Universidad Católica de Honduras

"Nuestra Señora Reina de la Paz"

Campus Global

"Entregable 3 Sistema de seguridad de la información"

Alumnos:

Andrea Celeste Posas Salgado (1503-1996-01407)

Denia Julissa Chavarría 0318-2002- 01281

Mauricio Leonardo Zavala Osorto 0703-2004-3040

Karla Gissel López 0318-2003-01323

Cristian Alexander Aguilera Lemus 0321-1999-00020

Asignatura:

Seguridad informática y gestión de riesgos

Catedrática:

Lic. Blanca Patricia Medina

Sección:

1501

Fecha:

30 de julio del 2022

Índice

Introducción

La tecnología se está volviendo algo fundamental, es difícil no hacer uso de ella cuando se trata de una empresa ya que nos facilita el trabajo en muchas áreas. Pero no es suficiente solo implementar un sistema de información si no también un sistema de seguridad de datos para asegurar la información o prevenir posibles ataques.

El propósito de este análisis es evaluar a la empresa ONG PAG Proyecto Aldea Global por medio de la metodología Magerit. Primero conociendo sus debilidades y riesgos, identificando los sistemas con los que cuenta, e ir orientando y proponiendo estrategias para cada uno de los departamentos en los cuales esta se divide.

Una vez el análisis finalizado recomendar que tipo de sistema de seguridad es el adecuado tomando en cuenta las normas ISO y auditorías que la empresa necesita implementar.

Objetivo General

Realizar un análisis de riesgo para la empresa ONG Proyecto Aldea Global(PGA), por medio de la metodología Magerit, haciendo un análisis de los sistemas, evaluar riesgos y por último crear un plan de contingencia que se adapte a la empresa aplicando el sistema ya antes mencionado.

Objetivos específicos

- Planear estrategias para poder detectar posibles problemas y amenazas de seguridad.
- Brindar soporte y capacitación informática para el personal de cada departamento que conforma la ONG.

- Generar y asesorar a los colaboradores en planes de desarrollo informático y de seguridad.
- Implementar un servidor para administrar la red de datos.
- Establecer las políticas de seguridad informática pertinentes.
- Realizar auditorías de seguridad informática.

Planteamiento del problema

Justificación

La empresa ONG PAG Proyecto Aldea Global, maneja datos como transacciones, nombres de personal, jefes, etc. De cada uno de sus departamentos y es información delicada que debe ser segura.

Aunque la empresa no cuenta con un sistema de información para ir registrando todos los datos la posibilidad está abierta y con eso una gran responsabilidad de hacer uso adecuado de cada dato que se registra. Es por ello que es necesario una valoración y asesoría de un análisis de riesgos para un adecuado sistema de seguridad.

Al final de esta valoración de sistema de seguridad el cliente (la empresa) podrá tener una mejor idea de los beneficios que obtendrán como mejor manejo de la información, respaldar los datos, no tener filtraciones de entrada o salida de efectivo, uso adecuado de los activos, información de empleados, secciones por departamento, prevención ante amenazas, políticas de seguridad, capacitación.

Marco Conceptual

¿Qué es seguridad informática?

Es el proceso de prevenir y detectar el uso no autorizado de un sistema informático. Implica el proceso de proteger contra intrusos el uso de nuestros recursos informáticos con intenciones maliciosas o con intención de obtener ganancias, o incluso la posibilidad de acceder a ellos por accidente. La seguridad informática en realidad es una rama de un término más genérico que es la seguridad de la información, aunque en la práctica se suelen utilizar de forma indistinta ambos términos. La seguridad informática abarca una serie de medidas de seguridad, tales como programas de software de antivirus, firewalls, y otras medidas que dependen del usuario, tales como la activación de la desactivación de ciertas funciones de software, como scripts de Java, ActiveX, cuidar del uso adecuado de la computadora, los recursos de red o de Internet.

¿Qué es Margerit?

Es la metodología de análisis y gestión de riesgos elaborada en su día por el antiguo Consejo Superior de Administración Electrónica de España y actualmente mantenida por la Secretaría General de Administración Digital con la colaboración del Centro Criptológico Nacional. MAGERIT es una metodología de carácter público que puede ser utilizada libremente y no requiere autorización previa. Interesa principalmente a las entidades en el ámbito de aplicación del Esquema Nacional de Seguridad (ENS) para satisfacer el principio de la gestión de la seguridad basada en riesgos, así como el requisito de análisis y gestión de riesgos, considerando la dependencia de las tecnologías de la información para cumplir misiones, prestar servicios y alcanzar los objetivos de la organización.

Objetivos de Magerit:

- Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos

- Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)
- Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control Indirectos
- Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso

¿Qué es SGSI?

Es un conjunto de políticas de administración de la información. El término se denomina en inglés "Information Security Management System" (ISMS). El término SGSI es utilizado principalmente por la ISO/IEC 27001, que es un estándar internacional aprobado en octubre de 2005 por la International Organization for Standardization y por la comisión International Electrotechnical Commission. El SGSI tiene como objetivo evaluar todos los riesgos asociados con los datos e información que se manejan en una empresa.

El SGSI es un sistema de fácil implantación tanto para grandes empresas como para pymes. Es una herramienta para conocer y gestionar los riesgos a los que se enfrenta el negocio al manejar su información en el día a día. Al implementar SGSI se podrá eliminar esos riesgos o establecer los mecanismos necesarios para mitigar sus consecuencias.

Los principales beneficios que obtiene una empresa al implantar un sistema SGSI para la seguridad de sus datos son:

Reducción de riesgos. Se identificarán los riesgos y amenazas gracias a controles, protocolos, políticas y monitorización de procesos logrando reducir el número de amenazas de forma notable. En caso de que se produzca un incidente relacionado con

los datos, el negocio estará preparado para actuar de forma inmediata minimizando su impacto.

Reducción de costes. Se optimizará todo el proceso para evaluar y detectar amenazas descartando aquellos poco eficaces. Con un uso racional de los recursos se conseguirá un ahorro de costes en seguridad.

Integración de la seguridad en el negocio. Este sistema requiere de la implicación de todos los miembros de la empresa y del cambio de mentalidad, pasando a ser la seguridad uno de los componentes más importantes en cualquier proceso o actividad del negocio.

Cumplimiento de la normativa vigente en seguridad. Las leyes nacionales e internacionales para el tratamiento y protección de datos estarán cubiertas garantizando que se cumplen en todos los niveles o áreas de la empresa.

Incremento de la competitividad. Con este sistema se dispondrá de una prestigiosa certificación ISO de seguridad que será un elemento diferenciador con la competencia. Los clientes se sentirán más confiados y seguros de compartir sus datos personales, bancarios, gustos, y similares al saber que la empresa utiliza las mejores prácticas para garantizar que estén seguros.

Normas ISO en la seguridad:

Las normas ISO son normas o estándares de seguridad establecidas por la Organización Internacional para la Estandarización (ISO) y la Comisión Electrotécnica Internacional (IEC) que se encargan de establecer estándares y guías relacionados con sistemas de gestión y aplicables a cualquier tipo de organización internacionales y mundiales, con el propósito de facilitar el comercio, facilitar el intercambio de información y contribuir a la transferencia de tecnologías.

En concreto la familia de normas ISO/IEC 27000 son un conjunto de estándares de seguridad que proporciona un marco para la gestión de la seguridad. Dentro de este conjunto están:

ISO/IEC 27000; Vocabulario estándar para el SGSI para todas las normas de la familia. Se encuentra en desarrollo actualmente.

ISO/IEC 27001; Certificación que deben obtener las organizaciones. Norma que especifica los requisitos para la implantación del SGSI. Es la norma más importante de la familia. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos. Fue publicada como estándar internacional en octubre de 2005.

ISO/IEC 27002; Es un código de buenas prácticas para la gestión de seguridad de la información. Fue publicada en julio de 2005 como ISO 17799:2005 y recibió su nombre oficial ISO/IEC 27002:2005 el 1 de julio de 2007.

ISO/IEC 27003; Directrices para la implementación de un SGSI. Es el soporte de la norma ISO/IEC 27001. Publicada el 1 de febrero del 2010, no está certificada actualmente.

ISO/IEC 27004; Métricas para la gestión de seguridad de la información. Es la que proporciona recomendaciones de quién, cuándo y cómo realizar mediciones de seguridad de la información. Publicada el 7 de diciembre del 2009, no se encuentra traducida al español actualmente.

ISO/IEC 27005; Normativa dedicada exclusivamente a la gestión de riesgos en seguridad de la información. Proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de Seguridad en la Información, en soporte del proceso de gestión de riesgos de la norma

ISO/IEC 27001; Es la más relacionada a la actual British Standard BS 7799 parte 3. Publicada en junio de 2008.

ISO/IEC 27006; Requisitos para la acreditación de las organizaciones que proporcionan la certificación de los sistemas de gestión de la seguridad de la información. Esta norma específica requisitos para la certificación de SGSI y es usada en conjunto con la norma 17021-1, la norma genérica de acreditación

Marco teórico

Información general sobre la empresa

Nombre de la empresa: Aldea global

Propietario y fundador: Chet Thomas y Ellworth Culver

Dirección: Siguatepeque, Barrio Santa Marta

Teléfono: 2239-8311; 2239-8400

NUESTRA MISIÓN

Empoderando familias para reducir la pobreza y construir comunidades justas, pacíficas y productivas basados en valores cristianos.

NUESTRA VISIÓN

Una organización líder, que potencia capacidades y recursos de las comunidades, abriendo oportunidades de desarrollo.

NUESTRO LEMA

Intentar hacer algo tan grandioso para Dios, que terminaría en fracaso si Él no es parte de ello.

Proyecto Aldea Global

Inició sus acciones en 1983 en respuesta a las necesidades sociales y económicas urgentes de las áreas rurales de Honduras.

Los programas de PAG iniciaron su enfoque de crecimiento de líderes comunitarios quienes se convertirían en los líderes de programas de salud, agricultura y sociales enfocados en la familia y la comunidad para luchar contra la pobreza y la injusticia.

Este crecimiento gradual y diversificación de la programación son resultado directo del compromiso de PAG a un enfoque holístico para el trabajo de desarrollo, en lugar de centrar todos sus esfuerzos y recursos en un área. Después de haber establecido una presencia duradera en algunas comunidades durante más de tres décadas, PAG ha desarrollado relaciones sólidas y mucha credibilidad tanto con los líderes comunitarios como con los gobiernos locales.

El fuerte énfasis en la sostenibilidad local ha producido programas modelo en salud comunitaria, desarrollo agroindustrial y desarrollo de microempresas y créditos que han sido reconocidos por organizaciones de desarrollo a nivel mundial.

Mas sin embargo a lo largo de estos años la ONG se ha dado cuenta que aun tienen deficiencias en los diferentes departamentos en los que esta se divide y una de las principales preocupaciones es tomar las medidas de seguridad informática adecuadas para proteger la información que ellos manejan de las empresas, proyectos y usuarios, así mismo el equipo y software con el que cuenta no les permite brindar al usuario una

mejor atención por esta razón al tener fallos eléctricos no se brinda una respuesta rápida hacia el usuario.

Tomando en cuenta lo mencionado anteriormente se debe saber que los Sistemas de Información deben preservar la confidencialidad, disponibilidad e integridad, asegurándose que la información es accesible solo a las personas autorizadas, permitiendo proteger la información contra accesos o divulgación no autorizados, así mismo la implementación del equipo y software necesario para el funcionamiento correcto de la ONG.

Por ende, es necesario realizar el análisis de riesgo ya que nos permite identificar las vulnerabilidades que debilitan el sistema y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo.

1. Planificación

1.1 Planeación de la seguridad informática en la organización.

En esta etapa se tiene en consideración el plan de seguridad que se desea implementar. La empresa cuenta con un conjunto de bienes que conforman tanto su estructura física, como información detallada, también se cuenta el personal de la empresa, y todas las herramientas informáticas con las que cuenta. Cabe resaltar que la seguridad depende mucho de los individuos que conforman la empresa. No existe una seguridad total y cada institución depende de su personal para lograr los niveles de seguridad.

El primer paso para obtener una buena seguridad informática es identificar los riesgos y las vulnerabilidades, como se ha mencionado la empresa no cuenta con ningún

tipo de seguridad que respalde o proteja la información de ningún tipo de amenaza o mal manejo del activo. Constatar si ha habido algún tipo de incidente en el pasado para comenzar a proteger la información desde ese punto de referencia.

El segundo paso es hacer controles de manera constante tanto del hardware como del software, dentro de esto entran los dispositivos, aplicaciones/programas y archivos que se utilizaran dentro de la empresa, esto se llevará a cabo para tener una mejor gestión.

El tercer paso se basa en la creación de registros de reportes de errores y de correcciones realizadas para así tener un historial y facilitar las soluciones en posibles problemas futuros.

El cuarto paso consiste en realizar una división de responsabilidades que tendrá cada personal, es decir que se asignan responsabilidades y accesos según el cargo que este llevando a cabo cada persona.

El quinto paso es hacer un orden de prioridades, la empresa cuenta con distintos departamentos y es necesario establecer un orden de riesgos y al momento de un ataque que amenaza debe atenderse primero.

El sexto punto es aplicar el plan de seguridad tomando en cuenta las opciones anteriores, teniendo presente que debe funcionar de manera inmediata ya que la empresa debe mantenerse activa en todo momento, aquí también se toma en cuenta la capacitación del personal para el correcto manejo del sistema y quienes tendrán acceso a la total información ya sea por departamento o a nivel general.

1.2 Alcance del análisis y evaluación de riesgos del Sistema Informático.

El alcance establecido para el análisis y evaluación de riesgos para Aldea Global será basado en el método Magerit, de esta manera conocer los riesgos a los que se expone la ONG, para así poder detectar las vulnerabilidades y amenazas que enfrentan los departamentos en los que la ONG está dividido y que presentan un riesgo para la perdida de información, dando prioridad a aquellos riesgos que tengan mayor probabilidad de generar un impacto negativo en Aldea Global, para así invertir mayores recursos en prevenir y de esta manera implementar un Sistema de seguridad que contrarreste estas amenazas en la empresa.

En los resultados esperamos obtener las amenazas y vulnerabilidades que la empresa pueda tener en el futuro y de esta forma implementar un plan de gestión de riesgos para poder contraatacar las amenazas y vulnerabilidades que se presentan en cada uno de los departamentos, para evitar pérdidas de información. También podrán tener una infraestructura adecuada con un Sistema de software Seguro y equipo adecuado; acorde a las necesidades que se presenten.

1.3 Objetivos del análisis y evaluación de riesgos del Sistema Informático.

¿Qué es lo que se quiere lograr realizando el análisis y evaluación de riesgos?

1. Analizar y comprender el estado actual en el que se encuentra la infraestructura en términos de seguridad informática.

2. Examinar la manera en la que se puede eliminar los problemas e identificar los riesgos y vulnerabilidades.

3. Influenciar a todo el personal a seguir las normas que se quieren implicar sobre la seguridad de información y recursos.

4. Considerar el tiempo, esfuerzo y recursos necesarios para contrarrestar los problemas.

5. Plantear e implementar el SGSI, dependiendo del resultado del análisis correspondiente y tomando en cuenta las posibilidades de la ONG para realizar las mejoras.

6. Concientizar a las partes encargadas sobre la importancia y el impacto de manera positiva que genera la seguridad informática.

2. Análisis de Riesgos

2.1 Descripción de los activos o recursos informáticos de la empresa u organización.

Activo	Descripción
Servidores	Los servidores son los encargados de almacenar toda la información de la empresa, teniendo en cuenta que son dos servidores, estos dos se dividen en dos departamentos, uno es del departamento de contabilidad y el otro es el que almacena la información de todos los proyectos con los que PAG trabaja.

Routers	Los routers son los encargados de llevar los datos de un pc a otro y también se encargan de la conexión de los diferentes dispositivos que se usan como por ejemplo las impresoras. En PAG las redes de computadoras se hacen por medio de redes wifi, pero se hacen una sola red wifi haciendo la conexión entre los routers. Haciendo la excepción el área de la contabilidad por que es una red aparte.
PBX	La red PBX que es brindada por la red Telefónica Hondutel permite la comunicación de los empleados de la empresa y así mismo permite las llamadas a terceros.
COMPUTADORAS	Las computadoras son el principal objeto con el que se trabaja en la empresa PAG y las cuales permiten el funcionamiento de la misma.
SWITCH	Es el encargado del compartimento de toda la red ethernet en la empresa, este es el que comunica toda la empresa a través del cableado de red de routers.
Información	La información es el activo en nuestra opinión más valioso, la que aquí se llevan todos los registros y transacciones de la empresa.

2.2 Valoración y Confidencialidad de los Activos o recursos

Principio de Seguridad	Clasificación	Definición
Confidencialidad	Público (1)	Esta información es considerada de carácter público y puede ser divulgada a cualquier persona o entidad interna o externa de la empresa.
	Interna (2)	Este se lleva a cabo 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 empresa
	Confidencial (3)	Esta información es sensible y solo pueden utilizarlo ciertas personas o un área específica. No puede ser conocida por terceros sin autorización previa de la empresa.
Integridad	No Sensitiva (1)	La pérdida o modificación no autorizada de esta información podría causar un daño leve o nulo para la empresa.
	Sensitiva (2)	La pérdida o modificación de este activo podría causar un daño importante que afecten a la empresa, pero puede ser absorbido o asumido por este.
	Altamente Sensitiva (3)	La pérdida o modificación no autorizada de esta información podría causar un daño grave, que afectan significativamente a la empresa y que difícilmente podrían ser asumidos por ésta.
Disponibilidad Principio de Seguridad	No Critico (1)	Esta información puede no estar disponible por un período de tiempo sin afectar las operaciones de la empresa.
	Importante (2)	La no disponibilidad de este activo afectaría operaciones y servicios de los funcionarios de la empresa.
	Misión Crítica (3)	La no disponibilidad de este activo afectaría las operaciones, servicios de la empresa y el acceso a la información

2.2.1 Valoración y Confidencialidad de Activos

	Valoración de Activos		**Valoración de confidencialidad**			
Activos	Valor	Descripción	C	I	D	Valor Final
Servidores	9	Importantes para tener todo el acceso a los datos	3	3	3	3
Routers	10	Esenciales para la comunicación entre redes(distintas computadoras)	1	1	2	1
Computadoras	10	Esencial para el desempeño y buen manejo de la empresa	2	3	3	3
PBX	6	Importante para hacer llamadas	1	1	1	1
Switch	8	Importante para conectar todos los equipos de la empresa a una red. Incluido Computadoras, impresoras y servidores.	1	1	2	1
Información	10		2	3	3	3

2.3 Identificación de amenazas y probabilidad

Se entiende como amenaza informática toda aquella acción que aprovecha una vulnerabilidad para atacar o invadir un sistema informático. Pero existen muchos factores no solo el ataque directamente a un sistema sino también los desastres naturales. En la siguiente tabla se muestran cómo se definen las amenazas, clasificamos del 1 al 3 la frecuencia con la que pueden ocurrir.

2.4 Amenazas clasificadas por su tipo y su nivel de probabilidad

Nivel	Descripción de Probabilidad de amenaza
1	Improbable, sin evidencia de que ha ocurrido
2	Probable de que una Amenaza ocurra cada año
3	Probable que surja una amenaza cada 3 meses

	Amenaza	Descripción	NP	Razón de la calificación
A1	Desastres Naturales	Huracanes, lluvias constantes, rayos	2	Los huracanes o temporadas de lluvias fuertes pueden causar grandes daños y como consecuencia pérdida parcial o total de material de trabajo e información
A2	Error Humano	No conocer como es el manejo de la información o de equipos	3	La probabilidad que ocurra puede ser cada 3 meses, por personal nuevo que no está debidamente capacitado o simplemente un descuido del personal.
A3	Hackeo	Entrada de personas ajenas al sistema con el único fin de obtener información y hacer mal uso de ella.	1	Esta probabilidad nunca ha ocurrido pero podría ocurrir, nunca se está exento cuando de una empresa se trata

A4	Fallas en la red	Fallas en el equipo de red que impiden acceder al sistema	2	Esta probabilidad puede ocurrir cada año, por daños en los cables, equipo dañado, o fallas lógicas ajenas a la empresa
A5	Copias de seguridad	Perder información es fácil si esta no se respalda	3	Olvidar respaldar o no hacerlo adecuadamente es una probabilidad que puede ocurrir cada 3 meses
A6	Ingeniería Social	Personas que se hacen pasar por empleados cuya intención es obtener información	1	Es una probabilidad que nunca ha ocurrido pero puede ser posible
A7	Robo de equipos	Introducción a las instalaciones y robar equipos físicos	1	Es una probabilidad que nunca ha ocurrido pero es posible
A8	Personal interno malintencionado	Por rencor o malos entendidos pueden borrar información o ingresar al sistema y editar información, etc	3	Es probable que una amenaza ocurra cada año
A9	Virus	Ya sea de forma intencional o por error que dañan información y provocan pérdidas	2	Una probabilidad que puede ocurrir cada año y detener el trabajo de meses o días

A10	Incendios	Esto puede surgir por factores intencionales	1	Esta probabilidad nunca ha ocurrido pero puede deberse a sobrecarga de equipos, cables dañados, o una mano malintencionada asi que podria ocurrir

2.5 Matriz de impacto potencial

Valor	**Valor de Amenaza**	**Descripción**
1	Muy Alta	Consecuencias muy altas que conllevan daños extremos
2	Alta	Consecuencias altas que son un problema para la empresa
3	Media	Consecuencias que generan problemas a la empresa pero que tienen solución
4	Baja	Consecuencias que influyen poco en la empresa
5	Muy Baja	Consecuencias mínimas en la empresa

Activa	**Código**	**Amenaza**	**Impacto**
Hardware	A1	Inundación	1
	A2	Incendio	1

	A3	Robo o Hackeo (Hurto de información y equipo)	2
	A4	Mal Acondicionamiento del local	3
	A5	Desinformación del uso del Software	2
	A6	Falla en el Sistema de Red	3
Software	A1	Inundación	4
	A2	Incendio	4
	A3	Robo o Hackeo (Hurto de información y equipo)	2
	A4	Mal Acondicionamiento del local	5
	A5	Desinformación del uso del Software	3
	A6	Falla en el Sistema de Red	3
Datos	A1	Inundación	1
	A2	Incendio	1
	A3	Robo o Hackeo (Hurto de información y equipo)	2
	A4	Mal Acondicionamiento del local	3
	A5	Desinformación del uso del Software	2
	A6	Falla en el Sistema de Red	3

2.6 Riesgo Potencial

Luego de haber identificado el impacto que tuviera y la probabilidad es hora de sacar el riesgo potencial, el riesgo potencial es el producto del impacto y la probabilidad.

Luego el valor que tenemos, lo debemos de comparar con la matriz de potencial de riesgos el cual se definió de que los valores menores o iguales a 2 es un riesgo extremo, luego los que están en el rango de 3 y 4 son riegos de la zona alta, de 5 a 7 son riegos de zona media y de 8 a 15 son riegos de zona baja.

Tenemos comprendido la letra B para la zona baja, M para la zona media, A para la zona alta y E para la zona extrema.

Probabilidad	Muy Alta (1)	Alta (2)	Media (3)	Baja (4)	Muy baja (5)
1	E1	E2	A3	A4	M5
2	E2	A4	M6	B8	B10
3	A3	M6	B9	B12	B15
	B: Zona de riesgo baja (8-15)				
	A: Zona de riesgo Alta (3-4)				
	M: Zona de riesgo Media (5-7)				
	E: Zona de riesgo Extrema (1-2)				

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

Zona de riesgo	Hardware	Software	Datos	Total
Zona de Riesgo Bajo				
Inundación	0	0	0	0
Incendio	0	0	0	0
Robo o Hackeo (Hurto de información y equipo)	0	0	0	0
Mal Acondicionamiento del local	0	1	0	1
Desinformación del uso del Software	0	0	0	0
Falla en el Sistema de Red	0	0	0	0
Total Zona de riego bajo:				**1**
Zona de Riesgo Medio				
Inundación	0	1	0	**1**
Incendio	0	1	0	**1**
Robo o Hackeo (Hurto de información y equipo)	0	0	0	**0**
Mal Acondicionamiento del local	0	0	0	**0**
Desinformación del uso del Software	0	0	0	**0**
Falla en el Sistema de Red	0	0	0	**0**
Total Zona de riego medio:				**2**
Zona de Riesgo Alta				
Inundación	0	0	0	**0**

Incendio	0	0	0	**0**
Robo o Hackeo (Hurto de información y equipo)	1	1	1	**3**
Mal Acondicionamiento del local	1	0	1	**2**
Desinformación del uso del Software	1	1	1	**3**
Falla en el Sistema de Red	1	1	1	**3**
Total Zona de riesgo Alta:				**14**
Zona de Riesgo Extremo				
Inundación	1	0	1	**2**
Incendio	1	0	1	**2**
Robo o Hackeo (Hurto de información y equipo)	0	0	0	**0**
Mal Acondicionamiento del local	0	0	0	**0**
Desinformación del uso del Software	0	0	0	**0**
Falla en el Sistema de Red	0	0	0	**0**
Total Zona de riesgo Extremo:				**4**

2.8 Matriz de riesgo potencial

Los datos que se muestran en la siguiente tabla son la una unión entre la tabla de Riesgo Potencial y la Tabla de matriz de impacto potencial ya que muestra el código de amenaza(su probabilidad) y el código de impacto de dicha amenaza.

Tipo activo	Código amenaza	Amenazas	Impacto	Nivel de probabilidad	Riesgo Potencial	Zona de riesgo
HARDWARE	A1	Inundación	1	1	1	E
	A2	Incendio	1	1	1	E
	A3	Robo o Hackeo (Hurto de información y equipo)	2	1	2	E
	A4	Mal Acondicionamiento del local	3	1	3	A
	A5	Desinformación del uso del Software	2	3	6	M
	A6	Falla en el Sistema de Red	3	2	6	M
SOFTWARE	A1	Inundación	4	1	4	A
	A2	Incendio	4	1	4	A
	A3	Robo o Hackeo (Hurto de información y equipo)	2	1	2	E
	A4	Mal Acondicionamiento del local	5	1	5	M
	A5	Desinformación del uso del Software	3	3	9	B
	A6	Falla en el Sistema de Red	3	2	6	M
DATOS	A1	Inundación	1	1	1	E
	A2	Incendio	1	1	1	E
	A3	Robo o Hackeo (Hurto de información y equipo)	2	1	2	E
	A4	Mal Acondicionamiento del local	3	1	3	A
	A5	Desinformación del uso del Software	2	3	6	M
	A6	Falla en el Sistema de Red	3	2	6	M

El dato de riesgo potencial fue sacado usando una operación matemática la cual consistía en la multiplicación entre el campo Impacto y el campo Nivel de probabilidad.

2.9 Salvaguardas o controles existentes

La empresa por la ubicación en donde está establecida, tiene muchos aspectos en los cuales salvaguardar, por ejemplo, en caso de desastres naturales, error humano, hackeo, error en la red, robo o hurto, virus, incendios. Aldea Global es una organización que cuenta con muy pocos recursos informáticos, la manera de salvaguardar su información es manual ya que cuentan con un archivo por lo que están al margen de cometer fallas humanas por no estar al 100% capacitados, al contar con personal no capacitado surge el mal manejo del equipo informático dando un mal uso a este equipo propenso a virus y siendo víctimas de hackeo.

SALVAGUARDAR	
COD	Descripción
SG-01	Antivirus de windows actualizado y funcional en todo momento.
SG-02	Protocolo de mantenimiento de equipos y seguridad para ser aplicado mensualmente
SG-03	Comprobación de actualizaciones diarias y automáticas para el equipo informático.
SG-04	UPS que ayuden a la alimentación de energía eléctrica a los equipos y los protejan de anomalías en la misma.

SG-05	Cámaras dentro y fuera de las instalaciones para evitar robos o personal malintencionado.
SG-06	Adición de un sistema anti incendios.
SG-07	Renovación de las instalaciones y fortificación de la estructura de la misma

2.9.1 Controles implementados según el activo, la amenaza y su nivel de efectividad.

Desastres naturales						
Activos Afectado	Vulnerabilidad	Controles	Tipo de control	Control Implementado	Efectividad del control	Comentarios
Hardware, software, información	Zona propensa a inundaciones	Los laboratorios que contienen equipo de cómputo no deberían de estar en zonas que son propensas a inundaciones	Minimizador	No	3	Se encuentra en una zona fácil de inundaciones en tiempos de invierno.
	Falta de un backup	Se debe tener al	Prevención	No	2	El personal

	en un lugar alterno	menos una copia de seguridad en un lugar diferente en caso de que ocurra este incidente				autorizado debe tener acceso a una copia y esto puede ser desde la nube.

Fuga de información						
Activos Afectado	Vulnerabilidad	Controles	Tipo de control	Control Implementado	Efectividad del control	Comentarios
Hardware, software, información	Ausencia de supervisión a trabajos del persona externo	Se deben de establecer mecanismos para garantizar la seguridad de la información del personal externo	Minimizador	Si	3	No permiten el ingreso de otras personas que no sean de Aldea Global
	Carencia de normas de seguridad para el resguardo de la información	Se deben de establecer procedimientos para poder garantiza la seguridad de la información.	Minimizador	No	3	Es muy necesario contar con todas las medidas de seguridad
	Inadecuado procedimiento al	Se debe de ser minuciosos con las	Minimizador	No	3	Al no contar con

	momento de quitar acceso al sistema a un empleado despedido	personas que tienen acceso al sistema, para poder evitar que un empleado que ya no trabaje ahí, pueda divulgar información				procedimientos todo el personal puede acceder a información confidencial
	Ausencia de protocolos en caso de fuga de información	Se deben de establecer políticas en caso de una fuga de información	Minimizador	No	2	No tienen políticas porque no a ocurrido un problema de ese tipo

Virus Informáticos						
Activos Afectado	Vulnerabilidad	Controles	Tipo de control	Control Implementado	Efectividad del control	Comentarios
Hardware, software, información	Deficiencias en las gestión de los recursos	Se debe de definir detalladamente que usuarios tienen acceso a que recursos, para asegurar la protección de estos	Prevención	No	3	Muchos colaboradores tienen acceso a la información
	Utilización de antivirus piratas o de mala calidad	Se debe de hacer un análisis para elegir que antivirus	Prevención	No	3	Cuentan con anti virus piratas

		utilizar y tomando en cuenta pagar una licencia				
	Ausencia de normas para los usuarios	Se debe dejar en claro lo que deben y no deben de hacer los usuarios, para evitar la propagación de algún virus informático	Minimizador	No	2	Aun no hay normas para cada cargo en la empresa
	Ausencia de protocolos en caso de propagación de virus informáticos	Se debe de establecer pasos a seguir en caso de una situación de una propagación de algún virus informático para poder mitigar el daño	Minimizador	No	2	Al no tener ese tipo de problemas no cuentan con un plan

Amenaza por incendios						
Activo	Vulner	Controles	Tipo de	Control Impleme	Efectividad del	Comen

s Afectado	abilidad		control	ntado	control	tarios
Hardware, software, información	Carencia de un sistema de detección de incendios	Se debe de contar con un sistema que pueda alertar en caso que este sucediendo un incendio	Minimizador	No	2	No se cuenta con un sistema en Aldea Global
	Ausencia de equipo contra incendios	Se debe de colocar equipo contra incendios en lugares estratégicos	Minimizador	Si	2	Cuentan con extintores en el Instituto
	Falta de un mecanismo automático para mitigar el incendio	Se debe de contar con un sistema que pueda mitigar de manera automática el incendio una vez este ultimo a sido detectado	Minimizador	No	2	No se cuenta con un sistema de este tipo pero sería muy útil contar con el

3. Gestión de Riesgos

3.1 Impacto residual

Desastres Naturales					
Activos Afectado	Vulnerabilidad	Tipo de control	Efectividad del control	Impacto Potencial	Impacto Residual
Hardware, software, información	Zona propensa a inundaciones	Minimizador	3	1	0.33
	Falta de un backup en un lugar alterno	Prevención	2	1	0.5

Fuga de información					
Activos Afectado	Vulnerabilidad	Tipo de control	Efectividad del control	Impacto Potencial	Impacto Residual
Hardware, software, información	Ausencia de supervisión a trabajos del persona externo	Minimizador	3	1	0.33
	Carencia de normas de seguridad para el resguardo de la información	Minimizador	3	1	0.33
	Inadecuado procedimiento al momento de quitar acceso al sistema a un empleado despedido	Minimizador	3	1	0.33
	Ausencia de protocolos en caso de fuga de información	Minimizador	2	1	0.5

Virus Informáticos					
Activos Afectado	Vulnerabilidad	Tipo de control	Efectividad del control	Impacto Potencial	Impacto Residual
Hardware, software, información	Deficiencias en las gestión de los recursos	Prevención	3	1	0.33
	Utilización de antivirus piratas o de mala calidad	Prevención	3	1	0.33
	Ausencia de normas para los usuarios	Minimizador	2	1	0.5
	Ausencia de protocolos en caso de propagación de virus informáticos	Minimizador	2	1	0.5

Amenaza por incendios					
Activos Afectado	Vulnerabilidad	Tipo de control	Efectividad del control	Impacto Potencial	Impacto Residual
Hardware, software, información	Carencia de un sistema de detección de incendios	Minimizador	2	1	0.5
	Ausencia de equipo contra incendios	Minimizador	2	1	2.5
	Falta de un mecanismo automático para mitigar el	Minimizador	2	1	0.5

	incendio				

3.2 Matriz de impacto residual y riesgo residual.

Desastres Naturales								
Activos Afectado	Vulnerabilidad	Tipo de control	Efectividad del control	Impacto Potencial	Impacto Residual	Nivel de probabilidad	Riesgo Residual	Zona de riesgo residual
Hardware, software, información	Zona propensa a inundaciones	Minimizador	3	5	1.7	2	3.4	M6
	Falta de un backup en un lugar alterno	Prevención	2	5	2.5	2	5	A4

Fuga de información								
Activos Afectado	Vulnerabilidad	Tipo de control	Efectividad del control	Impacto Potencial	Impacto Residual	Nivel de probabilidad	Riesgo Residual	Zona de riesgo residual
	Ausencia de supervisión a trabajos	Minimizador	3	5	1.7	3	5.1	A3

Hardware, software, información	del persona externo							
	Carencia de normas de seguridad para el resguardo de la información	Minimizador	3	5	1.7	2	3.4	A4
	Inadecuado procedimiento al momento de quitar acceso al sistema a un empleado despedido	Minimizador	3	5	1.7	3	5.1	M6
	Ausencia de protocolos en caso de fuga de información	Minimizador	2	5	2.5	2	5	E2

Virus Informáticos								
Activos Afectado	Vulnerabilidad	Tipo de control	Efectividad del control	Impacto Potencial	Impacto Residual	Nivel de probabilidad	Riesgo Residual	Zona de riesgo residual
Hardware, software, información	Deficiencias en las gestión de los recursos	Prevención	3	5	1.7	3	5.1	B9
	Utilización de antivirus piratas o de mala calidad	Prevención	3	5	1.7	2	3.4	E2
	Ausencia de normas para los usuarios	Minimizador	2	5	2.5	2	5	A4
	Ausencia de protocolos en caso de propagación de virus informáticos	Minimizador	2	5	2.5	2	5	E2

Amenaza por incendios								
Activos Afectado	Vulnerabilidad	Tipo de control	Efectividad del control	Amenaza por incendios	Amenaza por incendios	Nivel de probabilidad	Riesgo Residual	Zona de riesgo residual
Hardware, software, información	Carencia de un sistema de detección de incendios	Minimizador	2	5	2.5	2	5	M6
	Ausencia de equipo contra incendios	Minimizador	2	5	2.5	1	2.5	A4
	Falta de un mecanismo automático para mitigar el incendio	Minimizador	2	5	2.5	2	5	A4

3.3 Comunicación del riesgo y recomendaciones

Con el análisis de Magerit una vez finalizado y abarcando todos los puntos en las tablas anteriores, lo que continua es detallar cómo deben manejarse los riesgos y con qué prioridad debe atenderse para así tener un plan de contingencia con posibles o futuros daños.

Para los riesgos definidos en la B y zona M, son aceptables pero deben ser monitoreados y estar en observación, ya que los riesgos de impacto pueden ser susceptibles al cambio.

Para la zona A, zona E se recomienda actuar de inmediato tomando los pasos siguientes:

- Capacitar(activos): capacitar a los empleados a utilizar los activos correctamente y también a cómo actuar en caso de una emergencia ya sea error humano, virus, hackeo.
- Capacitar(desastres naturales o accidentes): la empresa debe contar con las medidas de seguridad pertinentes en caso de incendios, inundaciones y cómo deben actuar en caso de que esto ocurra.
- Respaldar: la información debe ser diariamente respaldada, si surge cualquier incidente de software no se perderá ningún dato.
- Contar con un seguro: con respecto al hardware es importante asegurar los equipos así en cualquier "desastre" se puede recuperar lo invertido o al menos una parte de él que le permita a la empresa reponerse pronto

La decisión de ejercer estas medidas depende de los encargados de la empresa ONG PAG Proyecto Aldea Global si deciden implementarlas de inmediato para evitar estos riesgos. El siguiente cuadro representa el resumen de la cantidad de riesgos en las zonas agrupadas por tipo de amenaza.

Amenazas	**Nivel de Riesgo**	
	Extrema	**Alta**
Desastres Naturales	0	1
Fuga de información	1	2

Virus Informatico	2	1
Amenazas por incendios	0	2
Total	**3**	**6**

3.3.1 Tratamiento del riesgo

Se han identificado algunas amenazas y se ha buscado una solución para cada una de las amenazas de esta manera se podrá salvaguardar cada activo e instalaciones de la empresa, identificando de esta manera las debilidades y fortalezas.

Amenazas	Riesgo	Fortaleza	Debilidades	Acción
Desastres Naturales	Daño a instalaciones y/o activos	Mantener los activos en zonas no vulnerables y en instalaciones bien estructuradas	Mantener los activos en zonas vulnerables y instalaciones en mala condición	Mejor distribución, ubicación adecuadas para los activos
Fuga de información	Uso mal intencionado de la información	Mejor seguridad, accesos restringidos en cuanto a la información	Acceso a la información a cualquier colaborador sin importar el cargo que desempeña	Accesos restringidos únicamente a personal autorizado acceder a la información
Virus Informatico	Daños al hardware de la empresa	Contar con una licencia de antivirus en todo los equipos	Contar con antivirus piratas	Adquirir licencias de antivirus
Amenazas por incendios	Daños a personal activos e infraestructura	Contar con el equipo necesario para esta emergencia	No contar con el equipo necesario en caso de incendios	Adquirir el equipo necesario y capacitar al personal con medidas de seguridad en una

Amenazas	Riesgo	Fortaleza	Debilidades	Acción
				emergencia

3.4 Costos en Seguridad Informática

Problema a Solucionar	Solución al Problema	Costo Mensual	Costo Anual	Costo Inmediato
Desastres Naturales	Mejorar el entorno.			L.100,000.00
Fuga de información	Contratar personal calificado(Área de Administración) para que pueda organizar y dar permisos a los otros empleados para que puedan acceder solo a sus correspondientes zonas.	L.12,000.00	L.144,000.00	
Virus Informatico	Contratar un antivirus seguro	L. 250.00	L. 2900.00	
Amenazas por incendios	Más extintores al igual que instalación de alarma de humos			L.40,000.00
	Total:	L.12,250.00	L.146,990.00	L. 140,000.00

3.5 Conclusiones y recomendaciones

Conclusiones

- De lo anterior se desprende la importancia de planear estrategias para detectar posibles problemas y amenazas de tal manera que al identificarlas estas puedan tener una posible solución .
- En conclusión, asesorar a los colaboradores en planes de desarrollo informático y de seguridad es muy importante de tal manera que el personal tenga posibles soluciones en caso de emergencia.

- Que la información es un activo valioso por ende la importancia de establecer políticas de seguridad pertinentes.
- Es importante tener bien segmentadas las áreas para poder localizar de una manera más eficiente algún tipo de amenaza que esté sucediendo.

Recomendaciones

- Recomendamos a la ONG capacitar al personal encargado del hardware de la empresa ya que uno de los mayores riesgos que pueden existir en una empresa es que los usuarios no sepan utilizar de manera adecuada los activos importantes para el correcto funcionamiento, esto para ocasionar menos fallas, menos errores y así generar menos costos.
- Recomendamos a la ONG mantenerse actualizado con licencias de antivirus en el equipo para evitar pérdida de información y otros daños causados por virus y malware.
- Una vez aplicada las soluciones en cuanto amenazas, mantenerlas para mantener un estándar de calidad y generar nuevas futuras amenazas al sistema.
- Recomendamos a la ONG mejorar su entorno y su ubicación para evitar algún tipo de daño que pueda ser causado por un desastre natural.

Bibliografía

Carlos Arturo Guamanga, C. L. (2015). *Analisis de Riesgo de Seguridad de la Información Basado en la Medología Magerit.* Bogotá,DC.

Global Suite. (5 de marzo de 2020). Obtenido de https://www.globalsuitesolutions.com/es/que-son-normas-iso/#:~:text=Las%20normas%20ISO%20son%20un,de%20productos%20en%20la%20industria.

Proyecto Aldea Global. (s.f.). Obtenido de https://www.paghonduras.org/