Universidad Católica de Honduras

"Nuestra Señora Reina de la Paz"

Campus Sagrado Corazón de Jesús

Entregable #3

Grupo #2

Nombre	Número de cuenta
Bryan Samuel Martinez Zelaya	0801-2001-22106
Andres Eduardo Archila Lanza	0801-2002-00198
Fernando Roberto Vallecillo Hernandez	0801-2000-23821
Jose Armando Cisne Aguilera	0801-1999-22326

Docente

Lic. Patricia Medina

Asignatura y Sección

IF630 - Seguridad informática y gestión de riesgo - 1501

Tercer Parcial - Primer Periodo 2022

Índice

Introducción

La seguridad informática se define como la forma en la que las organizaciones trabajan para reducir el riesgo de un ataque cibernético y su efecto potencial en las empresas, protegiendo los dispositivos y servicios que utiliza.

Siendo la seguridad informática algo primordial en lo que las empresas deben enfocarse para poder mejorar sus servicios con sus clientes pero también para poder funcionar mejor dentro de la empresa para todos sus empleados.

Así que en el presente informe se va a presentar un proyecto sobre el análisis de sistemas de información, la seguridad de este centro de cómputo y cómo se podría mejorar para una empresa llamada Laboratorios Fleming, laboratorio designado a los exámenes clínicos.

Para el desarrollo del análisis de este proyecto se utilizará la metodología MAGERIT para poder evaluar y gestionar los riesgos de mejor manera para poder analizar el impacto que puede tener para la empresa la violacion de la seguridad.

Esta metodología es demasiado útil para las empresas que quisieran iniciar con la gestión de seguridad de la información que contiene la empresa, por lo cual va a ser una buena metodología a utilizar para Laboratorios Fleming, que nunca ha tenido un análisis de seguridad.

Objetivos

Objetivo general

- Realizar un análisis completo sobre la empresa Laboratorios Fleming para conocer sus procesos a realizar, los riesgos que se pueden tener en cada uno y al final que se podría hacer para poder mejorar la seguridad dentro de la empresa utilizando la metodología MAGERIT.

Objetivos específicos

- Planear un análisis de seguridad y riesgos posibles para los Laboratorios Fleming.
- Poder utilizar la metodología MAGERIT de manera apropiada para mejorar la seguridad de la empresa.
- Calcular la evaluación de riesgos que se pueden presentar en la empresa.
- Calificar posibles amenazas que la empresa posiblemente pueda tener o presentar.
- Identificar los activos que tienen actualmente en la empresa.
- Evaluar la valoración de los activos que tiene la empresa.
- Determinar cómo los riesgos localizados y presentados se pueden mejorar o incluso anular con mejores prácticas que se podrían realizar en la empresa.

Planteamiento del problema

La seguridad informática siempre ha sido un tema prioritario a tomar en cuenta en las labores cotidianas. Las amenazas web no son algo nuevo, pues con el paso de los años los virus han ido evolucionando en conjunto con las nuevas tecnologías, lo cual ha obligado a los usuarios a mantenerse constantemente actualizados en cuanto a amenazas informáticas. Existe una gran cantidad de maneras por la cual podemos caer en engaños en donde se nos pueda comprometer la información que tenemos y transmitimos cada día para la empresa a la que uno trabaja. Pero también existe una gran cantidad de formas de poder defenderse de todas estas amenazas, simplemente con mejor inventario de computo, mejor administración y capacitación personal se pueden mitigar varias amenazas.

De la manera en la que los Laboratorios Fleming deberían de funcionar es que se reduzca la mayor cantidad de amenazas y riesgos que puedan tener la empresa con respecto a ella y con los clientes. Mejorando el sistema informático de los Laboratorios Fleming no solo ayudaría con posibles fugas de información o robo de información por parte de la empresa, sino que tambien podria mejorar de mejor manera la productividad de la empresa sino que también aumentar la seguridad y confiabilidad de los clientes al utilizar los servicios de los Laboratorios Fleming.

Mencionado anteriormente, existe una gran cantidad de maneras en la que estos riesgos se pueden mitigar o desaparecer para la mejoría de la empresa, algunas pueden contener algún coste monetario, otras son simplemente mejores prácticas a utilizar que no tendrian ningun coste en absoluto, pero si hablamos de la seguridad de la empresa, es algo que en ningún momento se tiene que ver de menos hablando en términos financieros.

Con este proyecto pensamos encontrar varias fallas que puedan afectar los Laboratorios Fleming y proponer posibles soluciones a los posibles problemas que podamos encontrar durante el desarrollo de este proyecto.

Justificación

Este proyecto será necesario en llevar a cabo para mejorar la seguridad informática de los Laboratorios Fleming que actualmente no presentan en una manera demasiado amplia con respecto a la seguridad de su software.

Los beneficios que contendrá la realización de este proyecto son una mejora en la productividad en la empresa, una mejora en el apartado de ciberseguridad de sus datos y transacciones con sus clientes, mejor seguridad y confiabilidad por parte de sus clientes y socios al igual que atraer más clientes al aumentar de manera positiva la imagen de la empresa.

Este proyecto no simplemente ayudará a la identificación de posibles amenazas, sino que también proporciona posibles soluciones a estas amenazas al igual que abrir más puertas a la empresa para poder utilizar mejores prácticas y no solamente en casos de seguridad.

La comunicación con la empresa no será un gran problema que nos impida conseguir información relevante para ayudar a esta empresa ya que el contacto que nuestro grupo tiene con el propietario de la empresa es muy cercano.

Marco conceptual

Seguridad informática

La seguridad informática —también llamada ciberseguridad—se refiere a la protección de la información y, especialmente, al procesamiento que se hace de la misma, con el objetivo de evitar la manipulación de datos y procesos por personas no autorizadas. Su principal finalidad es que tanto personas como equipos tecnológicos y datos estén protegidos contra daños y amenazas hechas por terceros.

Metodología 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.

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.

Marco teórico

Información general sobre la empresa

Nombre de la empresa: Laboratorios Fleming

Propietario y fundador: José Enrique Cisne Foeller

Dirección: Choluteca, Barrio El Tamarindo

Telefono: 2782-7079

Rubro de la empresa: Laboratorio de exámenes clínicos

Servicios que ofrece la empresa:

- Exámenes generales
- Hematología
- Química sanguínea
- Inmunología
- Parasitología
- Pruebas especiales
- Pruebas de antidoping
- Pruebas de paternidad por ADN

Objetivo mision y vision de la empresa: Nuestra misión es mejorar la salud, bienestar y calidad de vida de nuestros clientes y pacientes, usando nuestro conocimiento, experiencia, profesionalismo, tecnología médica y servicio al cliente superior, para brindar los servicios de análisis clínicos más confiables, contribuyendo así a la prevención, diagnóstico y tratamiento de los problemas de salud de los habitantes de la zona sur de Honduras.

Historia: Los Laboratorios Fleming fueron fundados en el año 2000 en la ciudad de Choluteca, Honduras. Los Laboratorios Fleming tienen más de 15 años de experiencia ofreciendo los servicios de laboratorio clínico a clientes particulares y empresas de la zona sur de Honduras.

Organigrama de la empresa

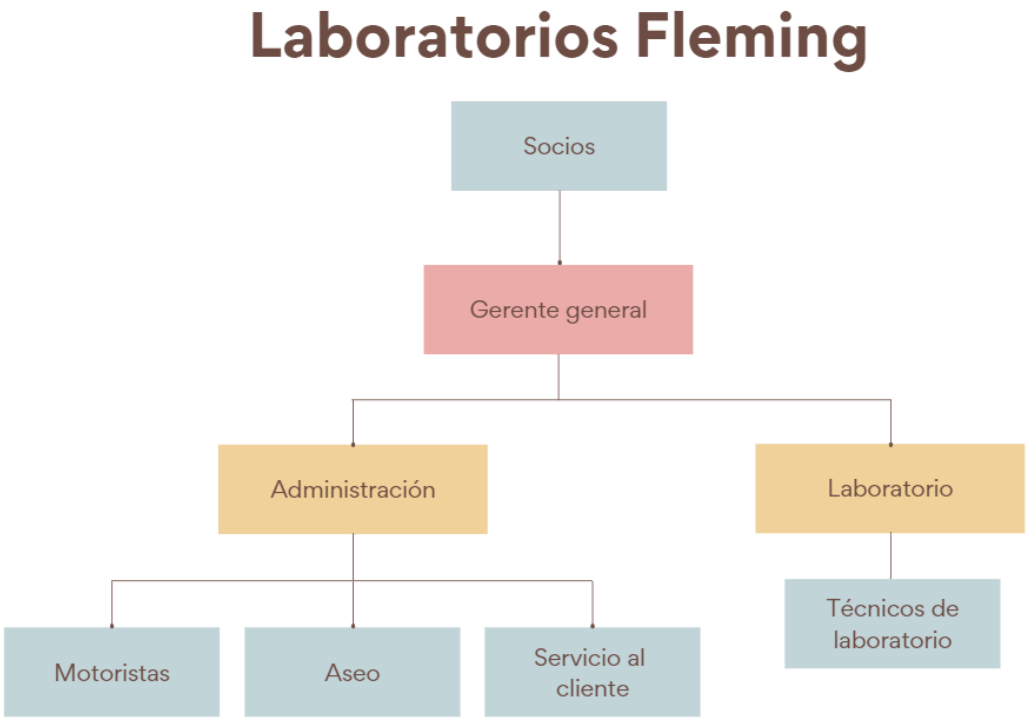


Diagrama de la base de datos

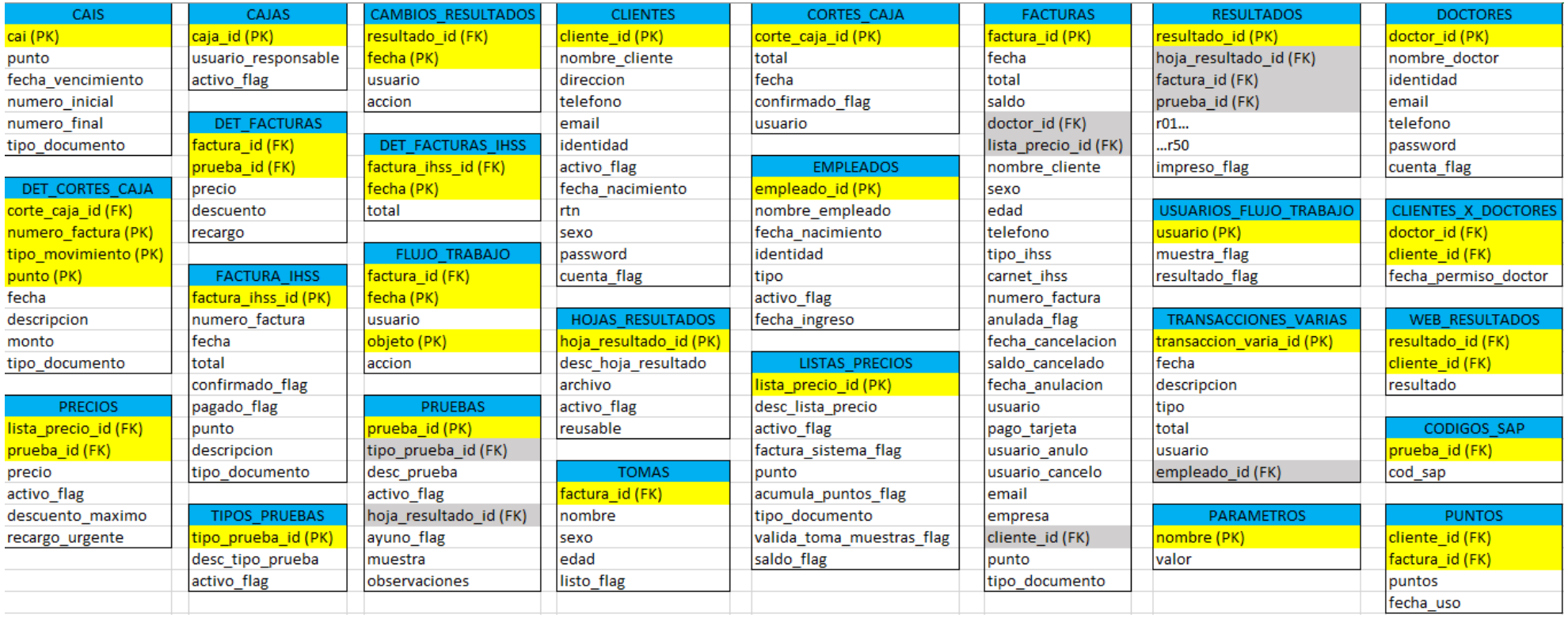
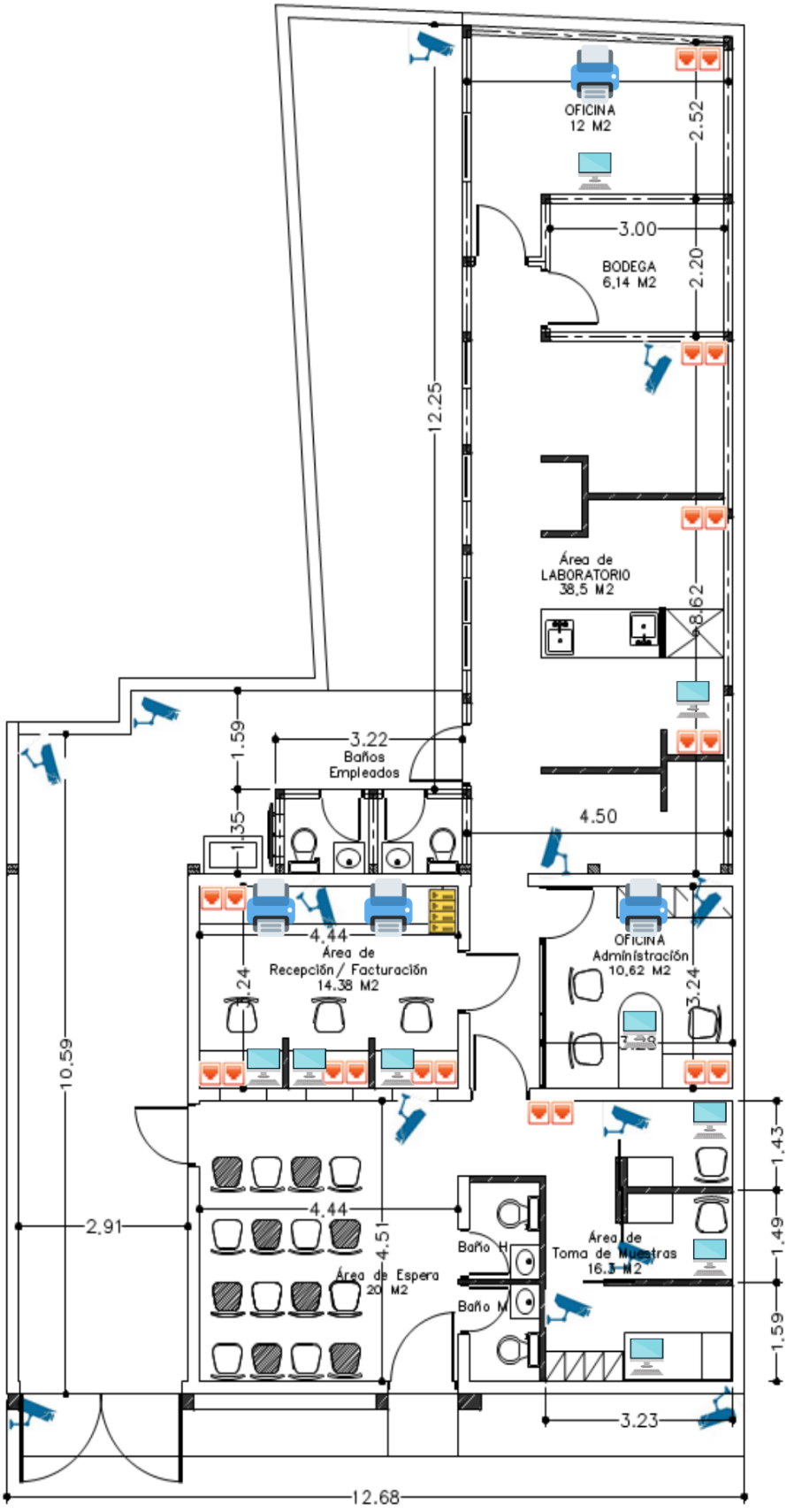


Diagrama físico de distribución de los activos



Perfiles de personas que tienen acceso al sistema

- El perfil de administrador: En este perfil se crea, quita o modifica las pruebas, precios, la lista de precios, y descuentos.
- El perfil de facturación (caja): Los empleados de este perfil hacen las facturas y cobran, luego hacen el corte de caja (el depósito).
- El perfil de técnico laboratorio: Los empleados de este perfil toman, entregan y reciben las muestras. (También pueden consultar resultados porque a veces es necesario ver el historial del paciente). Y escriben a mano la hoja de resultados.
- El perfil de pasar los resultados: Los empleados de este perfil digitan la hoja de resultados en el sistema (hecha a mano por los del perfil de técnico de laboratorio), la imprimen para ser revisados y luego la mandan.

1. Planificación

1.1 Planeación de la seguridad informática en la organización

Básicamente lo que haremos en esta etapa es definir el alcance del estudio informando a todo el personal implicado con los movimientos de la empresa. Así mismo identificando cuales son los activos principales de los servicios más importantes, ya sea como acceder el sistema para fines administrativos y financieros y almacenar la información que se genera en la empresa de forma segura en la base de datos.

Los problemas y las amenazas son muy importante que las identifiquemos para eliminar o reducirlas lo máximo posible. Las más importantes son referentes al acceso de terceros no implicados con la empresa y que nuestros softwares estén en la versión más reciente para que no existan problemas, y también se deben de mencionar las amenazas que están identificadas y están bajo control, pero buscar una manera aún más eficiente de controlarla o erradicarla.

En este caso, los salvaguardas, es muy importante tener el apoyo de todos los implicados ya que todo el personal tiene que colaborar con el jefe y administradores de que cada área, para que entre todos se adapten de las nuevas normas y procedimientos para que ellos se realicen de la mejor manera y progresiva para que sea consistente. Ya que tenemos que estar preparados para todo, de la seguridad de quien entre a nuestro sistema, o de quien entre de manera física a nuestra empresa y teniendo maneras de recuperación rápida de nuestra información por si ocurre un problema.

Para que la manera en la que controlamos los riesgos sea exitosa, siempre se debe de mantener en revisión diaria por todo el grupo que se encarga de la seguridad para que los niveles de riesgo no aumenten y que las salvaguardas estén siempre a disposición y se apliquen de manera correcta y continua.

1.2 Alcance del analisis y evaluacion de riesgos del sistema informático

El alcance establecido para el análisis son lograr evaluar los niveles de seguridad que maneja la empresa Laboratorios Fleming ubicados en Tegucigalpa, nos enfocaremos en lograr identificar las diferentes vulnerabilidades con las que cuenta la empresa como también analizar el nivel de seguridad que tiene la información que se maneja, accesos al sistema al igual que al ingreso del establecimiento, entre otros.

En los resultados esperamos obtener las diferentes amenazas que pueden afectar a la empresa para así poder implementar un plan de gestión de riesgos para evitar toda amenaza que pueda presentarse a futuro y así poder evitar grandes pérdidas.

1.3 Objetivos del análisis

- Conocer que tan bien está la seguridad actual para saber qué cambios se pueden llegar a hacer.
- Analizar la mejor manera en la que se puede erradicar los problemas.
- Identificar todos los riesgos y debilidades.
- Determinar si se necesita mejorar las medidas de seguridad.
- Identificar cada uno de los riesgos que tienen nuestros activos para minimizarlos con las salvaguardas.
- Influenciar a todo el personal a seguir las normas que se quieren implicar sobre la seguridad de información y recursos.
- Analizar el tiempo, esfuerzo y recursos necesarios para atacar los problemas.

2. Análisis de Riesgos

2.1 Descripción de los activos o recursos informáticos de la empresa

Descripción de activos

Activo	Descripción
Computadoras	Dispositivos conectados a la red para realizar varios tipos de tareas dentro del laboratorio. Por ejemplo: Facturar, revisar los resultados, enviar resultados por correo o Whatsapp, consultar el sistema del seguro social (para ver si la gente tiene derecho a un examen), ver el historial del paciente, ver los depósitos del banco, la planilla de los empleados, ofimática, pago de proveedores a través de sucursales electrónicas, y ver las cámaras de seguridad.
Impresoras	Dispositivos conectados a la red cuya función es imprimir cosas como: facturas, hojas de resultados, hojas de trabajo, recibos de planilla, recibos de caja, sobres para los resultados, e informes.
Gabinete de Red	Gabinete en donde se encuentra todo el equipo de red y comunicaciones. El cual está compuesto por: 2 patch panels, 1 switch, 1 NVR, organizadores de cables, el equipo terminal de Cable&Wireless (media converter y router), y 1 PDU.
Marcador Biométrico	Dispositivo conectado a red cuya función es llevar control de los horarios de entrada y salida de los empleados.
Control de acceso	Llavín magnético que funciona por medio del uso de tarjetas de proximidad para permitir el acceso al área de laboratorio a los empleados.
Scanners de código de barra	Dispositivos cuya función es escanear el código de barra de las hojas de trabajo y las muestras.
Impresora de etiqueta	Dispositivo para imprimir las etiquetas que se le ponen a las muestras.
Servidor	Servidor virtual, uno de desarrollo y otro de producción.

Características de los activos

Computadoras	Quad Core i5 5530, 8GB RAM, 240GB SSD.
Servidor	Quad Core i3 8100, 8GB RAM, 240GB SSD.
Impresoras	EPSON Workforce M200
Marcador biométrico y control de acceso	ZKTeco
Impresora de etiquetas	Brother QL700
Switch	Tenda 24 puertos
NVR	Lorex, 16 puertos POE
Router	Tenda, AC 2100
PDU	10 puertos

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 empresa.
	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 empresa.
	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 empresa o terceros externos sin autorización especial del responsable de la información o directivas de la empresa.
Integridad	No sensitiva (1)	La pérdida o modificación no autorizada de este activo podría causar un daño leve o nulo para la empresa.
	Sensitiva (2)	La pérdida o modificación de este activo podría causar un daño que genera perjuicios importantes que afecten a la empresa, 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 empresa 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 empresa.
	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 empresa 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 empresa	1	3	3	3
Impresoras	7	Importante para la empresa	1	2	2	2
Gabinete de red	10	Esencial para el desempeño de la empresa	2	3	3	3
Marcador biométrico	3	Importancia menor para la empresa	1	1	1	1
Control de acceso	3	Importancia menor para la empresa	2	1	2	2
Scanners de código de barra	8	Muy importante para la empresa	1	3	3	3
Impresora de etiqueta	7	Importante para la empresa	1	2	3	3
Servidor	10	Esencial para el desempeño de la empresa	3	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. Las amenazas informáticas para las empresas provienen en gran medida de ataques externos, aunque también existen amenazas internas (como robo de información o uso inadecuado de los sistemas).

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 empresa
3	La amenaza se materializa a lo mínimo una vez cada uno o dos años
4	La amenaza se materializa a lo mínimo una vez cada tres a seis meses.
5	La amenaza se materializa a lo mínimo una vez cada mes.

2.3.1 Listado de amenazas

Id	Amenaza	Descripción	P	Razón de clasificación
A1	Daños físicos al activo	Daños que son generados a los activos de la empresa ya sea por algún golpe recibido o dejado caer.	4	Han ocurrido algunos daños físicos dentro de la empresa por parte de empleados o ladrones.
A2	Daños de software al activo	Daños que son ocasionados por mal uso de algún software o mala utilización de programas que podrían causar problemas.	4	Es fácil que los empleados utilicen de mala manera el software por falta de capacitación
A3	Virus, gusanos y ransomware	Daños generados por la implantación de algún virus, gusanos o ransomware en los activos de la empresa como las computadoras	4	Es muy probable que los empleados conecten algún disco externo que contenga virus o descarguen alguno al utilizar las computadoras.

A4	Problemas de red	Problemas de conexión con el router a los activos o caídas de internet del servicio proveedor de internet	5	Es casi seguro que el proveedor de internet tenga alguna caída de servicio que podría inhabilitar las actividades de la empresa.
A5	Desperfectos al equipo	Fallos que se pueden ocasionar por algún equipo que venga mal de fábrica y tenga algún defecto.	2	Han habido ocasiones que se han comprado activos que han sido comprados en mal estado o que no funcionen adecuadamente.
A6	Fallas de escaneo	Fallas generadas por el mal escaneo al utilizar el activo de marcador biométrico o los scanners de código de barra.	5	Varias ocasiones al escanear facturas y productos las máquinas fallan, pero no es tan severo.
A7	Fallo de configuración	Fallas que puedan ocurrir en el presente o futuro en los activos debida a la mala instalacion y configuracion del activo	3	Algunos activos han sido mal instalados y configurados que han provocado demoras en las tareas de la empresa.
A8	Fallas al imprimir	Mala impresión de páginas al utilizar la impresora para generar facturas y exámenes de los clientes.	5	Siempre las impresoras fallan al momento de imprimir por una innumerable cantidad de razones
A9	Secuestro de registros	Secuestro de información por parte de personas de los servidores o computadoras.	1	No hay mucha competencia ni han habido tantos secuestros de registros en Honduras
A10	Phishing	Robo de información por parte del engaño o fraude que puedan ocasionar en los empleados	1	No han habido casos de robo de información ocasionados de parte externa
A11	Caída del activo por sobrecargas	Apagado o lentitud de los activos ocurridas por la gran carga que podrían recibir los activos	2	Siempre los activos tienen algún límite de carga que puedan tener, pero los activos de la empresa son algo potentes por lo tanto no puede ocurrir tan a menudo.
A12	Problemas por contraseñas	Problemas ocurridas por el acceso a otras personas por los empleados al utilizar contraseñas con un menor	3	Los empleados siempre buscan alguna contraseña fácil de colocar o fácil de

	débiles	nivel de seguridad		recordar y descifrar.
A13	Problemas por olvido o robo de cuentas	Problemas y pérdida de tiempo que ocurren cuando los empleados de la empresa pierden su contraseña y podría ser utilizada por alguna otra persona.	3	Ha habido casos en donde los empleados han olvidado sus credenciales para utilizar el sistema.
A14	Inundaciones	Fugas de agua o inundaciones ocasionados por ríos cercanos a la empresa.	1	Siempre hay casos de desastres naturales pero cerca de la empresa no hay ningún cuerpo de agua como río cercano.
A15	Terremotos	Movimientos súbitos de la tierra que podrían ocasionar la caída física de activos o daño a la infraestructura de la empresa	2	Se han presentado algunos temblores en algunas ocasiones en el área de la empresa
A16	Fuegos	Fuegos ocasionados por incendios ocurridos dentro de la empresa o algún otro edificio cercano	1	Puede que haya algún incendio que podría ocasionar pérdidas dentro del equipo
A17	Error humano	Fallos ocasionados por los errores que los empleados podrían ocasionar.	5	Siempre puede ocurrir en cualquier operación a realizar el error humano.

2.4 Amenazas clasificadas por su tipo y nivel de probabilidad

Las amenazas fueron clasificadas por medio de los activos que puedan afectar dentro de la empresa. Hay algunas amenazas que atacan a ciertos equipos y otras que no, por lo tanto la división se hizo de la manera mencionada. Luego, por cada amenaza identificada por equipo se le agregó un criterio de probabilidad que fue evaluado por cuantas veces esta amenaza podría ocurrir en la empresa en ciertas cantidades de tiempo. En este caso 1 siendo el valor de que es poco probable y 5 siendo de que la amenaza ocurra cada mes.

Tablas 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 empresa
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 a seis meses.
5	La amenaza se materializa a lo mínimo una vez cada mes.

2.4.1 Identificación de amenazas y criterio de probabilidad

Activo	**Descripción de amenazas**			**Criterio de probabilidad**
Activo	**Id**	**Amenaza**	**Tratamiento del riesgo**	**Probabilidad**
Computadora	**A1**	Daños físicos al activo	Mejor protección y ubicación segura para los equipos	2
	A2	Daños de software al activo	Mejor capacitación de los empleados para poder utilizar software sin preocupaciones	3

	A3	Virus, gusanos y ransomware	Instalación de antivirus y recomendar a los empleados que no inserten memorias no confiables.	2
	A5	Desperfectos al equipo	Conseguir equipos en tiendas confiables y revisión de equipos antes de utilizarlos	2
	A7	Fallo de configuración	Probar los equipos después de su configuración en el área de trabajo.	3
	A9	Secuestro de registros	Mejor seguridad e instalación de firewall en computadoras	1
	A10	Phishing	Capacitar a los empleados sobre el phishing y formas de no caer en fraudes.	1
	A12	Problemas por contraseñas débiles	Capacitar a los empleados al porqué utilizar una contraseña segura para sus computadoras	3
	A13	Problemas por olvido o robo de cuentas	Conseguir que los usuarios configuren sus cuentas con elementos que recordaran y no transmitir esa información con nadie	3
Impresoras	**A1**	Daños físicos al activo	Mejor protección y ubicación segura para las impresoras	3
	A5	Desperfectos al equipo	Conseguir equipos en tiendas confiables y revisión de equipos antes de utilizarlos.	2
	A7	Fallo de configuración	Probar las impresoras después de su instalación y configuración en el área de trabajo.	3
	A8	Fallas al imprimir	Realizar impresiones de prueba y darle mantenimiento a la impresora para la correcta instalación de cartuchos.	5
Gabinete de red	**A1**	Daños físicos al activo	Mejor protección y ubicación de una pared segura y aislada para instalar el gabinete de red.	1

	A4	Problemas de red	No saturar las descargas en las computadoras para que no falle el internet ni la comunicación del gabinete.	3
	A5	Desperfectos al equipo	Conseguir el gabinete de red en tiendas confiables y revisión de equipos antes de utilizarlos.	2
	A11	Caída del activo por sobrecargas	No sobreutilizar la red en cosas innecesarias o pesadas.	3
Marcador biométrico y control de acceso	**A1**	Daños físicos al activo	Conseguir controles de acceso muy resistentes a golpes.	1
	A5	Desperfectos al equipo	Buscar controles de acceso en tiendas confiables sobre seguridad.	2
	A6	Fallas de escaneo	Limpiar el control de acceso, darle mantenimiento y capacitar a los empleados a utilizar este acceso correctamente.	5
	A7	Fallo de configuración	Realizar mantenimiento y varias pruebas después de la instalación del activo.	3
Scanners de código de barra	**A1**	Daños físicos al activo	Colocar los scanners en lugares seguros y alejados de las personas no autorizadas a utilizarlos.	3
	A5	Desperfectos al equipo	Conseguir los scanners en tiendas y lugares seguros y confiables.	2
	A6	Fallas de escaneo	Limpiar y darle mantenimiento a los scanners, capacitar a los empleados sobre cómo utilizarlos.	5
Impresora de etiqueta	**A1**	Daños físicos al activo	Colocar las impresoras en ubicaciones aisladas y seguras.	3
	A5	Desperfectos al equipo	Conseguir las impresoras de tiendas confiables.	2
	A8	Fallas al imprimir	Mantenimiento a los equipos.	5

Servidor	**A1**	Daños físicos al activo	Dar acceso solo a personas capacitadas a los servidores para evitar daños por otras personas.	1
	A2	Daños de software al activo	Solo instalar software necesario y tener chequeo sobre las personas con acceso al servidor.	1
	A4	Problemas de red	Verificar que las conexiones sean correctas y no conectar dispositivos no verificados	2
	A7	Fallo de configuración	Realizar varias pruebas luego de la instalación del servidor	1
	A9	Secuestro de registros	Configurar de manera apropiada el firewall del servidor	1
	A11	Caída del activos por sobrecargas	Capacitar a los empleados a no utilizar consultas del servidor pesadas ni innecesarias.	3
Switch	**A1**	Daños físicos al activo	No mover el switch una vez instalado y dar acceso solo a personas capacitadas al acceso de este.	1
	A5	Desperfectos al equipo	Conseguir los switch en tiendas tecnológicas confiables y seguras	2
	A7	Fallo de configuración	Realizar varias pruebas sobre los switch antes de habilitarlos para su uso profesional.	2
NVR	**A1**	Daños físicos al activo	Colocar el NVR en una habitación segura y sin otras personas sin acceso a este activo.	2
	A5	Desperfectos al equipo	Conseguir el NVR en tiendas de seguridad y tecnología confiables y seguras.	3
	A7	Fallo de configuración	Realizar pruebas con las cámaras de seguridad para asegurar de que muestren imagen y video.	3

Router	**A1**	Daños físicos al activo	Instalar el router en una oficina central y con pocas personas con acceso.	1
	A4	Problemas de red	Estar al tanto sobre las conexiones al router y verificar que el proveedor de internet esté en servicio.	4
	A5	Desperfectos al equipo	Conseguir un router en tienda confiable y de buen rendimiento.	2
	A7	Fallo de configuración	Realizar varias pruebas al router para verificar que provea internet a otros dispositivos.	1
	A11	Caída del activos por sobrecargas	Capacitar a los empleados a que no utilicen el internet de la empresa en cosas innecesarias.	4
	A12	Problemas por contraseñas débiles	Colocar una contraseña muy segura para el acceso al router para que terceros no autorizados no utilicen el internet de la empresa.	2
PDU	**A1**	Daños físicos al activo	Colocar los PDU en lugares seguros y cerca de paredes para evitar golpes.	3
	A5	Desperfectos al equipo	Conseguir los PDU en tiendas tecnológicas seguras y revisar si el voltaje que recibe es adecuado y seguro.	2
Activos (General)	**A15**	Terremotos	Colocar todos los activos en lugares bastantes seguros y centrados para que no procedan a caerse por terremotos.	1
	A16	Fuegos	Tener extintores en cada rincón de habitación que contenga activos valiosos como computadoras y en la habitación del servidor.	1
	A17	Error humano	Capacitar a todos los empleados de la empresa para que conozcan y puedan utilizar de manera apropiada cada activo de su dia a dia para evitar error humano en lo mayor posible.	5

2.5 Matriz de impacto potencial

Una vez identificada las amenazas por activo en el apartado anterior, se les agregó un criterio de impacto a estas amenazas. El impacto se refiere a que tan dañino es que cada una de estas amenazas ocurran, y que tanto puedan afectar a la empresa esta amenaza al dañar el activo. La evaluación se hizo de 1 siendo el valor de que no tendría consecuencias si este activo se daña por cierto tiempo y 3 siendo el valor más alto que al dañarse este activo, la empresa no podría seguir con sus actividades laborales.

Tabla de estimación de impacto

Valor	Descripción
1	El daño derivado de la materialización de la amenaza no tiene consecuencias relevantes para la organización.
2	El daño derivado de la materialización de la amenaza tiene consecuencias reseñables para la organización.
3	El daño derivado de la materialización de la amenaza tiene consecuencias graves reseñables para la organización.

2.5.1 Tabla de matriz de impacto potencial

Activo	**Descripción de amenazas**		**Criterios de impacto**
Activo	**Id**	**Amenaza**	**Impacto**
Computadora	**A1**	Daños físicos al activo	2
	A2	Daños de software al activo	2
	A3	Virus, gusanos y ransomware	3
	A5	Desperfectos al equipo	1
	A7	Fallo de configuración	1
	A9	Secuestro de registros	1
	A10	Phishing	1

	A12	Problemas por contraseñas débiles	1
	A13	Problemas por olvido o robo de cuentas	1
Impresoras	**A1**	Daños físicos al activo	1
	A5	Desperfectos al equipo	1
	A7	Fallo de configuración	2
	A8	Fallas al imprimir	1
Gabinete de red	**A1**	Daños físicos al activo	2
	A4	Problemas de red	2
	A5	Desperfectos al equipo	2
	A11	Caída del activo por sobrecargas	3
Marcador biométrico y control de acceso	**A1**	Daños físicos al activo	1
	A5	Desperfectos al equipo	1
	A6	Fallas de escaneo	1
	A7	Fallo de configuración	1
Scanners de código de barra	**A1**	Daños físicos al activo	1
	A5	Desperfectos al equipo	1
	A6	Fallas de escaneo	2
Impresora de etiqueta	**A1**	Daños físicos al activo	1
	A5	Desperfectos al equipo	1
	A8	Fallas al imprimir	3
Servidor	**A1**	Daños físicos al activo	3
	A2	Daños de software al activo	3
	A4	Problemas de red	3
	A7	Fallo de configuración	2
	A9	Secuestro de registros	2

	A11	Caída del activos por sobrecargas	3
Switch	**A1**	Daños físicos al activo	1
	A5	Desperfectos al equipo	2
	A7	Fallo de configuración	2
NVR	**A1**	Daños físicos al activo	1
	A5	Desperfectos al equipo	1
	A7	Fallo de configuración	1
Router	**A1**	Daños físicos al activo	1
	A4	Problemas de red	3
	A5	Desperfectos al equipo	1
	A7	Fallo de configuración	2
	A11	Caída del activos por sobrecargas	3
	A12	Problemas por contraseñas débiles	2
PDU	**A1**	Daños físicos al activo	1
	A5	Desperfectos al equipo	1
Activos (General)	**A15**	Terremotos	3
	A16	Fuegos	3
	A17	Error humano	2

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 marginal, luego los que están en el rango de 3 y 8 son riesgos apreciables, los riesgos entre el rango de 9 y 12 son importantes, y los mayores o iguales a 15 son riesgos graves.

Matriz de potencial de riesgos						
		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

	Riesgo Grave
	Riesgo importante
	Riesgo apreciable
	Riesgo marginal

Valoración o estimación del impacto y probabilidad					
Activo	**Riesgo**	**Impacto**	**Probabilidad**	**Valor**	**Nivel de riesgo**
Computadora	Daños físicos al activo	2	2	4	APRECIABLE
	Daños de software al activo	2	3	6	APRECIABLE

	Virus, gusanos y ransomware	3	2	6	APRECIABLE
	Desperfectos al equipo	1	2	2	MARGINAL
	Fallo de configuración	1	3	3	APRECIABLE
	Secuestro de registros	1	1	1	MARGINAL
	Phishing	1	1	1	MARGINAL
	Problemas por contraseñas débiles	1	3	3	APRECIABLE
	Problemas por olvido o robo de cuentas	1	3	3	APRECIABLE
Impresoras	Daños físicos al activo	1	3	3	APRECIABLE
	Desperfectos al equipo	1	2	2	MARGINAL
	Fallo de configuración	2	3	6	APRECIABLE
	Fallas al imprimir	1	5	5	APRECIABLE
Gabinete de red	Daños físicos al activo	2	1	2	MARGINAL
	Problemas de red	2	3	6	APRECIABLE
	Desperfectos al equipo	2	2	4	APRECIABLE
	Caída del activo por sobrecargas	3	3	9	IMPORTANTE
Marcador biométrico y control de acceso	Daños físicos al activo	1	1	1	MARGINAL
	Desperfectos al equipo	1	2	2	MARGINAL
	Fallas de escaneo	1	5	5	APRECIABLE
	Fallo de configuración	1	3	3	APRECIABLE
Scanners de código de barra	Daños físicos al activo	1	3	3	APRECIABLE
	Desperfectos al equipo	1	2	2	MARGINAL
	Fallas de escaneo	2	5	10	IMPORTANTE
Impresora de etiqueta	Daños físicos al activo	1	3	3	APRECIABLE

	Desperfectos al equipo	1	2	2	MARGINAL
	Fallas al imprimir	3	5	15	MUY GRAVE
Servidor	Daños físicos al activo	3	1	3	APRECIABLE
	Daños de software al activo	3	1	3	APRECIABLE
	Problemas de red	3	2	6	APRECIABLE
	Fallo de configuración	2	1	2	MARGINAL
	Secuestro de registros	2	1	2	MARGINAL
	Caída del activos por sobrecargas	3	3	9	IMPORTANTE
Switch	Daños físicos al activo	1	1	1	MARGINAL
	Desperfectos al equipo	2	2	4	APRECIABLE
	Fallo de configuración	2	2	4	APRECIABLE
NVR	Daños físicos al activo	1	2	2	MARGINAL
	Desperfectos al equipo	1	3	3	APRECIABLE
	Fallo de configuración	1	3	3	APRECIABLE
Router	Daños físicos al activo	1	1	1	MARGINAL
	Problemas de red	3	4	12	IMPORTANTE
	Desperfectos al equipo	1	2	2	MARGINAL
	Fallo de configuración	2	1	2	MARGINAL
	Caída del activos por sobrecargas	3	4	12	IMPORTANTE
	Problemas por contraseñas débiles	2	2	4	APRECIABLE
PDU	Daños físicos al activo	1	3	3	APRECIABLE
	Desperfectos al equipo	1	2	2	MARGINAL

Activos (General)	Terremotos	3	1	3	APRECIABLE
	Fuegos	3	1	3	APRECIABLE
	Error humano	2	5	10	IMPORTANTE

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

En esta tabla estamos seccionando por los riesgos y activos, primero mostramos todos los riesgos marginales seccionado por los activos y cada uno de los activos con sus riesgos, para luego poner la cantidad de riesgos que hay en cada activo, y así en cada uno de los 4 riesgos.

Número de amenazas por potencial de riesgo y tipo de activo		
Riesgo marginales		
Activos	Riesgos	Total
Computadora	Desperfectos al equipo	3
	Secuestro de registros	
	Phishing	
Impresoras	Desperfectos al equipo	1
Gabinete de red	Daños físicos al activo	1
Marcador biométrico y control de acceso	Daños físicos al activo	2
	Desperfectos al equipo	
Scanners de código de barra	Desperfectos al equipo	1
Impresora de etiqueta	Desperfectos al equipo	1
Servidor	Fallo de configuración	2
	Secuestro de registros	

Switch	Daños físicos al activo	1
NVR	Daños físicos al activo	1
Router	Daños físicos al activo	3
	Desperfectos al equipo	
	Fallo de configuración	
PDU	Desperfectos al equipo	1
Total riesgos marginales		17
Riesgos apreciables		
Computadora	Daños físicos al activo	6
	Daños de software al activo	
	Fallo de configuración	
	Problemas por contraseñas débiles	
	Problemas por olvido o robo de cuentas	
	Virus, gusanos y ransomware	
Impresoras	Daños físicos al activo	3
	Fallo de configuración	
	Fallas al imprimir	
Gabinete de red	Problemas de red	2
	Desperfectos al equipo	
Marcador biométrico y control de acceso	Fallas de escaneo	2
	Fallo de configuración	
Scanners de código de barra	Daños físicos al activo	1
Impresora de etiqueta	Daños físicos al activo	1
Servidor	Daños físicos al activo	3
	Problemas de red	

	Daños de software al activo	
Switch	Desperfectos al equipo	2
	Fallo de configuración	
NVR	Desperfectos al equipo	2
	Fallo de configuración	
Router	Problemas por contraseñas débiles	1
PDU	Daños físicos al activo	1
Activos (General)	Terremotos	2
	Fuegos	
Total riesgos apreciables		26
Riesgos importantes		
Gabinete de red	Caída del activo por sobrecargas	1
Scanners de código de barra	Fallas de escaneo	1
Impresora de etiqueta	Daños físicos al activo	1
Servidor	Caída del activos por sobrecargas	1
Router	Problemas de red	2
	Caída del activos por sobrecargas	
Activos (General)	Error humano	1
Total riesgos importantes		7
Riesgos muy graves		
Impresora de etiqueta	Fallas al imprimir	1
Total riesgos muy graves		1
Total de riesgos		51

2.8 Matriz de riesgo potencial

En esta tabla sacamos los datos de una unión entre la tabla de Riesgo Potencial y la Tabla de matriz de impacto potencial ya que muestra el código de amenaza y la descripción de la amenaza, también utilizar el nivel de impacto, nivel de probabilidad, riesgo potencial y la zona de riesgo.

Tipo de activo	Codigo Amenaza	Amenaza	Impacto	Nivel de Probabilidad	Riesgo Potencial	Zona de Riesgo
Computadora	**A1**	Daños físicos al activo	2	2	4	APRECIABLE
	A2	Daños de software al activo	2	3	6	APRECIABLE
	A3	Virus, gusanos y ransomware	3	2	6	APRECIABLE
	A5	Desperfectos al equipo	1	2	2	MARGINAL
	A7	Fallo de configuración	1	3	3	APRECIABLE
	A9	Secuestro de registros	1	1	1	MARGINAL
	A10	Phishing	1	1	1	MARGINAL
	A12	Problemas por contraseñas débiles	1	3	3	APRECIABLE
	A13	Problemas por olvido o robo de cuentas	1	3	3	APRECIABLE
Impresoras	**A1**	Daños físicos al activo	1	3	3	APRECIABLE
	A5	Desperfectos al equipo	1	2	2	MARGINAL
	A7	Fallo de configuración	2	3	6	APRECIABLE
	A8	Fallas al imprimir	1	5	5	APRECIABLE
Gabinete de red	**A1**	Daños físicos al activo	2	1	2	MARGINAL
	A4	Problemas de red	2	3	6	APRECIABLE
	A5	Desperfectos al equipo	2	2	4	APRECIABLE
	A11	Caída del activo por sobrecargas	3	3	9	IMPORTANTE
Marcador biométrico y	**A1**	Daños físicos al activo	1	1	1	MARGINAL
	A5	Desperfectos al equipo	1	2	2	MARGINAL

control de acceso	**A6**	Fallas de escaneo	1	5	5	APRECIABLE
	A7	Fallo de configuración	1	3	3	APRECIABLE
Scanners de código de barra	**A1**	Daños físicos al activo	1	3	3	APRECIABLE
	A5	Desperfectos al equipo	1	2	2	MARGINAL
	A6	Fallas de escaneo	2	5	10	IMPORTANTE
Impresora de etiqueta	**A1**	Daños físicos al activo	1	3	3	APRECIABLE
	A5	Desperfectos al equipo	1	2	2	MARGINAL
	A8	Fallas al imprimir	3	5	15	MUY GRAVE
Servidor	**A1**	Daños físicos al activo	3	1	3	APRECIABLE
	A2	Daños de software al activo	3	1	3	APRECIABLE
	A4	Problemas de red	3	2	6	APRECIABLE
	A7	Fallo de configuración	2	1	2	MARGINAL
	A9	Secuestro de registros	2	1	2	MARGINAL
	A11	Caída del activos por sobrecargas	3	3	9	IMPORTANTE
Switch	**A1**	Daños físicos al activo	1	1	1	MARGINAL
	A5	Desperfectos al equipo	2	2	4	APRECIABLE
	A7	Fallo de configuración	2	2	4	APRECIABLE
NVR	**A1**	Daños físicos al activo	1	2	2	MARGINAL
	A5	Desperfectos al equipo	1	3	3	APRECIABLE
	A7	Fallo de configuración	1	3	3	APRECIABLE
Router	**A1**	Daños físicos al activo	1	1	1	MARGINAL
	A4	Problemas de red	3	4	12	IMPORTANTE
	A5	Desperfectos al equipo	1	2	2	MARGINAL
	A7	Fallo de configuración	2	1	2	MARGINAL
	A11	Caída del activos por sobrecargas	3	4	12	IMPORTANTE
	A12	Problemas por contraseñas débiles	2	2	4	APRECIABLE
PDU	**A1**	Daños físicos al activo	1	3	3	APRECIABLE

	A5	Desperfectos al equipo	1	2	2	MARGINAL
Activos (General)	**A15**	Terremotos	3	1	3	APRECIABLE
	A16	Fuegos	3	1	3	APRECIABLE
	A17	Error humano	2	5	10	IMPORTANTE

2.9 Salvaguardas o controles existentes

Luego de especificar los potenciales riesgos a los activos se prosigue a establecer las salvaguardas o controles existentes que existen para proteger a los activos en el caso de una posible amenaza. La efectividad de los controles se dividieron en 3 niveles: el nivel 1 representa la menor cantidad de efectividad, el nivel 2 representa una cantidad regular de efectividad, y el nivel 3 representa la mayor cantidad de efectividad.

Nivel	**Descripción de la Efectividad del Control**
1	Es muy probable que el control falle ante la presencia de una amenaza.
2	El control es funcional y es probable que funcione en la mayoría de los casos en los que haya algún tipo de amenaza.
3	Está garantizado que el control va a funcionar y va a cumplir con los niveles de protección necesarios para proteger los equipos.

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

En esta tabla se establecen los niveles de efectividad de los controles implementados a cada activo con sus posibles amenazas y su nivel de efectividad. Primero se especifica el activo, luego se especifican sus posibles amenazas, después se le asigna el nivel de efectividad del control utilizado para las posibles amenazas, y por último se hace un comentario con respeto a la seguridad del activo.

Activos	Amenazas	Nivel de Efectividad del Control	Comentarios
Computadoras	Daños físicos al equipo	**2**	Los usuarios no tienen permisos de administrador.
	Daños de software	**2**	
	Robo y saqueo de los equipos	**2**	
	Daños por incendios	**3**	
	Daños por inundaciones	**3**	
Impresoras	Daños físicos al equipo	**2**	Hay varias impresoras de repuesto en caso de que se arruine una.
	Daños de software	**3**	
	Robo y saqueo de los equipos	**2**	
	Daños por incendios	**3**	
	Daños por inundaciones	**3**	
Gabinete de Red	Daños físicos al equipo	**2**	El gabinete de red está localizado a una altura en donde es difícil que sufra daños por inundaciones.
	Daños de software	**2**	

	Robo y saqueo de los equipos	**3**	
	Daños por incendios	**3**	
	Daños por inundaciones	**3**	
Marcador Biométrico	Daños físicos al equipo	**2**	Está conectado a la red junto con el control de acceso.
	Daños de software	**3**	
	Robo y saqueo de los equipos	**2**	
	Daños por incendios	**2**	
	Daños por inundaciones	**2**	
Control de Acceso	Daños físicos al equipo	**3**	Está conectado a la red junto con el marcador biométrico.
	Daños de software	**3**	
	Robo y saqueo de los equipos	**3**	
	Daños por incendios	**3**	
	Daños por inundaciones	**3**	
Scanners de Código de Barra	Daños físicos al equipo	**2**	Hay scanners de código de barra

	Daños de software	**3**	de repuesto en el caso de que se arruine uno.
	Robo y saqueo de los equipos	**1**	
	Daños por incendios	**3**	
	Daños por inundaciones	**3**	
Impresora de Etiquetas	Daños físicos al equipo	**2**	Hay varias impresoras de etiquetas de repuesto en caso de que se arruine una.
	Daños de software	**3**	
	Robo y saqueo de los equipos	**2**	
	Daños por incendios	**1**	
	Daños por inundaciones	**1**	
Servidor	Daños físicos al equipo	**2**	Hay un servidor de respuesta en donde hay una copia exacta del sistema. (Se hacen 6 respaldos al día).
	Daños de software	**2**	
	Robo y saqueo de los equipos	**3**	
	Daños por incendios	**2**	
	Daños por inundaciones	**3**	

2.10 Impacto residual

El impacto residual se define como el daño sobre el activo debido a la materialización de la amenaza aún existiendo las salvaguardas que lo protejan. En esta tabla, se identificó las amenazas y los activos, al igual que los controles de cada amenaza por activo junto con que tipo de control es este. Luego se informa si este control está siendo implementado dentro de la empresa y se obtienen los valores de la eficacia de control de la tabla de 2.9.1 Controles implementados y el valor del impacto potencial de la tabla 2.5.1 Impacto potencial.
Para obtener el valor del impacto residual lo que se hace es dividir el Impacto Potencial entre la Eficacia del Control.

Tipo de activo	Amenazas	Controles	Tipos de control	Control implementado?	Eficacia del control	Impacto potencial	Impacto residual
Computadoras	Daños físicos al equipo	Los equipos deben de estar colocados en zonas de poco acceso, aseguradas y bien colocadas	Minimizador	Si	2	2	1
	Daños de software	Los equipos solo se deben instalar los programas necesarios y no conectar otros dispositivos de almacenamiento	Prevención	Si	2	2	1
	Robo y saqueo de los equipos	Los equipos deben estar asegurados por garantías al igual que colocarlos en lugares seguros	Minimizador	Si	2	3	1.5
	Daños por incendios	Se debe de tener un agente químico protegiendo estos equipos al igual que extintores cercanos	Minimizador	Si	3	3	1
	Daños por inundaciones	Asegurar que la calle tenga un buen drenaje y no dejar los equipos en el suelo	Minimizador	Si	3	3	1
Impresoras	Daños físicos al equipo	Los equipos deben de estar colocados en zonas de poco acceso, aseguradas y bien	Minimizador	Si	2	1	0.5

		colocadas					
	Daños de software	Los equipos solo se deben instalar los programas necesarios y no conectar otros dispositivos de almacenamiento	Prevención	Si	3	1	0.33
	Robo y saqueo de los equipos	Los equipos deben estar asegurados por garantías al igual que colocarlos en lugares seguros	Minimizador	Si	2	3	1.5
	Daños por incendios	Se debe de tener un agente químico protegiendo estos equipos al igual que extintores cercanos	Minimizador	Si	3	3	1
	Daños por inundaciones	Asegurar que la calle tenga un buen drenaje y no dejar los equipos en el suelo	Minimizador	Si	3	3	1
Gabinete de red	Daños físicos al equipo	El equipo debe de estar colocado en zonas de poco acceso, aseguradas y bien colocadas	Minimizador	Si	1	2	2
	Daños de software	El equipo solo se debe instalar los programas necesarios y no conectar otros dispositivos de almacenamiento	Prevención	Si	1	2	2
	Robo y saqueo de los equipos	El equipo debe estar asegurados por garantías al igual que colocarlo en lugares seguros	Minimizador	Si	3	3	1
	Daños por incendios	Se debe de tener un agente químico protegiendo este equipo al igual que extintores cercanos	Minimizador	Si	3	3	1
	Daños por inundaciones	Asegurar que la calle tenga un buen drenaje y no colocar este equipo cerca del suelo	Minimizador	Si	3	3	1
Marcador biométric	Daños físicos al	El equipo debe de estar colocado en zonas de poco	Minimizador	Si	2	1	0.5

o	equipo	acceso, aseguradas y bien colocadas					
	Daños de software	El equipo solo se debe instalar los programas necesarios y no conectar otros dispositivos de almacenamiento	Prevención	Si	3	1	0.33
	Robo y saqueo de los equipos	El equipo debe estar asegurados por garantías al igual que colocarlo en lugares seguros	Minimizador	Si	2	2	1
	Daños por incendios	Se debe de tener un agente químico protegiendo este equipo al igual que extintores cercanos	Minimizador	Si	2	3	1.5
	Daños por inundaciones	Asegurar que la calle tenga un buen drenaje y no colocar este equipo cerca del suelo	Minimizador	Si	2	3	1.5
Control de acceso	Daños físicos al equipo	El equipo debe de estar colocado en zonas de poco acceso, aseguradas y bien colocadas	Minimizador	Si	3	1	0.33
	Daños de software	El equipo solo se debe instalar los programas necesarios y no conectar otros dispositivos de almacenamiento	Prevención	Si	3	1	0.33
	Robo y saqueo de los equipos	El equipo debe estar asegurados por garantías al igual que colocarlo en lugares seguros	Minimizador	Si	3	2	0.67
	Daños por incendios	Se debe de tener un agente químico protegiendo este equipo al igual que extintores cercanos	Minimizador	Si	3	3	1
	Daños por inundaciones	Asegurar que la calle tenga un buen drenaje y no colocar este equipo cerca del suelo	Minimizador	Si	3	3	1
Scanners	Daños	Los equipos deben de estar	Minimizad	Si	2	1	0.5

de código de barra	físicos al equipo	colocados en zonas de poco acceso, aseguradas y bien colocadas	or				
	Daños de software	Los equipos solo se deben instalar los programas necesarios y no conectar otros dispositivos de almacenamiento	Prevención	Si	3	1	0.33
	Robo y saqueo de los equipos	Los equipos deben estar asegurados por garantías al igual que colocarlos en lugares seguros	Minimizador	Si	1	3	3
	Daños	Se debe de tener un agente químico protegiendo estos equipos al igual que extintores cercanos	Minimizador	Si	3	3	1
	Daños por inundaciones	Asegurar que la calle tenga un buen drenaje y no dejar los equipos en el suelo	Minimizador	Si	3	3	1
Impresora de etiquetas	Daños físicos al equipo	Los equipos deben de estar colocados en zonas de poco acceso, aseguradas y bien colocadas	Minimizador	Si	2	1	0.5
	Daños de software	Los equipos solo se deben instalar los programas necesarios y no conectar otros dispositivos de almacenamiento	Prevención	Si	3	1	0.33
	Robo y saqueo de los equipos	Los equipos deben estar asegurados por garantías al igual que colocarlos en lugares seguros	Minimizador	Si	2	3	1.5
	Daños por incendios	Se debe de tener un agente químico protegiendo estos equipos al igual que extintores cercanos	Minimizador	Si	1	3	3
	Daños por inundaciones	Asegurar que la calle tenga un buen drenaje y no dejar los equipos en el suelo	Minimizador	Si	1	3	3

Servidor	Daños físicos al equipo	El equipo debe de estar colocado en zonas de poco acceso y restringida de personas no deseables	Minimizador	Si	2	3	1.5
	Daños de software	El equipo solo se debe instalar los programas necesarios y no conectar otros dispositivos de almacenamiento	Prevención	Si	2	3	1.5
	Robo y saqueo de los equipos	El equipo debe estar asegurados por garantías al igual que colocarlo en lugares seguros con buena seguridad	Minimizador	Si	3	3	1
	Daños por incendios	Se debe de tener un agente químico protegiendo este equipo al igual que extintores cercanos	Minimizador	No	2	3	1.5
	Daños por inundaciones	Asegurar que la calle tenga un buen drenaje y colocar un piso falso para poner el servidor encima de este	Minimizador	No	3	3	1

2.11 Matriz de impacto residual y riesgo residual

En esta tabla estamos calculando el riesgo residual al mismo tiempo que mostramos los datos de la tabla pasada, ya que la manera de obtener el valor del riesgo residual es haciendo la multiplicación del Impacto Residual con la probabilidad y así mismo mostramos la zona de riesgo a la cual pertenecen.

Tipo de activo	Amenazas	Controles	Tipos de control	Eficacia del control	Impacto potencial	Impacto residual	Nivel de probabilidad	Riesgo residual	Zona de riesgo residual
Computadoras	Daños físicos al equipo	Los equipos deben de estar colocados en zonas de poco acceso, aseguradas y bien colocadas	Minimizador	2	2	1	2	2	APRECIABLE
	Daños de software	Los equipos solo se deben instalar los programas necesarios y no conectar otros dispositivos de almacenamiento	Prevención	2	2	1	3	3	APRECIABLE
	Robo y saqueo de los equipos	Los equipos deben estar asegurados por garantías al igual que colocarlos en lugares seguros	Minimizador	2	3	1.5	2	3	APRECIABLE

	Daños por incendios	Se debe de tener un agente químico protegiendo estos equipos al igual que extintores cercanos	Minimizador	3	3	1	2	2	MARGINAL
	Daños por inundaciones	Asegurar que la calle tenga un buen drenaje y no dejar los equipos en el suelo	Minimizador	3	3	1	3	3	APRECIABLE
Impresoras	Daños físicos al equipo	Los equipos deben de estar colocados en zonas de poco acceso, aseguradas y bien colocadas	Minimizador	2	1	0.5	1	0.5	MARGINAL
	Daños de software	Los equipos solo se deben instalar los programas necesarios y no conectar otros dispositivos de almacenamiento	Prevención	3	1	0.33	1	0.33	MARGINAL
	Robo y saqueo de los equipos	Los equipos deben estar asegurados por garantías al igual que colocarlos en lugares seguros	Minimizador	2	3	1.5	3	4.5	APRECIABLE

	Daños por incendios	Se debe de tener un agente químico protegiendo estos equipos al igual que extintores cercanos	Minimizador	3	3	1	3	3	APRECIABLE
	Daños por inundaciones	Asegurar que la calle tenga un buen drenaje y no dejar los equipos en el suelo	Minimizador	3	3	1	3	3	APRECIABLE
Gabinete de red	Daños físicos al equipo	El equipo debe de estar colocado en zonas de poco acceso, aseguradas y bien colocadas	Minimizador	1	2	2	2	4	MARGINAL
	Daños de software	El equipo solo se debe instalar los programas necesarios y no conectar otros dispositivos de almacenamiento	Prevención	1	2	2	3	6	APRECIABLE
	Robo y saqueo de los equipos	El equipo debe estar asegurados por garantías al igual que colocarlo en lugares seguros	Minimizador	3	3	1	5	5	APRECIABLE

	Daños por incendios	Se debe de tener un agente químico protegiendo este equipo al igual que extintores cercanos	Minimizador	3	3	1	1	1	MARGINAL
	Daños por inundaciones	Asegurar que la calle tenga un buen drenaje y no colocar este equipo cerca del suelo	Minimizador	3	3	1	3	3	APRECIABLE
Marcador biométrico	Daños físicos al equipo	El equipo debe de estar colocado en zonas de poco acceso, aseguradas y bien colocadas	Minimizador	2	1	0.5	2	1	APRECIABLE
	Daños de software	El equipo solo se debe instalar los programas necesarios y no conectar otros dispositivos de almacenamiento	Prevención	3	1	0.33	3	0.99	IMPORTANTE
	Robo y saqueo de los equipos	El equipo debe estar asegurados por garantías al igual que colocarlo en lugares seguros	Minimizador	2	2	1	1	1	MARGINAL

	Daños por incendios	Se debe de tener un agente químico protegiendo este equipo al igual que extintores cercanos	Minimizador	2	3	1.5	2	3	MARGINAL
	Daños por inundaciones	Asegurar que la calle tenga un buen drenaje y no colocar este equipo cerca del suelo	Minimizador	2	3	1.5	5	7.5	APRECIABLE
Control de acceso	Daños físicos al equipo	El equipo debe de estar colocado en zonas de poco acceso, aseguradas y bien colocadas	Minimizador	3	1	0.33	3	0.99	APRECIABLE
	Daños de software	El equipo solo se debe instalar los programas necesarios y no conectar otros dispositivos de almacenamiento	Prevención	3	1	0.33	3	0.99	APRECIABLE
	Robo y saqueo de los equipos	El equipo debe estar asegurados por garantías al igual que colocarlo en lugares seguros	Minimizador	3	2	0.67	2	1.34	MARGINAL

	Daños por incendios	Se debe de tener un agente químico protegiendo este equipo al igual que extintores cercanos	Minimizador	3	3	1	5	5	IMPORTANTE
	Daños por inundaciones	Asegurar que la calle tenga un buen drenaje y no colocar este equipo cerca del suelo	Minimizador	3	3	1	3	3	APRECIABLE
Scanners de código de barra	Daños físicos al equipo	Los equipos deben de estar colocados en zonas de poco acceso, aseguradas y bien colocadas	Minimizador	2	1	0.5	2	1	MARGINAL
	Daños de software	Los equipos solo se deben instalar los programas necesarios y no conectar otros dispositivos de almacenamiento	Prevención	3	1	0.33	5	1.65	MUY GRAVE
	Robo y saqueo de los equipos	Los equipos deben estar asegurados por garantías al igual que colocarlos en lugares seguros	Minimizador	1	3	3	1	3	APRECIABLE

	Daños	Se debe de tener un agente químico protegiendo estos equipos al igual que extintores cercanos	Minimizador	3	3	1	1	1	APRECIABLE
	Daños por inundaciones	Asegurar que la calle tenga un buen drenaje y no dejar los equipos en el suelo	Minimizador	3	3	1	2	2	APRECIABLE
Impresora de etiquetas	Daños físicos al equipo	Los equipos deben de estar colocados en zonas de poco acceso, aseguradas y bien colocadas	Minimizador	2	1	0.5	1	0.5	MARGINAL
	Daños de software	Los equipos solo se deben instalar los programas necesarios y no conectar otros dispositivos de almacenamiento	Prevención	3	1	0.33	1	0.33	MARGINAL
	Robo y saqueo de los equipos	Los equipos deben estar asegurados por garantías al igual que colocarlos en lugares seguros	Minimizador	2	3	1.5	3	4.5	IMPORTANTE

	Daños por incendios	Se debe de tener un agente químico protegiendo estos equipos al igual que extintores cercanos	Minimizador	1	3	3	1	3	MARGINAL
	Daños por inundaciones	Asegurar que la calle tenga un buen drenaje y no dejar los equipos en el suelo	Minimizador	1	3	3	2	6	APRECIABLE
Servidor	Daños físicos al equipo	El equipo debe de estar colocado en zonas de poco acceso y restringida de personas no deseables	Minimizador	2	3	1.5	2	3	APRECIABLE
	Daños de software	El equipo solo se debe instalar los programas necesarios y no conectar otros dispositivos de almacenamiento	Prevención	2	3	1.5	2	3	MARGINAL

	Robo y saqueo de los equipos	El equipo debe estar asegurados por garantías al igual que colocarlo en lugares seguros con buena seguridad	Minimizador	3	3	1	3	3	APRECIABLE
	Daños por incendios	Se debe de tener un agente químico protegiendo este equipo al igual que extintores cercanos	Minimizador	2	3	1.5	3	4.5	APRECIABLE
	Daños por inundaciones	Asegurar que la calle tenga un buen drenaje y colocar un piso falso para poner el servidor encima de este	Minimizador	3	3	1	1	1	MARGINAL

3. Gestión de Riesgos

3.1 Comunicación del riesgo y recomendaciones

Con la etapa de análisis de riesgos finalizada se prosigue a presentarle a los directivos de la empresa Laboratorios Fleming y a los encargados de las áreas en donde se encuentran los riesgos, los resultados para que ellos decidan qué acciones prefieren tomar para poder lidiar con los posibles daños.

Se recomienda que los riesgos dentro del rango 1 a 2 (riesgos marginales) y los riesgos de rango 3 a 8 (riesgos apreciables) sean considerados aceptables con tal de que estén siendo vigilados y se empiece a considerar posibles soluciones en el caso de que en el futuro causen algún tipo de daño en la empresa.

En el caso de los riesgos dentro del rango de 9 a 12 (riesgos importantes) y los riesgos de rango 13 a 15 (riesgos graves), se recomienda que se implementen soluciones lo más pronto posible ya que estos son riesgos de alto nivel que tienen grandes posibilidades de causar daños dentro de la empresa.

Las opciones de tratamiento que se sugieren para los riesgos importantes y graves son los siguientes:

- **Capacitación:** Consiste en capacitar a los empleados de la empresa para que puedan usar los activos de manera adecuada y así evitar daños causados a los activos por medio de los empleados u otros tipos de errores humanos.

- **Seguro:** Consiste en pagar para el servicio de un seguro que cubra los costos de los daños de los activos dentro de la empresa.

Los directivos de la empresa Laboratorios Fleming aceptaron la recomendación y decidieron que van a monitorear, planear medidas y posibles soluciones para los riesgos marginales y apreciables.

En el caso de los riesgos importantes y graves decidieron actuar de manera inmediata y van a proseguir con los tratamientos recomendados, priorizando los riesgos graves y luego los importantes.

Amenazas	**Nivel de Riesgo**	
	Importante	**Grave**
Daños físicos al activo	1	
Problemas de red	1	
Caídas de activo por sobrecarga	3	
Fallas al imprimir		1
Fallas de escaneo	1	
Error humano	1	
Total	**7**	**1**

3.1.1 Tratamiento del riesgo

Se han encontrado ciertas amenazas en los departamentos de IT, departamento administrativos, departamento del laboratorio y el departamento de muestras y se ha tratado de buscar una solución en general para cada tipo de amenaza para así salvaguardar cada activo de la empresa viendo así la fortalezas y debilidades de cada uno.

Amenaza	Riesgo	Fortaleza	Debilidades	Acción
Daños físicos al activo	Elementos tecnológicos inservibles	Contar con seguridad para los activos	No contar con seguridad	Seguridad de hardware
Daños de software al activo	Daño a activos y tiempo en reparación	Contar con personal de mantenimiento y backups	Capacitaciones al personal y no existe backup	Capacitaciones de software
Virus, gusanos y ransomware	Daños al sistema de la empresa	Contar con antivirus en todas las máquinas	No contar con antivirus en las máquinas.	Antivirus
Problemas de red	Incapacidad de realizar actividades laborales	Contar con personal de mantenimiento.	No contar con el personal adecuado.	Capacitación Empleados sobre el uso correcto de internet
Desperfectos al equipo	Mal funcionamiento de la empresa	Contar con personal de mantenimiento.	No contar con el personal adecuado.	Mantenimiento continuo
Fallas de escaneo	Pérdida de tiempo al escanear	Personal especializado en mantenimiento	No contar con el personal adecuado	Mantenimiento continuo
Fallo de configuración	Sistema inservible en algunos activos	Personal especializado en mantenimiento	No contar con el personal adecuado.	Configuracione s General
Fallas al imprimir	Utilización de más papel y tinta	Personal especializado en mantenimiento	No contar con el personal adecuado.	Mantenimiento continuo
Secuestro de	Robo de	Capacitación al	No contar con	Capacitaciones

registros	información	personal en caso de robo de información.	capacitaciones	de seguridad a personal
Phishing	Robo de información	Capacitaciones al personal en cuanto seguridad de información.	No contar con capacitaciones	Capacitaciones de seguridad a personal
Caída del activo por sobrecargas	Daño a activos o incendios	Capacitaciones al personal en cuanto a los activos.	No contar con capacitaciones	Capacitación del correcto uso de los equipos al personal
Problemas por contraseñas débiles	Robo de información	Capacitación al personal en seguridad en cuanto a contraseñas.	No contar con capacitaciones	Capacitaciones de seguridad a personal
Problemas por olvido o robo de cuentas	Robo de información	Capacitación al personal en caso de robo de información.	No contar con capacitaciones	Capacitaciones de seguridad a personal
Inundaciones	Daños a activos	Mantener los activos en zonas elevadas.	No mantener los activos en zonas elevadas	Ubicación de hardware estratégico
Terremotos	Daño a infraestructura y activos	Mantener los activos en zonas protegidas.	No contar con zonas protegidas.	Salidas de emergencia y equipo en lugares protegidos
Fuegos	Daño a activos, infraestructura y personal	Contar con extintores bien posicionados.	No contar con el equipo adecuado para una emergencia	Extintores y equipo antiincendios

3.2 Costos estimados

A continuación, se presentará un estimado sobre los costos que tendría que realizar esta empresa para que las amenazas, riesgos y defectos sean solucionados y además se presentará el coste del proyecto de este informe para que la empresa considere que nuestro equipo realice todo lo que listamos.

Problemas a solucionar	Solución al problema	Valor mensual	Valor anual	Valor instantáneo
Daños físicos al activo	Comprar equipos más robustos.			L. 100,000
Daños de software al activo	Capacitación a los usuarios sobre la utilización adecuada de los activos			L. 5,000
Virus, gusanos y ransomware	Contratar un antivirus seguro	L. 208.3	L. 2,500	
Fallas de escaneo	Comprar mejores herramientas para escaneos			L. 50,000
Fallo de configuración	Capacitación para las personas que instalan los activos en la empresa			L. 30,000
Fallas al imprimir	Comprar mejores herramientas para imprimir			L. 20,000
Secuestro de registros	Capacitación a empleados y escaneo mensual de estas amenazas		L. 5,000	L. 5,000
Problemas por contraseñas débiles y robo de cuentas	Capacitación a los empleados			L. 10,000
Terremotos	Mejorar la infraestructura del edificio y la ubicación de los activos			L. 150,000
Fuegos	Más extintores al igual que instalacion de alarma de humos			L. 30,000
Servidor en riesgo de	Instalacion de piso falso en el área del			L. 30,000

inundación	servidor			
Servidor en riesgo de incendio	Instalación de sistema de dispersión del agente químico contra incendios			L. 20,000
Informe	Precio de este informe y recomendaciones por parte del equipo			L. 80,000
	Total:	L. 208.3	L. 7,500	L. 530,000

3.3 Conclusiones y recomendaciones

3.3.1 Conclusiones

- Se cumplieron todos los objetivos específicos y el principal de acuerdo al análisis de los Laboratorios Fleming. La empresa por medio de este informe ahora es consciente de todos las amenazas que podría tener, las fallas que afectan su rendimiento y posibles soluciones a estas amenazas.

- Se hizo una descripción de todos los activos importantes para el funcionamiento completo de la empresa, y se identificó de manera exitosa todas las fallas que estos activos podrían tener, logrando mejorar la visión sobre estos activos y listar qué tan valiosos son para el desarrollo de la empresa.

- Es importante como empresa conocer qué elementos se podrían mejorar dentro de ellas para no sólo mejorar uno como empresa, sino también para crear un buen ambiente entre los empleados por medio de disminuir preocupaciones dentro de esta y también para mejorar el servicio al cliente y por medio de esta mejora lograr conseguir muchos más clientes.

- La identificación de todos los elementos para la creación de este informe fue muy fácil de conseguir con una gran rapidez ya que la empresa fue muy servicial y proveer esta información necesaria.

3.3.2 Recomendaciones

- Recomendamos a la empresa que tome acciones sobre la mayoría de cosas o si se podría, con todos los elementos peligrosos, advertencias, posibles fallas y lugares en donde mejorar para que la empresa pueda proveer un mejor servicio y un mayor aporte a la comunidad y a sus empleados.\

- Lo más esencial que identificamos como una gran falla para la empresa es que no contenga un buen sistema de protección contra incendios dentro de su centro de datos. Es una falla grave que si esta amenaza se logra materializar haría una gran cantidad de daños ya que este es un activo crítico para la empresa. Recomendamos a la empresa que instale algún tipo de sistema de protección contra incendios dentro del centro de datos para no ocasionar pérdidas de datos de la empresa y datos de los usuarios.

- Recomendamos a la empresa que evalúe y tome nota y posibles acciones sobre las fallas graves que logramos localizar en sus activos y amenazas a estos activos como por ejemplo en los riesgos potenciales. Ya que las fallas graves que existen en estos activos son activos que son esenciales para poder operar de manera funcional dentro de la empresa.

- Los mayores riesgos que pueden existir en una empresa es que los usuarios no sepan utilizar de manera adecuada los activos importantes para el funcionamiento de la empresa, pueden ocasionarles fallas de software o dañarlos de manera física, por lo tanto, al observar que la mayoría de estas amenazas provienen de los empleados recomendamos que la empresa capacité en las áreas que más pueda a sus empleados, para ocasionar menos fallas, menos errores y así generar menos costos y mas ingresos.

3.4 Bibliografía

- Anónimo. (s.f.). Laboratorios Fleming. marzo 25, 2022, de Laboratorios Fleming Sitio web: http://www.laboratoriosfleming.com/inicio.html

- Gómez Vieites, A. (). Enciclopedia de la seguridad informática. Alfaomega

- Guamanga, C. y Perilla, C. (2015). Análisis de riesgos de seguridad de la información basado en la metodología magerit para el área de datacenter de una entidad promotora de salud