	Mínimo
Puntos de Acceso Inalámbricos	Acceso no autorizado	Para evitar instalación de puntos de accesos no autorizados, se debe configurar WLC con políticas de puntos de acceso y utilizar un software de monitoreo	Monitoreo	3	1	**3**	Mínimo
	Ciberataques(Virus, troyanos, gusanos, spyware, phishing, rootkit,	Tener una vigilancia en el monitoreo de actividades en la	Prevención	2	2	**4**	Considerable

	keyloggers, MTM)	red y que los usuarios estén autenticados.					
	Ataques de denegación de servicio	Usar sistemas de detección y prevención de intrusiones.	Prevención	1.5	2	**3**	Mínimo
	Problemas de configuración	Probar los activos después de su configuración	Prevención	0.67	1	**0.67**	Mínimo
	Intercepción de datos	Los datos deben estar encriptados	Prevención	1.5	1	**1.5**	Mínimo
Teléfonos IP	Ciberataques	Capacitar al personal sobre seguridad informática	Prevención	1	1	**1**	Mínimo
	Daños de hardware	Mejorar la protección del activo y su ubicación	Reducción del daño	2	2	**4**	Considerable
	Daños de software	Capacitar al personal para hacer un mejor uso del activo	Prevención	2	2	**4**	Considerable
	Problemas de configuración	Probar los activos después de su configuración	Prevención	0.33	1	**0.33**	Mínimo
Smartphones Personales	Ciberataques(Virus, troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	Implementar un software antivirus y capacitar al personal sobre seguridad informática	Prevención	2.5	2	**5**	Considerable
	Daños de hardware	Mejorar la protección del activo y su ubicación	Reducción del daño	1	2	**2**	Mínimo
	Daños de software	Capacitar al	Reducci	1	2	**2**	Mínimo

		personal para hacer un mejor uso del activo	ón del daño				
	Instalar aplicaciones de terceros no autorizadas	Restringir a los empleados descargas de aplicaciones no deseadas, no compartir datos sensibles por apps de terceros, monitorear las apps, asegurarse que todos los datos compartidos que son confidenciales sean encriptados	Monitoreo	0.5	2	**1**	Mínimo
Conexiones de Energía y red local Ethernet	Ciberataques(Virus, troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	Implementar un software antivirus y capacitar al personal sobre seguridad informática	Reducción del daño	2.5	1	**2.5**	Mínimo
	Intercepción de datos	Los datos deben estar encriptados	Reducción del daño	1	1	**1**	Mínimo

3.3 Comunicación del riesgo y recomendaciones

Tomando en cuenta la matriz de impacto residual, tabla 3.2, se recomienda que los riesgos que se encuentran en zona de riesgo residual "Mínimo" y "Considerable" se estimen como admisibles siempre y cuando exista una medida de control y solución en caso que pueda perjudicar a gran escala la institución. Si la zona de riesgo es "Importante" y "Grave", se recomienda que se ejecute un plan de acción para solucionar los problemas que puedan indicar un mayor impacto de daño en la institución.

Las recomendaciones para solucionar los riesgos "Mínimo", "Considerable", "Importante" y "Grave" son:

- Velar por el cumpliento de las políticas de seguridad del centro de datos de la institución
- Mejorar la protección de los activos
- Capacitar al personal laboral para hacer un mejor uso de los activos y acerca del tema de seguridad informática
- Utilizar softwares de monitoreo, incidencias y de prevención de intrusiones

Se debe priorizar en orden jerárquico la zona de riesgo "Mínimo", "Considerable", "Importante" y "Grave" con mayor cantidad de incidencias de la tabla 2.7.1 para poder ser solucionado en caso que se quiera actuar de manera inmediata y no se pueda brindar soporte a todos los riesgos al mismo tiempo.

3.3.1 Tratamiento del riesgo

En la institución se han encontrado posibles amenazas para los activos en el departamento de TI y se han brindado los riesgos que estos pueden traer a la institución, la acción a tomar para salvaguardar los activos, la debilidad que implican las amenazas y las fortalezas que se cuentan para prevenir dichas amenazas.

Amenaza	Fortaleza	Riesgo	Debilidad	Acción
Daños por incendio	Tener extintores que no usan agua en las oficinas de la institución	Daños generados por la incorrecta instalación o manipulación del hardware de los activos produciendo chispas o cortocircuitos que generen fuego.	No contar con la implementación de detectores de incendios o rociadores	Implementar detectores de incendios automáticos y extintores que no usan agua
Daños por suministros de energía inestable	Tener un sistema de alimentación ininterrumpida (UPS)	Daños producidos por las fluctuaciones de tensión eléctrica del suministro de energía pública	No contar con una medida de seguridad para controlar el voltaje	Utilizar controladores de voltaje
Daños por humedad en las habitaciones	Aplicación de pintura selladora a las paredes y cubrir goteras	Daños producidos por goteras y filtraciones de agua dentro de las instalaciones	Agrietamiento, moho en las paredes causadas por las filtraciones de agua	Cubrir las goteras para evitar filtraciones de agua
Daños por desastres naturales	Mantener los activos en áreas seguras	Daños graves producidos por tormentas eléctricas, granizadas e inundaciones	• Tener que desconectar los servicios de energía eléctrica • Evacuar el edificio si es necesario	Protección contra rayos, alojamiento de sistemas informáticos en lugares altos para evitar inundaciones
Robo de Activos	• Contratación de guardia de seguridad para el manejo de las personas que entran y salen del edificio • Tener un control del personal que labora en las instalaciones del edificio	Daños producidos por acceso no autorizado a las instalaciones de la organización o hurto por parte de los propios trabajadores de la institución	Falta de instalación de cámaras de seguridad	• Verificar en el inventario qué activos se robaron y cuántos • Acceso restringido al personal no autorizado • Asegurar a los activos con mayor valor en áreas

				restringidas ● Tener cámaras de seguridad en las instalaciones del edificio
Acceso no autorizado	● Tener un control del personal que labora en las instalaciones del edificio ● Respetar políticas de seguridad	Daños producidos por el acceso de personal no autorizado a instalaciones restringidas de la organización o acceso no autorizado a los sistemas informáticos de la organización	No contar con métodos de autentificación a las áreas restringidas del edificio	Utilizar métodos de autenticación para ingresar a las instalaciones restringidas de la organización o acceso no autorizado a los sistemas informáticos
Ciberataques(Virus, troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	● Software antivirus implementado ● Personal capacitado para soporte técnico	Daños producidos por cualquier tipo de ciberataque a la organización que ponga en peligro la integridad de los sistemas	Información importante o activos corruptos por ciberataques	● Establecer políticas de uso de las computadoras ● Capacitar al personal sobre seguridad informática
Ataques de denegación de servicio	● Personal capacitado para soporte técnico ● Sistemas de detección y prevención de intrusiones que alerte si se detectan intentos de acceso no autorizado o mal uso de protocolos	Daños producidos por la interrupción de cualquiera de los servicios informáticos de la organización producidos por un atacante interno o externo intencionalmente	No contar con un sistema de mitigación de ataques mediante anti-DDoS	Asegurarse que el ataque ha finalizado haciendo uso del anti-DDoS
Daños de hardware	● Personal capacitado para soporte técnico ● Personal Capacitado para	Daños producidos por la mala manipulación o circunstancias no controlables que produzcan una mala	El activo no tenga reparación y deba ser sustituido por uno nuevo	● Mantener el activo en un lugar seguro, exento de caídas y golpes

	hacer un mejor uso del activo	función en un equipo de la organización		• Realizar mantenimiento periódicamente
Daños de software	• Herramienta de soporte de TI, incidencias y soporte técnico • Personal capacitado para soporte técnico • Personal Capacitado para hacer un mejor uso del activo	Daños producidos por la mala manipulación o circunstancias no controlables que produzcan una mala función en un elemento de software de la organización	El activo no regrese a su operación normal y deba ser sustituido por uno nuevo	• Mantener sistemas operativos actualizados • Tener un control de programas instalados • Proteger el sistema con antivirus • Capacitar al personal para hacer un mejor uso del activo
Problemas de configuración	• Aplicación de configuración adecuada y necesaria • Verificación constante del óptimo funcionamiento del dispositivo	Daños producidos por la incorrecta configuración del software o equipos con que cuenta la organización que producen cortes inmediatos o futuros en el desarrollo de las actividades de la organización	Verificar nuevamente el proceso de configuración y sino funciona el activo, devolver el dispositivo a la tienda donde fue adquirida	Verificar periódicamente el funcionamiento óptimo del dispositivo
Activos defectuosos	Adquisición de los activos en negocios confiables	Daños producidos por productos defectuosos entregados por los proveedores	El activo no tenga una operación normal y deba ser sustituido por uno nuevo	Adquirir los activos en negocios confiables y revisarlos previamente a su compra
Documentación impresa no reclamada	Cada personal laboral se hace responsable su documentación impresa	Daños producidos por posible exposición de información confidencial dejada en las bandejas de impresión de las impresoras	Documentación importante extraviada	El personal autorizado retire la documentación y la coloque en un lugar seguro dependiendo de la confidencialidad de la información

		multifuncionales		
Daños por inseguridad de red de impresoras	Personal capacitado para soporte técnico	Daños producidos por la exposición de los archivos no protegidos en los servidores de colas de impresión	• Robo de información • Daño de información	Proteger la información sensible en la cola del servidor
Puertos de red abiertos	• Personal capacitado para soporte técnico • Políticas de seguridad de usos restrictivos de puertos de los routers	Daños producidos por el acceso no autorizado vía los puertos de red de los routers de la organización.	• Explotar la vulnerabilidad de seguridad • Ataques de denegación de servicio	Todos los datos transmitidos sean encriptados
Problemas o fallos de red	• Personal capacitado para soporte técnico	Daños que se producen por el funcionamiento deficiente de los routers, switches o proveedores del servicio de red local y para acceso a internet.	• Robo de información • Daño de información	Verificar que los puntos de red estén conectados, tampoco saturar la cantidad de descargas en las computadoras
Sobrecargas en el activo de red	Sistemas informáticos de alta disponibilidad y alta fiabilidad	Daños producidos por el uso indebido de los recursos de red utilizándolos para fines incorrectos o no autorizados produciendo cortes e interferencias en el servicio.	Caída del activo en horas pico laborales	No utilizar la red en asuntos que son innecesarias y pesados para evitar que el activo sufra una caída
Tener el gabinete de red sin identificación para el mantenimiento por fallas en un cable	Puntos de red identificados tanto en el patch panel como en el lado usuario	Daños producidos por el retraso en el mantenimiento o reparación de los servicios de red producido por la insuficiente identificación de los componentes	No contar con un generador de tonos	• Verificar que los puntos de red estén conectados • Desconectar cada cable uno por uno hasta identificar en dónde está el

		internos de un gabinete de red.		fallo
Intercepción de datos	• Datos cifrados con WPA 3 o cifrado WEP Empresarial	Daños producidos por la utilización de malware malintencionado para interceptar datos que se transfieren entre los dispositivos de la organización.	• Robo de información • Daño de información	• Considerar el uso de AP Isolation para los dispositivos más sensibles • Configurar la autodefensa basada en AI de los routers Cisco Meraki. • Verificar mediante un escaneo de red el dispositivo/IP de donde se está realizando el ataque.
Instalar aplicaciones de terceros no autorizadas	• Personal Capacitado para hacer un mejor uso del activo • Cada personal laboral se hace responsable de su activo	Daños a los equipos consecuencia de la instalación de aplicaciones de terceros no autorizadas en las computadoras de los empleados.	• Robo de información • Daño de información	• Restringir a los empleados descargas de aplicaciones no deseadas • No compartir datos sensibles por apps de terceros • Monitorear las apps

3.4 Costos en Seguridad Informática

A continuación, se presentará un estimado de los costos posibles que World Vision tendría que incurrir para que las amenazas, riesgos y defectos sean solucionados. Además se incluye el coste de la consultoría aplicada por nuestro grupo para la elaboración de este informe de análisis y gestión de riesgos.

Nota: *Cabe recalcar que no todos los elementos son requisitos inmediatos ya que muchas de las amenazas son planteadas a futuro por lo que no incurre en un costo exacto en un periodo de tiempo específico.*

Amenaza	Solución	Cant	Precio Ud.	Valor Mensual	Valor Anual	Valor Instantáneo
Daños por incendio	Comprar extintores a base de C02	4	L. 950.00	N/A	L. 2,500.00 (Revisión)	L. 3,800.00
	Comprar detectores de humo e incendios automáticos	4	L. 1,000.00	N/A	N/A	L. 4,000.00
Daños por suministros de energía inestable	Comprar un sistema de alimentación ininterrumpida con controlador de voltaje automático	4	L. 3,000.00	N/A	N/A	L. 12,000.00
Daños por humedad en las habitaciones	Aplicación de pintura selladora a las paredes y cubrir goteras	-	L. 10,000	N/A	N/A	L. 10,000.00
Daños por desastres naturales	Implementar protección contra rayos	1	L. 40,000	N/A	N/A	L. 40,000.00
Robo de Activos	● Tener un control del personal que labora en las instalaciones del edificio via controles biométricos	4	L. 6,000.00	N/A	N/A	L. 6,000.00
Ciberataques(Virus , troyanos, gusanos, spyware, phishing, rootkit, keyloggers, MTM)	● Software antivirus implementado	22	L. 1,000.00	N/A	L. 1,000.00	N/A
Ataques de denegación de servicio	● Sistemas de detección y prevención de intrusiones que	Incluido con Fire	N/A	N/A	N/A	N/A

	alerte si se detectan intentos de acceso no autorizado o mal uso de protocolos	wall				
Daños de hardware	• Personal capacitado para soporte técnico • Personal Capacitado para hacer un mejor uso del activo	-	L. 3,000.00	N/A	L. 3,000.00	N/A
Daños de software	• Herramienta de soporte de TI, incidencias y soporte técnico • Personal capacitado para soporte técnico • Personal Capacitado para hacer un mejor uso del activo	-	L. 5,000.00	N/A	N/A	L. 5,000.00
Problemas de configuración	• Aplicación de configuración adecuada y necesaria • Verificación constante del óptimo funcionamiento del dispositivo	-	L. 3,000.00	N/A	L. 3,000.00	N/A
Documentación impresa no reclamada	Personal Capacitado para hacer una prevención correcta	-	L. 3,000.00	N/A	L. 3,000.00	N/A
Daños por inseguridad de red de impresoras	Personal capacitado para soporte técnico	-	L. 3,000.00	N/A	L. 3,000.00	N/A
Puertos de red abiertos	• Personal capacitado para soporte técnico	-	L. 3,000.00	N/A	L. 3,000.00	N/A

	● Políticas de seguridad de usos restrictivos de puertos de los routers					
Problemas o fallos de red	● Personal capacitado para soporte técnico	-	L. 3,000.00	N/A	L. 3,000.00	N/A
Sobrecargas en el activo de red	Sistemas informáticos de alta disponibilidad y alta fiabilidad	-	L. 10,000.00	N/A	N/A	L. 10,000.00
Tener el gabinete de red sin identificación para el mantenimiento por fallas en un cable	Puntos de red identificados tanto en el patch panel como en el lado usuario, generador de tonos	1	L. 2,800.00	N/A	N/A	L. 2,800.00
Intercepción de datos	Datos cifrados con WPA 3 o cifrado WEP Empresarial	Incluido con los AP	N/A	N/A	N/A	N/A
Instalar aplicaciones de terceros no autorizadas	● Personal Capacitado para hacer un mejor uso del activo ● Cada personal laboral se hace responsable de su activo	-	L.3,000.00	N/A	N/A	L. 3,000.00
Valor de la consultoría	Precio de honorarios del informe y las recomendación descritas	-	L. 40,000.00	N/A	N/A	L. 40,000.00
Total					**L. 18,500.00**	**L. 163,600.00**

3.5 Conclusiones y Recomendaciones

3.5.1 Conclusiones

- Durante el desarrollo del estudio de seguridad informática en la institución World Vision/Programa Integrado Lenca, se lograron identificar y valorar los elementos informáticos (equipos, activos) que sirven de principal soporte para la realización de las actividades laborales e institucionales.

- Se identificaron y clasificaron las amenazas que pueden llegar a afectar a los dispositivos informáticos dentro de la institución, de la misma manera se estimó la probabilidad de que dichas amenazas se materialicen tomando como referencia las condiciones y las incidencias anteriores que han existido en el contexto institucional.

- En base a una matriz de riesgo potencial, las amenazas fueron clasificadas y analizadas considerando que las mismas puedan materializarse dentro de la institución, dando como resultados un total de 6 amenazas cuyo indicador es Grave o Importante.

- La identificación y descripción de las amenazas que pueden afectar la integridad de los sistemas informáticos brinda un contexto más claro sobre Seguridad Informática a los encargados de T.I, quienes en base a estos detalles, pueden planear y ejecutar actividades destinadas a mitigar o incluso eliminar la posibilidad de que dichas amenazas se materialicen, evitando así que causen pérdidas significativas tanto económicas como de tiempo en la organización.

- La tecnología y los sistemas informáticos son elementos que cambian o mejoran constantemente, sin embargo, esta continua evolución brinda a su vez nuevas técnicas que pueden ser consideradas como amenazas, mismas que pueden ser utilizadas por personas con intención de dañar la integridad de la infraestructura tecnológica de una institución.

- Mantener una seguridad robusta y confiable en los sistemas informáticos es una tarea que debe desarrollarse en conjunto con todos los usuarios de tecnologías de la información. dentro de la institución, por lo que es necesario capacitar constantemente a cada miembro del personal, con el fin de mantenerlos informados sobre los nuevos riesgos o amenazas de la información.

3.5.2 Recomendaciones

- Es necesario realizar acciones o implementar medidas para mitigar o eliminar el riesgo de que las amenazas se materialicen, en especial aquellas cuya clasificación es Grave o Importante, puesto que representan un peligro para la integridad tecnológica de la institución.

- Si bien algunas amenazas no tienen altas probabilidades de materializarse, es necesario contemplar medidas que deben actuar en caso de que sucedan. Es importante mencionar que, a pesar de un bajo nivel de probabilidad, algunas podrían significar un impacto significativo a toda la institución.

- La constante actualización y capacitación sobre las nuevas amenazas del mundo tecnológico es un factor fundamental para reducir la probabilidad de que las mismas sucedan, por lo que es considerable realizar alguna de ellas cada 4 - 6 meses o cuando surjan novedades importantes.

- El monitoreo constante de las medidas implementadas o existentes debe ser permanente. De esta manera se garantiza que los controles siguen vigentes y puedan ser efectivos en caso de un incidente inesperado.

- Debido a que no todo el trabajo suele hacerse directamente desde las instalaciones de la Institución, los dispositivos que utilizan los usuarios, como computadoras y teléfonos, deben estar actualizados de acuerdo a las últimas tendencias de seguridad, así como a las últimas versiones o parches ofrecidos por los proveedores de sistemas operativos o el mismo fabricante del equipo.

Bibliografía

- Vieites, G. A. (2022). *Enciclopedia de la seguridad informática* (2.ª ed.). Ra-Ma.
- Eset Security. (2013, 14 mayo). *MAGERIT: metodología práctica para gestionar riesgos*. We Live Security - Eset. https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/
- Ambit Team. (s. f.). *¿Para qué sirve un SGSI? Controles y fases*. Ambit. Recuperado 4 de mayo de 2021, de https://www.ambit-bst.com/blog/para-qu%C3%A9-sirve-un-sgsi-controles-y-fases
- Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica. (2013). *MAGERIT – versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro 1* (3.ª ed.). Ministerio de Hacienda y Administraciones Públicas.