UNIVERSIDAD POLITÉCNICA SALESIANA
SEDE QUITO

CARRERA:

COMPUTACIÓN

Trabajo de titulación previo a la obtención del título de:

Ingenieros en Ciencias de la Computación

TEMA:

PROPUESTA DE UN PLAN DE CONTINGENCIA Y DE RECUPERACIÓN DE DESASTRES FRENTE A LOS RIESGOS INFORMÁTICOS DEL DEPARTAMENTO DE TIC DE LA FUERZA AÉREA ECUATORIANA EN LA BASE MARISCAL SUCRE

AUTORES:

FRANCIS DHALINT BORJA PÉREZ

ANDRÉS RICARDO CEVALLOS OROSCO

TUTOR:

JOSÉ LUIS AGUAYO MORALES

Quito, octubre del 2021

CESIÓN DE DERECHOS DE AUTOR

Nosotros, Francis Dhalint Borja Pérez, con documento de identificación N° 1721516175 y Andrés Ricardo Cevallos Orosco, con documento de identificación N° 1719120097, manifestamos nuestra voluntad y sedemos a la Universidad Politécnica Salesiana la titularidad sobre los derechos patrimoniales en virtud de que somos autores del trabajo de titulación intitulado: PROPUESTA DE UN PLAN DE CONTINGENCIA Y DE RECUPERACIÓN DE DESASTRES FRENTE A LOS RIESGOS INFORMÁTICOS DEL DEPARTAMENTO DE TIC DE LA FUERZA AÉREA ECUATORIANA EN LA BASE MARISCAL SUCRE, mismo que ha sido desarrollado para optar por el título de: INGENIEROS EN CIENCIAS DE LA COMPUTACIÓN, en la Universidad Politécnica Salesiana, quedando la Universidad facultada para ejercer plenamente los derechos cedidos anteriormente.

En aplicación a lo determinado en la Ley de Propiedad Intelectual, en nuestra condición de autores nos reservamos los derechos morales de la obra antes citada. En concordancia, suscribo este documento en el momento que hacemos entrega del trabajo final en formato digital a la Biblioteca de la Universidad Politécnica Salesiana.

…….

Francis Dhalint Borja Pérez

1721516175

……

Andrés Ricardo Cevallos Orosco

1719120097

Quito, octubre del 2021

DECLARATORIA DE COAUTORIA DEL DOCENTE TUTOR

Yo declaro que bajo mi dirección y asesoría fue desarrollado el Proyecto Técnico, con el tema: PROPUESTA DE UN PLAN DE CONTINGENCIA Y DE RECUPERACIÓN DE DESASTRES FRENTE A LOS RIESGOS INFORMÁTICOS DEL DEPARTAMENTO DE TIC DE LA FUERZA AÉREA ECUATORIANA EN LA BASE MARISCAL SUCRE, realizado por Francis Dhalint Borja Pérez y Andrés Ricardo Cevallos Orosco, obteniendo un producto que cumple con todos los requisitos estipulados por la Universidad Politécnica Salesiana para ser considerado como trabajo final de titulación.

Quito, octubre del 2021

José Luis Aguayo Morales

C.I: 1709562597

ÍNDICE GENERAL

Índice Tablas

Índice Figuras

RESUMEN

La Fuerza Aérea Ecuatoriana en la Base Mariscal Sucre (FAEBMS), preocupada por la seguridad de su información, pretende mejorarla a través del departamento de TIC. Por lo tanto, este trabajo se enfocará en el departamento de TIC de la FAEBMS, donde fue necesario realizar evaluaciones de riesgo de TI y desastres naturales, para emitir recomendaciones basadas en la metodología MAGERIT. El departamento de TIC es un lugar donde se encuentran las tecnologías de la información y comunicación, por ende, es el entorno con mayor vulnerabilidad a ataques informáticos y desastres naturales, ya que existen dispositivos e información valiosa que proteger.

Los activos y los riesgos que se pudieron identificar en el departamento de TIC fueron mediante la metodología MAGERIT, gracias a ello se logró realizar el análisis de gestión de riesgos de los sistemas de información, por lo consiguiente se procedió a la elaboración de un plan de contingencia y recuperación ante desastres tomando en cuenta cada fase para establecer controles determinando la acción de transferir, eliminar, asumir o mitigar, reduciendo en un 65% las amenazas, vulnerabilidades y riesgos informáticos en el departamento de TIC de la FAEBMS.

Posteriormente se realizó un análisis de costo/beneficio el cual se obtuvo como resultado que el coste de la solución es menor al coste de la exposición del riesgo, logrando tener un porcentaje del cálculo de ROSI del 3680% en los activos de información, teniendo como efecto que la implementación de las soluciones propuestas son factibles en los 9 de los 11 activos con un nivel de alto riesgo.

ABSTRACT

The Ecuadorian Air Force at the Mariscal Sucre Base (FAEBMS), concerned about the security of your information, intends to improve it through the TIC department. Therefore, this work will focus on the TIC department of the FAEBMS, where an IT risk and natural disasters assessments was necessary to be conducted, to issue recommendations based on the MAGERIT methodology. The TIC department is a place where information and communication technologies are located, therefore, it is an environment with the greatest vulnerability to computer attacks and natural disasters, as there are valuable devices and information to protect.

The assets and risks that were identified in the TIC department were done through the MAGERIT methodology, thanks to this it was possible to carry out the risk management analysis of the information systems and, elaborate a plan of contingency and disaster recovery considering each phase establishing controls to determine the action to transfer, eliminate, assume, or mitigate, reducing by 65% the threats, vulnerabilities, and computer risks in the TIC department of the FAEBMS.

Subsequently, a cost / benefit analysis was done, and the results shown that the cost of the solution is less than the cost of the risk exposure, achieving a ROSI calculation percentage of 3680% in the information assets, taking into consideration that the implementation of the proposed solutions are feasible in 9 of the 11 assets with a high-risk level.

CAPÍTULO I

INTRODUCCIÓN

Antecedentes

La importancia en la protección de la información es un punto crucial, la Fuerza Aérea Ecuatoriana (FAE) al ser una institución del gobierno debe tener un nivel de seguridad alto. Según Alvarado-Zabala, Pacheco-Guzmán, & Martillo-Alchundia (2018):

> Las empresas públicas y privadas en la actualidad requieren de un mayor control en cuanto a los sistemas que realizan procesos con información, por lo cual el análisis y gestión de riesgos es considerado de suma importancia para dichas empresas.

Por ende, se procedió a la elaboración de una propuesta de un plan de contingencia y recuperación de desastres, recomendando procedimientos adecuados contra amenazas y vulnerabilidades en los activos de información.

Problema

Para el desarrollo de este trabajo previamente se han identificado las variables “plan de contingencia” y “recuperación de desastres” frente a los riesgos informáticos.

Un plan de contingencias contiene planificaciones, procesos y controles que permiten la recuperación de información (Swanson M, 2021). El plan de contingencia es una disciplina que se ocupa de estándares, procesos, métodos y tecnologías, y tiene como objetivo proporcionar condiciones seguras y confiables para el procesamiento de información/datos en sistemas informáticos.

Un desastre se puede definir como un evento inesperado que hace que los servicios de TI no estén disponibles durante un periodo de tiempo. Para mitigar los ataques cibernéticos, es importante detectar las amenazas con anticipación antes de que causen daños graves (Jiménez, 2018). Recientemente se está dando prioridad a la detección y solución de riesgos informáticos,

como ciberespionaje, cibersabotaje y el robo de información confidencial que afectan a las empresas a nivel mundial.

El presente proyecto de investigación responderá a la siguiente problemática: ¿Existe un plan de contingencia y de recuperación de desastres frente a los riesgos informáticos del Departamento de TIC de la Fuerza Aérea Ecuatoriana en la Base Mariscal Sucre (FAEBMS)?

Por lo expuesto, se analiza que la FAEBMS al ser una institución que maneja información sensible y confidencial, se debe tomar precauciones adecuadas para la protección ante amenazas, ya que dependen de agencias externas que les proporcionar presupuestos anuales limitados para la seguridad.

Justificación

El desarrollo de los sistemas de información y comunicación en el mundo y en el Ecuador ha desencadenado la necesidad de un sistema de gestión en la mayoría de las instituciones (ya sean privadas o públicas); con el fin de obtener seguridad, confiabilidad y escalabilidad en las mismas. Las organizaciones requieren cada vez más control sobre sus datos y los sistemas que utilizan para el procesamiento de la información, ya que son vulnerables a diversas amenazas desde dentro y fuera de la organización como son: la denegación de servicios, ataques informáticos, entre otros peligros potenciales.

Desafortunadamente, la mayoría de las amenazas ocurren en un segundo plano sin dejar rastro alguno, aún más si se hace referencia a los sistemas de información, por lo que estos manejan activos tan intangibles como los datos y la información que se obtiene a través de dichos sistemas.

Por ende, es fundamental analizar los riesgos informáticos que se pueden generar en las instituciones para tomar medidas de mitigación y seguridad.

La evaluación de riesgos informáticos permite a las organizaciones considerar en qué medida los eventos afectan a la institución, desde la perspectiva de la probabilidad y el impacto, de modo que se pueda prevenir la pérdida de información, adulteración de documentos confidenciales, suplantación de identidad, entre otros.

Este trabajo se enfocará en el departamento de TIC de la FAEBMS. Por lo tanto, es necesario realizar evaluaciones de riesgos informáticos para emitir recomendaciones basadas en una metodología.

Objetivos

Objetivo general: Proponer un plan de contingencia y recuperación de desastres frente a los riesgos informáticos del Departamento de TIC de la Fuerza Aérea Ecuatoriana en la Base Mariscal Sucre.

Objetivos específicos: Determinar los activos de información y sus riesgos informáticos en el Departamento de TIC de la Fuerza Aérea Ecuatoriana en la Base Mariscal Sucre para mitigarlos.

Proponer un plan de contingencia que mitigue los riesgos informáticos del departamento de TIC de la Fuerza Aérea Ecuatoriana en la Base Mariscal Sucre.

Plantear un plan de recuperación de desastres frente a los riesgos informáticos del Departamento de TIC de la Fuerza Aérea Ecuatoriana en la Base Mariscal Sucre.

Metodología

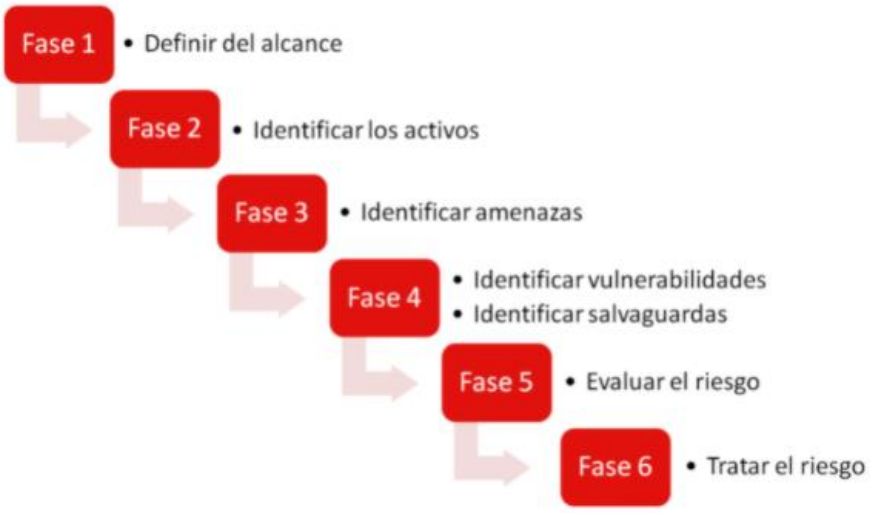
Para la realización de este proyecto, se basó en la metodología de investigación cualitativa, en sentido amplio, puede definirse como la investigación que produce datos descriptivos, es decir, las palabras de personas que pueden ser habladas o también escritas, y la conducta visible (L & Castaño, 2002). Para realizar la recopilación de datos y así seleccionar

procedimientos óptimos mediante una metodología específica, se escoge el tipo de investigación encuesta y cuestionario, que es ampliamente como un proceso de investigación, permitiendo conseguir y elaborar información rápida y eficaz. De esta manera se pueden analizar los riesgos que tengan mayor impacto en la institución y mejorar los procedimientos para la solución (Casas, 2003).

Implementar una metodología permite el análisis de gestión de riesgos de los Sistemas de Información, además, de seguir las fases para la realización del plan de contingencia, las cuales son:

Figura 1

Fases de la metodología MAGERIT



Nota. Fases que se llevaran a cabo en la metodología MAGERIT. Adaptado de Análisis de riesgos, por INCIBE Instituto Nacional de Ciberseguridad, 2017, (https://normas-apa.org/wp-content/uploads/Guia-Normas-APA-7ma-edicion.pdf).

CAPÍTULO II

FUNDAMENTACIÓN TEÓRICA

Riesgos de tecnologías de la información

El departamento de TIC de la FAEBMS es un lugar donde se encuentran las tecnologías de la información y comunicación, por ende, es el entorno con mayor vulnerabilidad de ataques informáticos y desastres naturales, de modo que existen dispositivos e información valiosa que proteger, mediante un plan de contingencia y recuperación de desastres. Según Solarte Solarte, Enriquez Rosero y Benavides Ruano (2015):

> Los riesgos informáticos son problemas latentes para las empresas del sector público y privado, que pueden perturbar a los sistemas de información o a los distintos equipos informáticos. (p. 498)

Riesgos de integridad

Uno de los riesgos más significativos dentro de una organización, ya que afectan directamente a la información, interfaces de software y procesamiento de esta, por ende, se asocia con la autorización, completitud, exactitud de la entrada y reportes que generan las diferentes aplicaciones utilizadas internamente.

Riesgos de relación

Este riesgo se enlaza directamente con los diferentes software que utiliza la organización para generar información relevante, la cual les sirven de guía para tomar una decisión a corto o largo plazo para el bienestar de esta.

Riesgos de acceso

Se centran en la inadecuada gestión de usuarios dentro de una organización, ya sea para acceder a una aplicación o sitio web mediante un usuario y una contraseña, poniendo en riesgo la información de bases de datos y demás de una organización.

Riesgos de utilidad

Afectan a las herramientas de desarrollo de software de una organización, poniendo en peligro las diferentes bibliotecas y base de datos de estas, perturbando las consultas que se puede hacer en las bases de datos y al soporte para la construcción y ejecución de una aplicación.

Riesgo de infraestructura

Se asocian directamente con los procesos que tiene el departamento de TIC, que definen, desarrollan, mantienen y operan toda una red interna de una organización.

Riesgos de seguridad general

Estos riegos se dividen en causa de riesgo interna que son las causadas por la misma organización entre estas destacan el robo de información o materiales, personal no capacitado, sabotaje, entre otras, y por otro lado son las causas de riesgo externa que generalmente se asocian con los fenómenos naturales como los incendios, cortes del suministro eléctrico, etc. Ocasionando pérdidas significantes dentro de una organización.

Valoración de los riesgos de tecnologías de la información

Para poder evaluar un riesgo de TI se ha dividido en tres fases que son: la identificación, el análisis y la determinación del nivel del riesgo, permitiendo ponderar de una manera eficaz y sencilla cada uno de estos.

Identificación del riesgo

Cuando se quiere identificar un riesgo es necesario ser permanente para determinar sus posibles consecuencias, y para mayor eficiencia y facilidad al momento de detallarlo se tiene que responder a cada una de estas preguntas: qué, cómo y por qué se genera dicho riesgo.

Para la identificación de los riesgos es fundamental elaborar un mapa de riesgos para agilizar y determinar con mayor exactitud las posibles causas y consecuencias de estos.

Figura 2

Mapa de riesgos

RIESGO	DESCRIPCIÓN	POSIBLES CONSECUENCIAS
Posibilidad de ocurrencia de aquella situación que pueda entorpecer el normal desarrollo de las funciones de la entidad y le impidan el logro de sus objetivos.	Se refiere a las características generales o las formas en que se observa o manifiesta el riesgo identificado	Corresponde a los posibles efectos ocasionados por el riesgo, los cuales se pueden traducir en daños de tipo económico, social, administrativo, entre otros

Nota. Definiciones correspondientes a lo que son los riegos y sus consecuencias. Fuente: (Castillo Reina, Cardenas Prado, Quezada Ancajima, Roncal Mejia, & Villanueva León, 2013).

Análisis del riesgo

Con toda la información proporcionada de la identificación de los riesgos mediante el mapa de riesgos es necesario dar una ponderación para su posterior análisis y así poder tomar acciones a corto o largo plazo.

Se han establecido dos aspectos primordiales para un eficiente análisis de riesgos, que son la probabilidad de ocurrencia del riesgo, la cual se pondera mediante los criterios de frecuencia o determinando la manifestación de factores internos/externos y las consecuencias que puede ocasionar a la organización la materialización del riesgo (impacto).

Figura 3

Valoración de la probabilidad de ocurrencia del riesgo

Probabilidad	Valor
Nunca	0
Año	1
Mes	2
Semana	3

Nota. Valoraciones que se otorgan a las probabilidades de ocurrencia de un riesgo. Fuente: (Amutio, Candau, & Mañas, 2012).

Figura 4

Valoración del impacto de los riesgos

Impacto	Valor
No hay consecuencias	0
No hay consecuencias relevantes	1
Consecuencias relevantes	2
Hay consecuencias graves	3

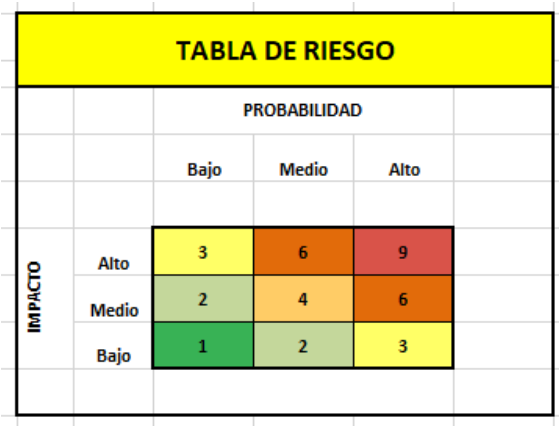
Nota. Valoraciones que se otorgan a las consecuencias que dejaría un riesgo en la institución (impacto). Fuente: (Amutio, Candau, & Mañas, 2012).

Determinación del nivel del riesgo

"La determinación del nivel del riesgo es el resultado de comparar el impacto y la probabilidad con los controles existentes al interior de una empresa y con los diferentes procesos que se realizan en las mismas" (Viteri Silva, 2015, pág. 12). Es fundamental tener bien determinados los puntos de control existentes en los diferentes procesos, ya que estos proporcionan información importante para tomar una decisión decisiva para el bien de la organización.

Figura 5

Tabla de riesgo



Nota. La probabilidad por el impacto da como resultado un nivel de impacto los cuales son: bajo, medio y alto correspondientemente. Fuente: (Amutio, Candau, & Mañas, 2012).

Alto: Cuando el riesgo hace altamente vulnerable a la empresa.

Medio: Cuando el riesgo es vulnerablemente mediano para la empresa.

Bajo: Cuando el riesgo es vulnerablemente bajo para la empresa.

METODOLOGÍA MAGERIT

El uso de la metodología está relacionado con las tecnologías de la información, dando pautas y técnicas para minimizar los riesgos informáticos. CSAE elabora MAGERIT para lograr metas que se proponen las instituciones referentes a los sistemas de información (Amutio, Candau, & Mañas, 2012).

MAGERIT permite saber la importancia de la información evaluando, dando a conocer el riesgo y protegerlo.

Proceso de la metodología MAGERIT

En el proceso de la metodología se dividió en 6 fases, aportando recomendaciones prácticas de cómo se debe realizar cada una de ellas.

Definir del alcance: Debe cubrir las áreas seleccionadas con las tecnologías de información que contienen.

Identificar los activos: Se refiere a los activos que posee la institución.

Identificar amenazas: Son amenazas que están expuesto los activos identificados.

Identificar vulnerabilidades / Identificar salvaguardas: El primer paso es identificar las vulnerabilidades es decir los puntos débiles. El segundo paso son las acciones que se tomarán para reducir el riesgo.

Evaluar el riesgo: Con diferentes procesos se estimará el riesgo del activo.

Tratar el riesgo: Estimado el riesgo, se tratará el riesgo con cuatro estrategias.

Definir alcance

Para la definición del alcance es importante iniciar por las áreas o departamento con mayor relevancia y continuar ampliando hacia toda la institución (Análisis de riesgos, 2017). La FAEBMS es una institución con una organizativa compleja y confidencial, la definición del

alcance es concretamente en un departamento con las áreas asignadas con sus respectivos activos de información.

Identificar los activos

Al identificar los activos se los debe relacionar con el departamento o sistema de objeto del estudio, para el manejo de la cantidad de información se utilizarán matrices, las cuales permitirán organizar los activos relevantes como se muestra a continuación a modo de ejemplo:

Tabla 1

Evaluación del tipo de activo Datos e Información

ACTIVO	CONFIDENCIALIDAD	INTEGRIDAD	DISPONIBILIDAD	CRITICIDAD
Documentos Secretos	3	3	3	3
Documentos Confidenciales	3	3	3	3
Documentos de Uso Interno	2	2	1	1.7
Documentos ordinarios	2	1	1	1.3
Base de datos	3	3	2	2.7

Nota. Está tabla muestra la evaluación de un tipo de activo que se realizó en el departamento de TIC de la FAEBMS. Fuente: (Amutio, Candau, & Mañas, 2012).

Identificar las amenazas

El conjunto de amenazas es variado y amplio, por lo que se necesita un esfuerzo para mantener un enfoque realista y aplicable (Análisis de riesgos, 2017). Para realizar un buen análisis de las amenazas se realizó la consulta al supervisor directo del área, el aporte otorgado por una persona que este directamente en el uso y configuración de los activos, es de suma importancia.

El siguiente listado recoge las principales amenazas a considerar en el ámbito de un análisis de riesgos de sistemas de información; se trata de un resumen de las más importantes del catálogo de amenazas de MAGERIT:

Figura 6

Catálogo de amenazas

De origen natural	Se refiere específicamente, a todos los fenómenos atmosféricos, hidrológicos, geológicos (especialmente sísmicos y volcánicos) y a los incendios que, por su ubicación, severidad y frecuencia, tienen el potencial de afectar adversamente al ser humano, a sus estructuras y a sus actividades
De origen industrial	Son amenazas que se originan a raíz de las condiciones tecnológicas o industriales, lo que incluye accidentes, procedimientos peligrosos, fallas en la infraestructura o actividades humanas específicas que pueden ocasionar la muerte, lesiones, enfermedades u otros impactos sobre la salud, al igual que daños a la propiedad, pérdida de medios de sustento y de servicios, trastornos sociales o económicos, o daños ambientales
Ataques intencionados	Son amenazas que deliberadamente intentar realizar un daño o conseguir un beneficio mediante técnicas como, por ejemplo: trashing, phishing, ingeniera social, etc
Errores y fallos no intencionados	No intencionales, en donde se producen acciones u omisiones de acciones que, si bien no buscan explotar una vulnerabilidad, ponen en riesgo los activos de información y pueden producir un daño

Nota. Principales amenazas del análisis de riesgos en los sistemas de información. Fuente: (Amutio, Candau, & Mañas, 2012).

Identificar vulnerabilidades – identificar salvaguardas

En esta fase se analizarán las vulnerabilidades o debilidades en la seguridad de los activos identificados (Análisis de riesgos, 2017). Conocer las vulnerabilidades que puede suponer en los activos, ayudan a identificar procesos que no se están realizando de forma correcta o simplemente no se tiene seguridad. En el siguiente paso se analizaron las medidas de seguridad que tiene implementadas en la institución.

Evaluar el riesgo

Luego de establecer e identificar amenazas, se debe evaluar el efecto que tiene en la institución con los siguientes elementos:

Probabilidad: Se determina la frecuencia con que puede suceder o sucedió una amenaza en el activo de información.

Figura 7

Probabilidad de Ocurrencia

PROBABILIDAD	
VALOR	DESCRIPCIÓN
0	La amenaza no se materializa nunca.
1	La amenaza se materializa una vez cada año.
2	La amenaza se materializa una vez cada mes.
3	La amenaza se materializa una vez cada semana.

Nota. Probabilidad de ocurrencias de los activos de información. Fuente: (Amutio, Candau, & Mañas, 2012).

Impacto: Es el efecto que puede generar la materialización de una amenaza sobre un activo de información.

Figura 8

Evaluación de Impacto

IMPACTO	
VALOR	DESCRIPCIÓN
0	No existen consecuencias si se materializa la amenaza
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 relevantes para la organización.
3	El daño derivado de la materialización de la amenaza tiene consecuencias graves para la organización.

Nota. Evaluación de impacto de los activos de información. Fuente: (Amutio, Candau, & Mañas, 2012).

Tratar el riesgo

Establecido el límite, se debe tratar el riesgo de los activos que superaron el umbral establecido (Análisis de riesgos, 2017). El umbral que se estableció fue que el riesgo sea superior a “1”.

Figura 9

Estrategias principales

Transferir	El riesgo a un tercero, es decir, contratando un servicio adicional que cubra los daños ocasionados a los activos
Eliminar	Eliminando un proceso o sistema que está sujeto a un riesgo elevado o que tenga varias vulnerabilidades de seguridad
Asumir	Permitir el riesgo, algunos riesgos no ocasionan consecuencias en la institución
Mitigar	Es una estrategia que busca prever el riesgo en un proyecto antes de que se ejecute

Nota. Estrategias principales para tratar el riesgo. Adaptado de Análisis de riesgos, por INCIBE Instituto Nacional de Ciberseguridad, 2017, (https://normas-apa.org/wp-content/uploads/Guia-Normas-APA-7ma-edicion.pdf).

CAPÍTULO III

METODOLOGÍA DE INVESTIGACIÓN

Fase 1: Definición del alcance

En este trabajo se realizará un plan de contingencia para determinar los activos de información y sus riesgos informáticos, mediante una metodología y mecanismos de mitigación. El alcance se dividirá en dos principales etapas que son:

La primera etapa está conformada por la información proporcionada y recopilada de la FAEBMS, al ser datos sensibles y de alta confidencialidad es necesario mitigar posibles amenazas y riesgos que podrían afectar a dicha información, los datos recopilados se analizarán mediante una metodología y se seleccionarán los mejores procedimientos para resolver problemas de una manera eficaz.

Por último, se planteará un plan de recuperación de desastres frente a los riesgos informáticos para salvaguardar y dar continuidad a las operaciones del Departamento de TIC de la FAEBMS.

Fase 2: Identificación de los activos

Figura 10

Definición de los activos de la información

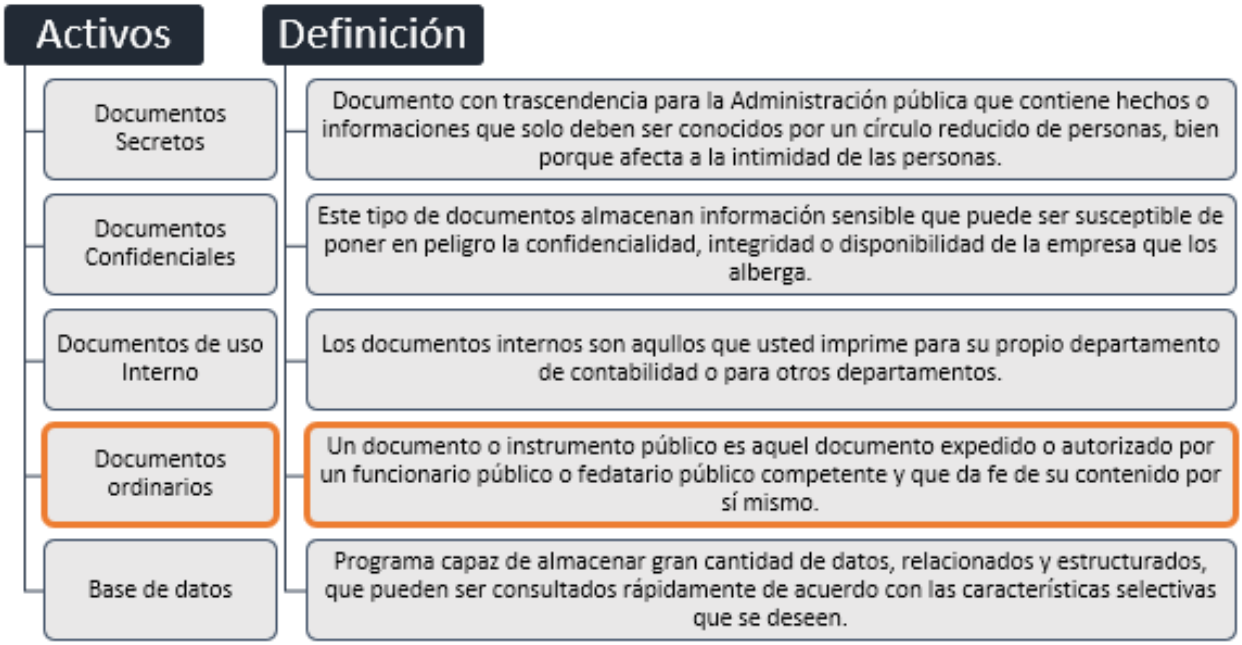
a. Servicios internos

Activos	Definición
Telefonía IP	La telefonía IP es la telefonía que establece las comunicaciones mediante Internet. y donde la transición de voz se realiza mediante Voz por IP.
Correo Institucional	El correo corporativo o institucional es, en otros términos, el que identifica de manera oficial a la empresa.
Servicios de mantenimiento motorolas	Previenen, predicen y reparan las posibles averías que pueden darse en las radios motorolas.
Servicio de mantenmiento camaras ip	Previenen, predicen y reparan las posibles averías que pueden darse en las camaras IP.
Servicio de mantenimiento de firewall	Previenen, predicen y reparan las posibles averías que pueden darse en los firewall.
Servicio de mantenimiento UTM	Previenen, predicen y reparan las posibles averías que pueden darse en la UTM.
Servicio de mantenimiento pagina web	Previenen, predicen y reparan los posibles errores que se puede generar es una pagina web.
Active Directory	Active Directory o Directorio Activo son los términos que utiliza Microsoft para referirse a su implementación de servicio de directorio en una red distribuida de computadoras.

b. Servicios externos

Activos	Definición
Internet	Internet se podría definir como una red global de redes de ordenadores cuya finalidad es permitir el intercambio libre de información entre todos sus usuarios.
Videoconferencia	Comunicación telefónica o realizada con otro soporte tecnológico de una duración prolongada que permite a dos o más personas hablar y verse a través de una pantalla y, a veces, compartir otros archivos informáticos.
Sistema F.A.E	El sistema F.A.E constituye el conjunto de recursos de la institución. que sirven como soporte para el proceso básico de captación, transformación y comunicación de la información.
Chasqui	El sistema de gestión documental permite el registro, control, circulación y organización de los documentos digitales y/o físicos que se envían y reciben en el Comando Conjunto de las Fuerzas Armadas.

c. Datos e información



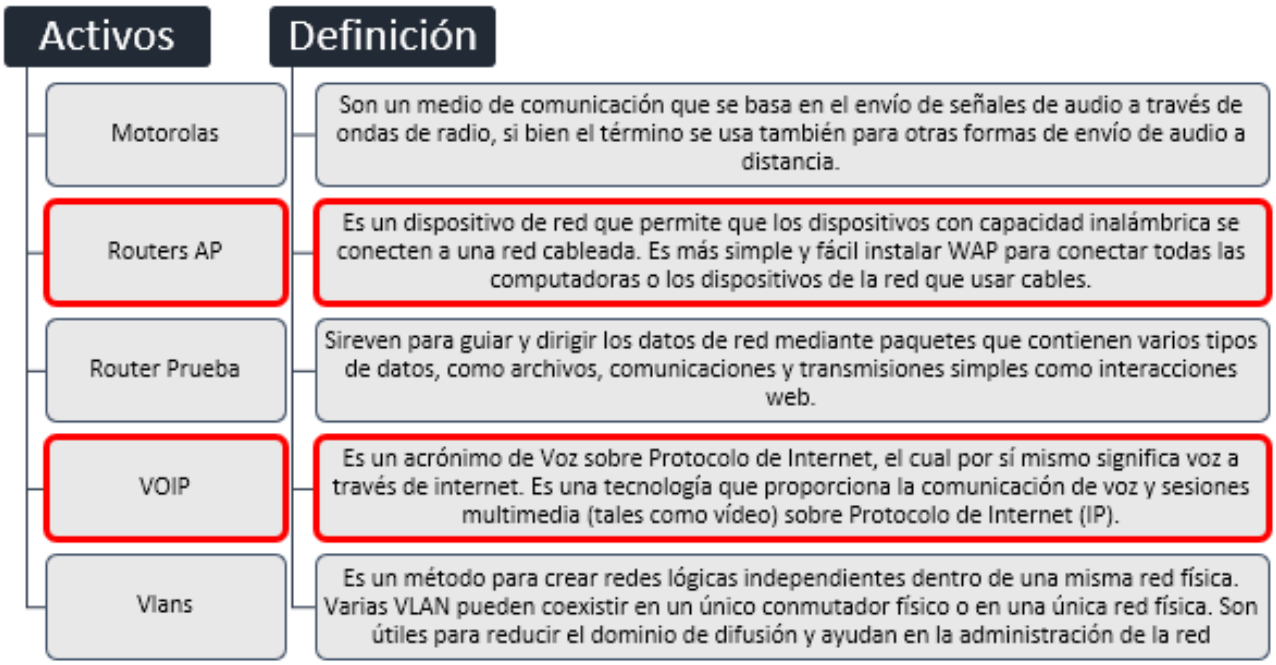
d. Aplicaciones (software)

Activos	Definición
Apache	Apache es un acrónimo de «a patchy server»es un servicio de paginas web HTTP de código abierto que sirve para colocar varias plataformas como Unix, BSD, GNU/Linux, Windows, Macintosh entre otros
Office	Office es un paquete de programas informáticos para oficina. Se trata de un conjunto de aplicaciones que realizan tareas ofimáticas, es decir, que permiten automatizar y perfeccionar las actividades habituales de una oficina.
Cobian	Es un programa multitarea capaz de crear copias de seguridad en un equipo, en una red local o incluso en/desde un servidor FTP. También soporta SSL.
Ocs Inventory	Es un software libre que permite a los Administradores de TI (Tecnología de Información) gestionar el inventario de sus activos de TI. OCS-NG recopila información sobre el hardware y software de equipos que hay en la red.
VNC	Son las siglas en inglés de Virtual Network Computing. VNC es un programa de software libre basado en una estructura cliente-servidor que permite observar las acciones del ordenador servidor remotamente a través de un ordenador cliente.
Putty	Es un emulador gratuito de terminal que soporta SSH y muchos otros protocolos. La mayoría de usuarios, especialmente los que trabajan sobre sistemas operativos Windows, lo encuentran muy útil a la hora de conectar a un servidor Unix o Linux a través de SSH.
MySQL	Es un sistema de gestión de bases de datos relacionales (RDBMS) de código abierto respaldado por Oracle y basado en el lenguaje de consulta estructurado (SQL).
Tera Term	Es un programa de emulador de terminal (comunicaciones) de código abierto, gratuito e implementado por software . Emula diferentes tipos de terminales de computadora.
Windows	Es un sistema operativo desarrollado por la compañía de software Microsoft Corporation, que cuenta con una interfaz gráfica de usuario basada en el prototipo de windows (su nombre en inglés).

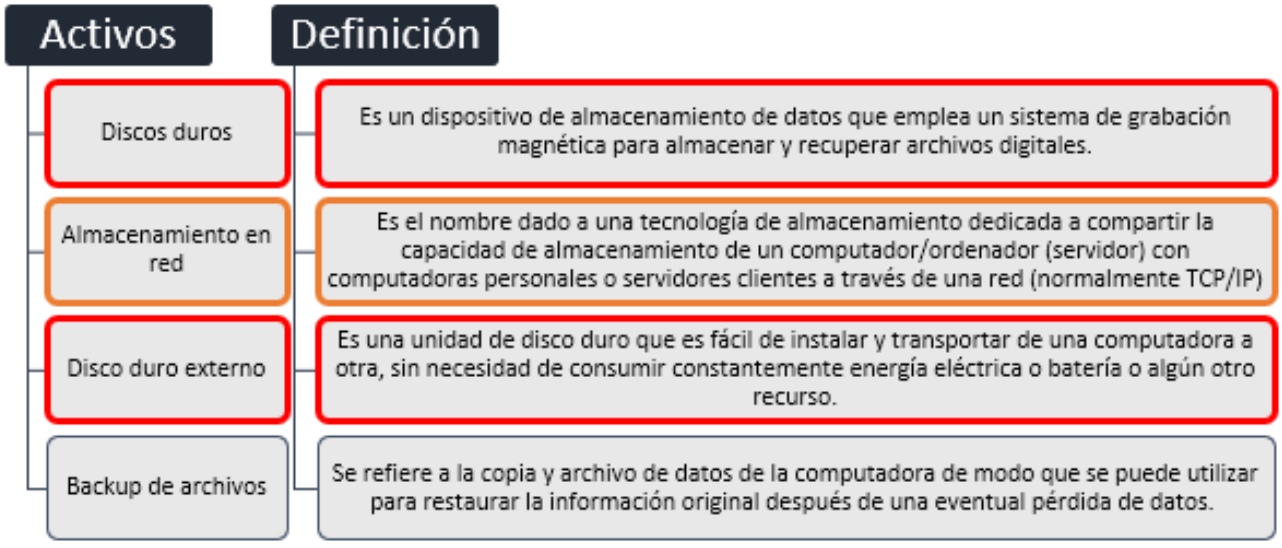
e. Equipos informáticos

Activos	Definición
Tester	Mide los parámetros estándar de tensión y corriente, además dispone de un análisis de red. Se puede comprobar por ejemplo las conexiones LAN y su funcionalidad.
Servidores de torre	Los servidores tipo torre, son unidades verticales e independientes que constan de todos los componentes tradicionales de un servidor. Ejecutan tareas que van más allá de la capacidad de una sola máquina corriente.
rack de switch	Estructura que permite sostener o albergar un dispositivo tecnológico como son los switch.
Servidor UTM	Son servdiores de seguridad de la información, por lo general, a un único producto de seguridad que ofrece varias funciones de protección en un solo punto en la red.
Servidor Firewall	Son servidores que permiten gestionar y filtrar la totalidad de trafico entrante y saliente que hay entre 2 redes u ordenadores de una misma red.
Servidor de Backup	Dan servicio de copias de seguridad remota, en línea o gestionado es un servicio que proporciona al ordenador de un usuario conexiones en línea con un sistema remoto para copiar y almacenar los ficheros de su ordenador.
Computadoras de Escritorio	Son un tipo de ordenador personal, diseñado y fabricado para ser instalado en una ubicación estática, como un escritorio o mesa.
Laptop	Es una computadora portátil de peso y tamaño ligero, su tamaño es aproximado al de un portafolio.

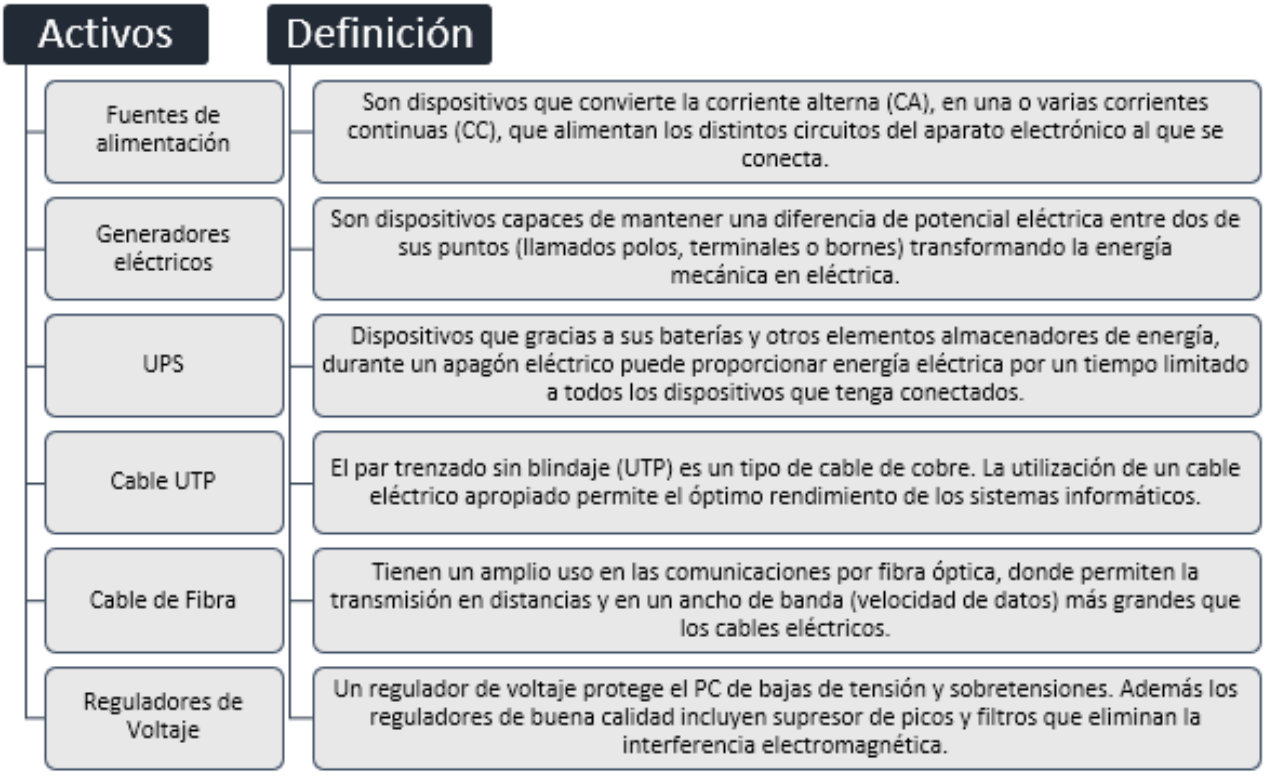
f. Equipos informáticos



g. Redes de comunicaciones



h. Soporte de información



Activos	Definición
Fuentes de alimentación	Son dispositivos que convierte la corriente alterna (CA), en una o varias corrientes continuas (CC), que alimentan los distintos circuitos del aparato electrónico al que se conecta.
Generadores eléctricos	Son dispositivos capaces de mantener una diferencia de potencial eléctrica entre dos de sus puntos (llamados polos, terminales o bornes) transformando la energía mecánica en eléctrica.
UPS	Dispositivos que gracias a sus baterías y otros elementos almacenadores de energía, durante un apagón eléctrico puede proporcionar energía eléctrica por un tiempo limitado a todos los dispositivos que tenga conectados.
Cable UTP	El par trenzado sin blindaje (UTP) es un tipo de cable de cobre. La utilización de un cable eléctrico apropiado permite el óptimo rendimiento de los sistemas informáticos.
Cable de Fibra	Tienen un amplio uso en las comunicaciones por fibra óptica, donde permiten la transmisión en distancias y en un ancho de banda (velocidad de datos) más grandes que los cables eléctricos.
Reguladores de Voltaje	Un regulador de voltaje protege el PC de bajas de tensión y sobretensiones. Además los reguladores de buena calidad incluyen supresor de picos y filtros que eliminan la interferencia electromagnética.

i. Equipamiento auxiliar

Activos	Definición
Central Telefónica	Es el lugar donde se alberga el equipo de conmutación y las demás instalaciones necesarias para la operación de las llamadas telefónicas.
Cuarto de Servidores	Es una lugar con aire acondicionado, dedicada al funcionamiento continuo de los servidores, los cuales son capaces de atender las peticiones requeridas por los usuarios, centro de datos.
Comunicaciones	Espacio utilizado exclusivamente para alojar los elementos de terminación del cableado estructurado y los equipos de telecomunicaciones
Área de Procesamiento de la informacion	Se encuentran los equipos informáticos necesarios para el procesamiento de la información donde se hace posible el almacenamiento y proceso de la información.
Área de Electronica	Esta área trata con circuitos eléctricos que involucran componentes eléctricos pasivos y tecnologías de interconexión.
Area de Informática	Área responsable de atender las necesidades de cómputo, tales como la asesoría en el manejo de software, configuración de equipo para impresión o conexión a Internet.
Area de Telefonía	En esta área hacen efectiva la comunicación, hacen uso de medios, ya sean físicos, como los medios de transmisión de los que se compone la red, o lógicos como el lenguaje utilizado o los programas que lo manejan.

j. Personal

Activos	Definición
Soporte Técnico	Son encargados de prestar un servicio de asistencia a los diferentes usuarios para garantizar el perfecto funcionamiento de los componentes físicos (equipos y otros dispositivos).
Redes	Son los responsables de mantener el buen funcionamiento del software y hardware de redes. Estas redes de datos son redes de área local (LAN), redes de área amplia (WAN), intranets y/o extranets.
Seguridad de la Información	Responsables de la gestión del plan de seguridad de información.
Centro Procesamiento de la Información	En esta area se encargan de recabar datos y traducir a información utilizable.
Radiocomunicaciones	En esta área se encargan de mantener en total funcionamiento el sistema de comunicación a distancia que se realiza por medios eléctricos o electromagnéticos.

Nota. Definición de los activos de información. Fuente: (Amutio, Candau, & Mañas, 2012).

Fase 3: Identificación de las amenazas

Figura 11

Definición de amenazas

a. Ataques intencionados

b. Amenazas de origen natural

Amenazas	Definición
Fuego	Material que se puede ver afectado por la combustión de una materia.
Daños por agua	Cualquier agua que cause la imposibilidad de uso (presente o futuro) de un dispositivo o área de trabajo.
Desastres naturales	Estructuras dañadas por la corriente de agua, inundación, derrumbes, entre otros.

c. Amenazas de origen industrial

Amenazas	Definición
Corte del suministro eléctrico	Fallo de alguno de los elementos que componen el sistema de suministro eléctrico y pueden llegar afectar el funcionamiento de algun dispositivo electrónico y/o área de trabajo.
Condiciones inadecuadas de temperatura	El calor y la humenadad pueden llegar a dañar o afectar un dispositivo electrónico y/o área de trabajo
Fallo de servicios de comunicaciones	Son aquellos que obstaculizan, distorsionan o desvirtúan los procesos de diálogo necesarios para la comunicación.
Desastres industriales	Desastres que resultan de las actividades tecnológicas en la sociedad son de carácter industrial u ocasionados por el hombre.

d. Errores y fallas no intencionados

Amenazas	Definición
Caída del sistema por sobrecarga	Es cuando el sistema declina por exceso de información, comandos, etc.
Errores de mantenimiento / actualización de equipos (hardware)	Errores o equivocaciones al dar manteniemiento a los equipos (hardware) y/o actualizanes de piezas fisicas de los mismos (ensamblaje).
Errores de mantenimiento / actualización de programas (software)	Errores o equivocaciones al dar manteniemiento a los equipos (software) y/o actualizanes de programas.
Difusión de software dañino	Dañar o causar un mal funcionamiento al sistema informático.
Degradación de los soportes de almacenamiento de la información	Corrupción gradual de datos informáticos a lo largo de los años debido a una acumulación de fallos no críticos en un dispositivo de almacenamiento de datos.
Errores de configuración	Es generado por una escritura incorrecta de las líneas del archivo de configuración o que el hardware este limitado a una configuración que no requiera de tantos recursos como esta.
Errores del administrador	Es generado por un mal control y supervisación del procesamiento de trabajo a través de computadoras centrales de gran capacidad y de una mala gestion de errores producidos en el sistema.
Errores de los usuarios	Es generado por errores de los usuarios al momento de usar mal un programa o un dispositivo informático.

Nota. Definición de las principales amenazas. Fuente: (Amutio, Candau, & Mañas, 2012).

Fase 4: Identificar vulnerabilidades

Con los activos identificados y sus respectivas amenazas, se tienen vulnerabilidades (puntos débiles), por lo que luego se realizaran recomendaciones para aumentar su seguridad.

Figura 12

Vulnerabilidades en los activos

Activo	Vulnerabilidades(Puntos debiles)
Internet	No hay un cifrado o esté es inseguro en las comunicaciones que realizan los dispositivos con la nube, el servidor o el usuario
Office	Programas de Office que no cuenta con licenciamiento, se puede dar el caso de que no reciban las últimas actualizaciones de seguridad. Esto podría dejar expuesto el equipo como tal y las más recientes vulnerabilidades descubiertas.
Apache	Código que se ejecuta en procesos o subprocesos secundarios con pocos privilegios podría permitir a un atacante ejecutar código arbitrario con los privilegios de root manipulando el marcador.
Windows	No hay un cifrado o esté es inseguro en las comunicaciones que realizan los dispositivos con la nube, el servidor o el usuario
Computadoras de Escritorio(10)	Una vulnerabilidad que no se controla es el uso de dispositivos de almacenamiento por los usuarios(USB, Discos Externos, etc). Los dispositivos al conectarse en otros lugares pueden tener virus
Discos Duros	No hay un cifrado o esté es inseguro por lo que cualquier persona puede ver la información que contiene el disco sin autorización
VoIP	Pérdida de privacidad. La mayor parte del tráfico de VoIP no está cifrado, lo que facilita a que intrusos escuchen sus conversaciones de VoIP.
Routers AP	Al conectarse la red la contraseña usualmente es guardada por todos los dispositivos conectados. Si un trabajador deja la organización, o si se pierde o roba un dispositivo Wi-Fi, pueden hacer uso de la conexión que se tiene a la red
Discos Duros Externos	Una vulnerabilidad que no se controla es el uso de dispositivos de almacenamiento por los usuarios(USB, Discos Externos, etc). Los dispositivos al conectarse en otros lugares pueden tener virus
Almacenamiento en Red	No se tiene perfiles de seguridad por lo que la información puede ser copiada, transmitida, visualizada, robada, destruida, alterada o se puede usar de forma no autorizada
Documentos Ordinarios	La información puede ser copiada, transmitida, visualizada, robada, destruida, alterada o se puede usar de forma no autorizada

Nota. Vulnerabilidades con los activos a trabajar. Adaptado de INCIBE Instituto Nacional de Ciberseguridad, 2017, (https://normas-apa.org/wp-content/uploads/Guia-Normas-APA-7ma-edicion.pdf).

Fase 5: Evaluar el riesgo

Para evaluar el riesgo se realizaron dos matrices:

Matriz de Probabilidad: En la matriz se realizó la evaluación presentada en la figura 7.

Matriz de Impacto: En la matriz se realizó la evaluación presentada en la figura 8.

Tomando en cuenta las valoraciones, luego se realizó la evaluación por cada activo con su amenaza.

Matriz de probabilidad:

Figura 13

Matriz de probabilidad

Probabilidad	Valor
Nunca	0
Año	1
Mes	2
Semana	3

N°	ACTIVO / AMENAZA	SERVICIOS												DATOS					APLICACIONES								
		Telefonia IP	Correo Institucional	Servicios de mantenimiento motorolas	Servicio de mantenimiento camaras ip	Servicio de mantenimiento de firewall	Servicio de mantenimiento UTM	servicio de mantenimiento pagina web	Active Directory	Internet	video conferencia	sistema F.A.E	Chasqui	Documentos Secretos	Documentos Confidenciales	Documentos de Uso Interno	Documentos ordinarios	Base de datos	Apache	Office	Cobian	Osc Inventory	VNC	Putty	MySQL	Tera Term	Windows
1	Fuego	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	Daños por agua	0	0	0	0	0	0	0	0	0	0	0	0	2	2	2	2	2	0	0	0	0	0	0	0	0	0
3	Desastres naturales	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	Corte del suministro eléctrico	1	1	1	1	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1	1	1	1	1
5	Condiciones inadecuadas de temperatura o humedad	0	0	0	0	0	0	0	0	0	0	0	0	2	2	2	2	2	0	0	0	0	0	0	0	0	0
6	Fallo de servicios de comunicaciones	1	1	1	1	1	1	1	1	1	1	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	2
7	Desastres industriales	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	Fuga de información	1	1	1	1	1	1	1	1	0	0	0	0	1	1	1	1	1	1	0	0	0	1	0	0	0	1
9	Introducción de falsa información	1	1	1	1	1	1	1	1	2	1	1	2	0	0	2	2	1	1	1	0	0	0	0	1	1	2
10	Acceso no autorizado	1	2	1	1	2	2	2	2	2	1	1	1	1	1	2	2	1	1	2	1	1	2	1	1	1	3
11	Vulnerabilidad de programas (software)	1	2	1	2	1	1	2	1	3	1	2	2	1	1	1	2	1	2	2	1	1	1	1	2	1	3
12	Corrupción de la información	2	2	1	1	1	1	2	1	2	1	1	2	1	1	2	2	1	1	2	1	1	1	1	2	1	2
13	Destrucción de información	1	2	1	1	1	1	1	1	3	1	2	2	1	1	1	2	1	1	2	1	1	1	1	1	1	2
14	Interceptación de información (escucha)	2	2	1	1	1	1	1	1	3	2	1	1	1	1	1	2	1	1	2	1	1	1	1	1	1	3
15	Indisponibilidad del personal	2	2	1	1	1	1	1	2	3	2	2	2	1	1	1	1	1	2	1	2	2	2	2	2	2	1
16	Agotamiento de recursos	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	0	0	0	0	0	0
17	Errores de los usuarios	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	2
18	Errores del administrador	2	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
19	Errores de configuración	1	1	1	1	1	1	1	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
20	Degradación de los soportes de almacenamiento de la información	1	2	1	1	1	1	1	2	2	1	1	1	1	1	1	1	2	2	1	1	1	1	1	1	1	2
21	Difusión de software dañino	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2
22	Errores de mantenimiento / actualización de programas (software)	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	1	1	1	2
23	Errores de mantenimiento / actualización de equipos (hardware)	1	1	1	1	1	1	1	1	2	2	1	1	1	1	1	1	1	0	0	0	0	0	0	0	0	0
24	Caída del sistema por sobrecarga	1	2	1	1	1	1	1	1	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	2

Probabilidad	Valor
Nunca	0
Año	1
Mes	2
Semana	3

N°	ACTIVO / AMENAZA	EQUIPOS INFORMÁTICOS											REDES DE COMUNICACIONES					SOPORTE DE INFORMACIÓN				EQUIPAMIENTO AUXILIAR					
		Tester	Servidores de torre HP Gen8	Switch de rack Cisco	Switch de rack Dlink	Switch de rack Huawei	Servidores de torre IBM	Servidor UTM	Servidor Firewall	Servidor de Backup	Computadoras de Escritorio (10)	Laptop (2)	Motorolas	Routers AP	Router Prueba	VOIP	Vlans	Discos Duros	Almacenamiento en Red	Disco Duro Externo	Back up de archivos	Fuentes de alimentación	generadores eléctricos	UPS	Cable UTP	Cable de Fibra	Reguladores de Voltaje
1	Fuego	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	Daños por agua	2	2	2	2	2	2	2	2	2	2	2	2	2	2	2	0	2	0	2	1	2	2	1	1	1	2
3	Desastres naturales	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	Corte del suministro eléctrico	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1
5	Condiciones inadecuadas de temperatura o humedad	1	2	2	2	2	2	2	2	2	2	2	2	2	2	0	0	1	1	1	1	1	1	1	1	1	1
6	Fallo de servicios de comunicaciones	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	0	0	0	1	1	0
7	Desastres industriales	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	Fuga de información	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	2	2	2	1	0	0	0	0	0	0
9	Introducción de falsa información	0	0	1	1	1	1	1	1	1	2	2	1	2	2	1	2	1	2	1	1	1	1	1	1	1	1
10	Acceso no autorizado	1	1	1	1	1	1	1	1	1	2	2	1	2	2	2	1	2	2	2	1	1	1	1	1	1	1
11	Vulnerabilidad de programas (software)	1	1	1	2	2	1	1	1	1	2	2	1	2	2	1	1	2	2	2	1	2	1	1	2	1	1
12	Corrupción de la información	0	1	1	2	2	1	1	1	1	2	2	1	2	2	1	1	2	2	2	1	1	1	1	2	2	1
13	Destrucción de información	0	1	1	1	1	1	1	1	1	2	2	1	1	2	1	1	2	2	2	1	1	1	1	1	1	1
14	Interceptación de información (escucha)	0	1	1	1	1	1	1	1	1	3	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
15	Indisponibilidad del personal	1	1	1	1	1	1	1	1	1	1	3	1	1	2	1	1	1	1	1	1	1	1	1	2	3	1
16	Agotamiento de recursos	2	1	2	2	2	1	1	1	1	1	3	2	1	2	1	1	1	1	1	1	1	1	1	2	3	1
17	Errores de los usuarios	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
18	Errores del administrador	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
19	Errores de configuración	0	1	1	1	1	1	1	1	1	1	1	2	1	1	1	2	1	1	1	1	1	1	1	1	1	1
20	Degradación de los soportes de almacenamiento de la información	0	1	1	1	1	1	1	1	1	2	2	1	1	1	1	1	2	2	2	1	1	1	1	1	1	1
21	Difusión de software dañino	0	1	1	1	1	1	1	1	1	2	2	0	1	1	1	1	2	2	2	1	1	1	1	1	1	1
22	Errores de mantenimiento / actualización de programas (software)	0	1	1	1	1	1	1	1	1	2	2	0	1	1	1	0	1	1	1	1	0	0	0	0	0	0
23	Errores de mantenimiento / actualización de equipos (hardware)	0	1	2	1	1	1	1	1	1	2	2	2	1	1	1	1	1	1	1	1	1	1	1	2	2	1
24	Caída del sistema por sobrecarga	0	1	2	2	2	1	1	1	1	1	1	2	3	2	2	1	2	2	2	1	1	1	1	1	1	1

Probabilidad	Valor
Nunca	0
Año	1
Mes	2
Semana	3

N°	ACTIVO / AMENAZA	REDES DE COMUNICACIONES					SOPORTE DE INFORMACIÓN				EQUIPAMIENTO AUXILIAR						INSTALACIONES							PERSONAL				
		Motorolas	Routers AP	Router Prueba	VOIP	Vlans	Discos Duros	Almacenamiento en Red	Disco Duro Externo	Back up de archivos	Fuentes de alimentación	generadores eléctricos	UPS	Cable UTP	Cable de Fibra	Reguladores de Voltaje	Central Telefonica	Cuarto de Servidores	Comunicaciones	Area de Procesamiento de la informacion	Area de Electronica	Area de Informatica	Area de Telefonia	Soporte Técnico	Redes	Seguridad de la Información	Centro Procesamiento de la Información	RadioComunicaciones
1	Fuego	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	Daños por agua	2	2	2	2	0	2	0	2	1	2	2	1	1	1	2	2	2	2	2	2	2	2	2	2	2	2	2
3	Desastres naturales	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	Corte del suministro eléctrico	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
5	Condiciones inadecuadas de temperatura o humedad	2	2	2	0	0	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	2	2
6	Fallo de servicios de comunicaciones	1	1	1	1	2	1	1	1	1	0	0	0	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1
7	Desastres industriales	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	Fuga de información	1	0	0	1	0	2	2	2	1	0	0	0	0	0	0	0	0	0	1	0	0	0	1	2	2	2	1
9	Introducción de falsa información	1	2	2	1	2	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	2
10	Acceso no autorizado	1	2	2	2	1	2	2	2	1	1	1	1	1	1	1	1	1	2	1	2	2	1	2	2	1	1	1
11	Vulnerabilidad de programas (software)	1	2	2	1	1	2	2	2	1	2	1	1	2	1	1	1	2	2	2	2	2	1	2	2	1	1	2
12	Corrupción de la información	1	2	2	1	1	2	2	2	1	1	1	1	2	2	1	2	1	2	1	2	2	1	2	2	1	1	2
13	Destrucción de información	1	1	2	1	1	2	2	2	1	1	1	1	1	1	1	2	1	1	2	1	2	1	2	2	1	1	1
14	Interceptación de información (escucha)	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	2	2	1	2	2	1	2	1	2	2
15	Indisponibilidad del personal	1	1	2	1	1	1	1	1	1	1	1	1	2	3	1	1	1	1	1	1	1	1	1	2	1	1	1
16	Agotamiento de recursos	2	1	2	1	1	1	1	1	1	1	1	1	2	3	1	1	1	1	1	1	1	1	1	2	1	1	1
17	Errores de los usuarios	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
18	Errores del administrador	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
19	Errores de configuración	2	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	2	2	1	1	1
20	Degradación de los soportes de almacenamiento de la información	1	1	1	1	1	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2
21	Difusión de software dañino	0	1	1	1	1	2	2	2	1	1	1	1	1	1	1	1	1	1	2	1	2	1	1	2	2	1	1
22	Errores de mantenimiento / actualización de programas (software)	0	1	1	1	0	1	1	1	1	0	0	0	0	0	0	0	1	0	1	0	1	0	0	1	1	1	1
23	Errores de mantenimiento / actualización de equipos (hardware)	2	1	1	1	1	1	1	1	1	1	1	1	2	2	1	2	2	2	2	1	2	2	2	2	1	2	2
24	Caída del sistema por sobrecarga	2	3	2	2	1	2	2	2	1	1	1	1	1	1	1	1	2	2	2	1	2	2	1	2	1	2	2

Probabilidad	Valor
Nunca	0
Año	1
Mes	2
Semana	3

N°	ACTIVO / AMENAZA	SERVICIOS												DATOS					APLICACIONES								
		Telefonia IP	Correo Institucional	Servicios de mantenimiento motorolas	Servicio de mantenmiento camaras ip	Servicio de mantenimiento de firewall	Servicio de mantenimiento UTM	servicio de mantenimiento pagina web	Active Directory	Internet	video conferencia	sistema F.A.E	Chasqui	Documentos Secretos	Documentos Confidenciales	Documentos de Uso Interno	Documentos ordinarios	Base de datos	Apache	Office	Cobian	Osc Inventory	VNC	Putty	MySQL	Tera Term	Windows
25	Denegación de servicio	2	1	1	1	1	1	1	2	2	1	1	1	1	1	1	1	1	2	1	2	1	1	1	1	1	2
26	Robo	1	1	1	1	1	1	1	2	2	2	1	1	1	1	1	2	1	1	2	1	1	1	1	1	1	2
27	Ataques destructivos	1	1	1	1	1	1	1	2	2	2	1	1	1	1	1	2	2	2	1	2	1	1	1	1	1	2
28	Extorsión	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
29	Ingeniería social	1	2	1	1	1	1	1	2	2	2	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1
30	Manipulación de logs	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2
31	Abuso de privilegios de acceso	1	1	1	1	1	2	1	2	3	1	1	1	1	1	1	2	1	1	1	1	1	1	2	1	2	2
32	Manipulación de equipos	1	1	1	1	1	1	1	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2
33	Manipulación de configuración	1	1	1	1	1	1	1	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	2
34	Alteración de la información	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	2

Probabilidad	Valor
Nunca	0
Año	1
Mes	2
Semana	3

N°	ACTIVO / AMENAZA	EQUIPOS INFORMÁTICOS											REDES DE COMUNICACIONES					SOPORTE DE INFORMACIÓN				EQUIPAMIENTO AUXILIAR					
		Tester	Servidores de torre HP Gen6	Switch de rack Cisco	Switch de rack Dlink	Switch de rack Huawei	Servidores de torre IBM	Servidor UTM	Servidor Firewall	Servidor de Backup	Computadoras de Escritorio (10)	Laptop (2)	Motorolas	Routers AP	Router Prueba	VOIP	Vlans	Discos Duros	Almacenamiento en Red	Disco Duro Externo	Back up de archivos	Fuentes de alimentación	generadores eléctricos	UPS	Cable UTP	Cable de Fibra	Reguladores de Voltaje
25	Denegación de servicio	0	1	1	1	1	1	1	1	1	1	1	1	2	2	2	1	1	1	1	1	1	1	1	1	1	1
26	Robo	0	1	1	1	1	1	1	1	1	2	2	1	2	2	2	1	1	1	1	1	1	1	1	1	1	1
27	Ataques destructivos	0	1	1	1	1	1	1	1	1	2	2	1	2	2	2	1	1	1	1	1	1	1	1	1	1	1
28	Extorsión	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
29	Ingeniería social	0	1	1	1	1	1	1	1	1	2	2	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1
30	Manipulación de logs	0	1	1	1	1	1	2	1	1	1	1	1	1	1	1	2	1	1	1	1	0	0	0	0	0	0
31	Abuso de privilegios de acceso	0	1	2	2	1	1	2	1	1	2	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1
32	Manipulación de equipos	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	2	1
33	Manipulación de configuración	0	1	1	1	1	1	2	1	1	2	2	1	1	1	1	2	1	1	1	1	1	1	1	1	2	1
34	Alteración de la información	0	1	2	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Probabilidad	Valor
Nunca	0
Año	1
Mes	2
Semana	3

N°	ACTIVO / AMENAZA	REDES DE COMUNICACIONES					SOPORTE DE INFORMACIÓN				EQUIPAMIENTO AUXILIAR						INSTALACIONES							PERSONAL				
		Motorolas	Routers AP	Router Prueba	VOIP	Vlans	Discos Duros	Almacenamiento en Red	Disco Duro Externo	Back up de archivos	Fuentes de alimentación	generadores eléctricos	UPS	Cable UTP	Cable de Fibra	Reguladores de Voltaje	Central Telefonica	Cuarto de Servidores	Comunicaciones	Area de Procesamiento de la informacion	Area de Electronica	Area de Informatica	Area de Telefonia	Soporte Técnico	Redes	Seguridad de la Información	Centro Procesamiento de la Información	RadioComunicaciones
25	Denegación de servicio	1	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	1	2	2	1	2	1	2	2
26	Robo	1	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	1	2	2	1	2	1	2	2
27	Ataques destructivos	1	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	1	2	2	1	2	1	2	2
28	Extorsión	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
29	Ingeniería social	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	2	2	1	2	1	1	2
30	Manipulación de logs	1	1	1	1	2	1	1	1	1	0	0	0	0	0	0	1	1	2	2	1	2	1	1	2	1	1	1
31	Abuso de privilegios de acceso	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	2	2	2	1	1	2	2	1	2	1	1	2
32	Manipulación de equipos	1	1	1	1	2	1	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1
33	Manipulación de configuración	1	1	1	1	2	1	1	1	1	1	1	1	1	2	1	1	2	2	1	1	2	1	2	2	1	1	1
34	Alteración de la información	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	1	2	1	1	2	1	1	1

Nota. Evaluación de la matriz de probabilidad. Fuente: (Amutio, Candau, & Mañas, 2012).

Matriz de impacto:

Figura 14

Matriz de impacto

Impacto	Valor
No hay consecuencias	0
No hay consecuencias relevantes	1
Consecuencias relevantes	2
Hay consecuencias graves	3

N°	ACTIVO / AMENAZA	SERVICIOS												DATOS					APLICACIONES								
		Telefonia IP	Correo Institucional	Servicios de mantenimiento motorolas	Servicio de mantenmiento camaras ip	Servicio de mantenimiento de firewall	Servicio de mantenimiento UTM	servicio de mantenimiento pagina web	Active Directory	Internet	video conferencia	sistema F.A.E	Chasqui	Documentos Secretos	Documentos Confidenciales	Documentos de Uso Interno	Documentos ordinarios	Base de datos	Apache	Office	Cobian	Osc Inventory	VNC	Putty	MySQL	Tera Term	Windows
1	Fuego	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	Daños por agua	0	0	0	0	0	0	0	0	0	0	0	0	3	3	2	2	3	0	0	0	0	0	0	0	0	0
3	Desastres naturales	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	Corte del suministro eléctrico	2	1	1	1	2	2	1	2	2	2	1	1	0	0	0	0	1	1	1	1	1	1	1	1	1	1
5	Condiciones inadecuadas de temperatura o humedad	0	0	0	0	0	0	0	0	0	0	0	0	3	3	2	2	3	0	0	0	0	0	0	0	0	0
6	Fallo de servicios de comunicaciones	2	1	1	1	1	1	1	1	1	1	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	2
7	Desastres industriales	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	Fuga de información	2	3	1	1	1	1	1	2	3	3	0	0	3	3	2	2	3	2	0	0	0	1	0	0	0	1
9	Introducción de falsa información	1	1	2	2	2	2	2	1	2	2	1	2	3	3	2	2	3	2	1	0	0	0	0	1	1	2
10	Acceso no autorizado	1	2	2	3	3	3	3	3	3	3	1	1	3	3	3	3	3	2	2	1	1	2	1	1	1	3
11	Vulnerabilidad de programas (software)	1	2	2	2	2	2	2	1	3	2	2	2	3	3	2	2	3	3	2	3	1	1	1	2	1	3
12	Corrupción de la información	2	2	2	2	2	2	2	2	2	2	2	2	3	3	2	2	3	3	2	3	1	1	1	2	1	2
13	Destrucción de información	1	2	2	2	3	3	2	3	2	2	2	2	3	3	3	3	3	3	2	3	2	2	2	2	2	2
14	Interceptación de información (escucha)	2	2	1	1	1	1	1	1	3	3	1	1	3	3	3	2	3	1	2	1	1	1	1	1	1	3
15	Indisponibilidad del personal	2	2	2	2	2	2	2	2	3	2	2	2	1	1	1	1	2	2	1	2	1	1	1	1	1	1
16	Agotamiento de recursos	1	1	2	2	2	2	2	1	2	2	1	1	1	1	1	1	1	1	0	1	0	0	0	0	0	0
17	Errores de los usuarios	1	2	1	1	1	1	1	1	2	2	1	1	2	2	2	2	2	2	2	2	1	1	1	1	1	2
18	Errores del administrador	2	2	1	2	2	3	1	1	2	1	2	2	2	2	2	1	1	1	1	1	1	1	2	1	2	1
19	Errores de configuración	1	2	1	2	2	3	2	1	2	1	2	2	3	2	2	1	1	1	1	1	1	1	2	1	2	1
20	Degradación de los soportes de almacenamiento de la información	1	2	1	1	1	1	1	2	2	1	1	1	1	1	1	1	2	2	1	1	1	1	1	1	1	2
21	Difusión de software dañino	1	2	2	1	2	3	2	2	2	1	2	2	3	2	2	1	1	2	1	1	1	1	2	1	2	2
22	Errores de mantenimiento / actualización de programas (software)	1	1	2	1	3	3	2	1	2	1	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	2
23	Errores de mantenimiento / actualización de equipos (hardware)	1	2	1	2	2	3	1	2	2	1	2	2	1	1	1	1	2	1	1	1	1	1	1	1	1	1
24	Caída del sistema por sobrecarga	1	2	1	1	3	3	2	2	2	1	2	2	2	2	2	1	1	2	1	1	1	1	2	1	2	2

Impacto	Valor
No hay consecuencias	0
No hay consecuencias relevantes	1
Consecuencias relevantes	2
Hay consecuencias graves	3

N°	ACTIVO / AMENAZA	EQUIPOS INFORMÁTICOS											REDES DE COMUNICACIONES					SOPORTE DE INFORMACIÓN				EQUIPAMIENTO AUXILIAR					
		Tester	Servidores de torre HP Gen6	Switch de rack Cisco	Switch de rack Dlink	Switch de rack Huawei	Servidores de torre IBM	Servidor UTM	Servidor Firewall	Servidor de Backup	Computadoras de Escritorio (10)	Laptop (2)	Motorolas	Routers AP	Router Prueba	VOIP	Vlans	Discos Duros	Almacenamiento en Red	Disco Duro Externo	Back up de archivos	Fuentes de alimentación	generadores eléctricos	UPS	Cable UTP	Cable de Fibra	Reguladores de Voltaje
1	Fuego	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	Daños por agua	2	3	3	3	3	3	3	3	2	2	2	2	2	2	2	0	2	0	2	1	2	2	2	2	2	2
3	Desastres naturales	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	Corte del suministro eléctrico	0	2	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1
5	Condiciones inadecuadas de temperatura o humedad	1	3	3	3	3	3	3	3	2	2	2	2	2	2	0	0	1	1	1	1	1	1	1	1	1	1
6	Fallo de servicios de comunicaciones	0	2	2	2	2	2	2	2	2	1	1	1	1	1	1	2	1	1	1	1	0	0	0	1	1	0
7	Desastres industriales	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	Fuga de información	0	0	0	0	0	0	0	0	0	0	0	1	0	0	1	0	2	2	2	1	0	0	0	0	0	0
9	Introducción de falsa información	0	2	2	2	2	2	2	2	2	2	2	1	2	2	1	2	1	2	1	1	1	1	1	1	1	1
10	Acceso no autorizado	0	3	3	3	3	3	3	3	3	2	2	1	2	2	2	1	2	2	2	1	1	1	1	1	1	1
11	Vulnerabilidad de programas (software)	0	2	2	2	2	2	2	2	2	2	2	1	2	2	1	1	2	2	2	1	2	1	1	2	1	1
12	Corrupción de la información	0	2	2	2	2	2	2	2	2	2	2	1	2	2	1	1	2	2	2	1	1	1	1	2	2	1
13	Destrucción de información	0	2	2	2	2	2	2	2	2	2	2	1	1	2	1	1	2	2	2	1	1	1	1	1	1	1
14	Interceptación de información (escucha)	0	1	1	1	1	1	1	1	1	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1
15	Indisponibilidad del personal	0	2	2	2	2	2	2	2	2	1	1	1	1	2	1	1	1	1	1	1	1	1	1	2	3	1
16	Agotamiento de recursos	0	1	2	2	2	1	1	1	1	1	3	2	1	2	1	1	1	1	1	1	1	1	1	2	3	1
17	Errores de los usuarios	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
18	Errores del administrador	0	2	2	2	2	2	2	2	1	1	1	2	1	0	1	3	1	1	1	1	1	1	1	2	3	1
19	Errores de configuración	0	2	2	2	2	2	3	2	1	1	1	2	1	0	1	3	1	1	1	1	1	1	1	1	2	1
20	Degradación de los soportes de almacenamiento de la información	0	1	1	1	1	1	1	1	1	2	2	1	1	1	1	1	2	2	2	1	1	1	1	1	1	1
21	Difusión de software dañino	0	2	2	2	2	2	3	3	1	2	2	1	1	1	1	1	2	2	2	2	1	1	1	1	1	1
22	Errores de mantenimiento / actualización de programas (software)	0	2	2	2	2	2	3	3	1	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
23	Errores de mantenimiento / actualización de equipos (hardware)	0	2	2	2	2	2	3	3	1	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
24	Caída del sistema por sobrecarga	0	3	3	3	3	3	3	3	2	2	1	1	1	0	1	3	1	1	1	1	1	1	1	2	2	1

Impacto	Valor
No hay consecuencias	0
No hay consecuencias relevantes	1
Consecuencias relevantes	2
Hay consecuencias graves	3

N°	ACTIVO / AMENAZA	REDES DE COMUNICACIONES					SOPORTE DE INFORMACIÓN				EQUIPAMIENTO AUXILIAR						INSTALACIONES							PERSONAL				
		Motorolas	Routers AP	Router Prueba	VOIP	Vlans	Discos Duros	Almacenamiento en Red	Disco Duro Externo	Back up de archivos	Fuentes de alimentación	generadores eléctricos	UPS	Cable UTP	Cable de Fibra	Reguladores de Voltaje	Central Telefonica	Cuarto de Servidores	Comunicaciones	Area de Procesamiento de la informacion	Area de Electronica	Area de Informatica	Area de Telefonia	Soporte Técnico	Redes	Seguridad de la Información	Centro Procesamiento de la Información	RadioComunicaciones
1	Fuego	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	Daños por agua	2	2	2	2	0	2	0	2	1	2	2	2	2	2	2	2	3	2	3	2	3	2	3	3	2	2	2
3	Desastres naturales	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
4	Corte del suministro eléctrico	1	1	1	1	1	1	1	1	1	0	1	1	1	1	1	1	2	1	2	1	2	1	3	3	1	1	3
5	Condiciones inadecuadas de temperatura o humedad	2	2	2	0	0	1	1	1	1	1	1	1	1	1	1	2	3	2	2	3	3	2	2	2	2	2	2
6	Fallo de servicios de comunicaciones	1	1	1	1	2	1	1	1	1	0	0	0	1	1	0	2	3	1	1	1	3	1	1	2	1	1	2
7	Desastres industriales	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
8	Fuga de información	1	0	0	1	0	2	2	2	1	0	0	0	0	0	0	2	2	2	2	2	2	2	2	2	2	2	2
9	Introducción de falsa información	1	2	2	1	2	1	2	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	2	2	2	2	2
10	Acceso no autorizado	1	2	2	2	1	2	2	2	1	1	1	1	1	1	1	2	2	2	2	2	2	2	2	2	2	2	2
11	Vulnerabilidad de programas (software)	1	2	2	1	1	2	2	2	1	2	1	1	2	1	1	2	2	2	2	2	2	2	2	2	2	2	1
12	Corrupción de la información	1	2	2	1	1	2	2	2	1	1	1	1	2	2	1	2	2	2	2	2	2	2	2	2	2	2	2
13	Destrucción de información	1	1	2	1	1	2	2	2	1	1	1	1	1	1	1	1	2	2	2	1	2	1	1	1	2	2	1
14	Interceptación de información (escucha)	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	1	2	2	1	2	2	1	2	1	2	2
15	Indisponibilidad del personal	1	1	2	1	1	1	1	1	1	1	1	1	2	3	1	2	2	1	2	1	2	1	2	3	2	2	2
16	Agotamiento de recursos	2	1	2	1	1	1	1	1	1	1	1	1	2	3	1	1	1	1	1	1	2	1	3	3	2	2	2
17	Errores de los usuarios	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	1
18	Errores del administrador	2	1	0	1	3	1	1	1	1	1	1	1	2	3	1	2	2	2	2	1	2	1	1	2	2	2	1
19	Errores de configuración	2	1	0	1	3	1	1	1	1	1	1	1	1	2	1	2	2	2	2	1	2	1	2	2	2	2	1
20	Degradación de los soportes de almacenamiento de la información	1	1	1	1	1	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2
21	Difusión de software dañino	1	1	1	1	1	2	2	2	2	1	1	1	1	1	1	2	2	2	3	1	2	1	1	2	3	3	2
22	Errores de mantenimiento / actualización de programas (software)	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	1	2	1	1	2	2	2	2
23	Errores de mantenimiento / actualización de equipos (hardware)	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
24	Caída del sistema por sobrecarga	1	1	0	1	3	1	1	1	1	1	1	1	2	2	1	2	3	2	2	1	2	1	1	2	3	3	1

Impacto	Valor
No hay consecuencias	0
No hay consecuencias relevantes	1
Consecuencias relevantes	2
Hay consecuencias graves	3

N°	ACTIVO / AMENAZA	SERVICIOS												DATOS					APLICACIONES								
		Telefonia IP	Correo Institucional	Servicios de mantenimiento motorolas	Servicio de mantenmiento camaras ip	Servicio de mantenimiento de firewall	Servicio de mantenimiento UTM	servicio de mantenimiento pagina web	Active Directory	Internet	video conferencia	sistema F.A.E	Chasqui	Documentos Secretos	Documentos Confidenciales	Documentos de Uso Interno	Documentos ordinarios	Base de datos	Apache	Office	Cobian	Osc Inventory	VNC	Putty	MySQL	Tera Term	Windows
16	Agotamiento de recursos	1	1	2	2	2	2	2	1	2	2	1	1	1	1	1	1	1	1	0	1	0	0	0	0	0	0
17	Errores de los usuarios	1	2	1	1	1	1	1	1	2	2	1	1	2	2	2	2	2	2	2	2	1	1	1	1	1	2
18	Errores del administrador	2	2	1	2	2	3	1	1	2	1	2	2	2	2	2	1	1	1	1	1	1	1	2	1	2	1
19	Errores de configuración	1	2	1	2	2	3	2	1	2	1	2	2	3	2	2	1	1	1	1	1	1	1	2	1	2	1
20	Degradación de los soportes de almacenamiento de la información	1	2	1	1	1	1	1	2	2	1	1	1	1	1	1	1	2	2	1	1	1	1	1	1	1	2
21	Difusión de software dañino	1	2	2	1	2	3	2	2	2	1	2	2	3	2	2	1	1	2	1	1	1	1	2	1	2	2
22	Errores de mantenimiento / actualización de programas (software)	1	1	2	1	3	3	2	1	2	1	2	2	2	2	2	2	2	1	1	1	1	1	1	1	1	2
23	Errores de mantenimiento / actualización de equipos (hardware)	1	2	1	2	2	3	1	2	2	1	2	2	1	1	1	1	2	1	1	1	1	1	1	1	1	1
24	Caída del sistema por sobrecarga	1	2	1	1	3	3	2	2	2	1	2	2	2	2	2	1	1	2	1	1	1	1	2	1	2	2
25	Denegación de servicio	1	2	1	1	3	3	1	1	2	1	2	2	3	3	2	1	1	2	1	1	1	1	1	1	1	2
26	Robo	1	2	1	1	1	2	1	1	2	1	2	2	3	3	2	1	1	1	1	1	1	1	1	1	1	1
27	Ataques destructivos	1	2	1	1	2	3	2	1	2	1	2	2	3	3	2	1	1	2	1	1	1	1	1	1	1	1
28	Extorsión	1	1	1	1	1	2	1	1	2	1	2	2	3	3	3	2	1	1	1	1	1	1	1	1	1	1
29	Ingeniería social	1	2	1	1	2	2	1	1	1	1	2	2	3	3	3	2	1	1	1	1	1	1	1	1	1	2
30	Manipulación de logs	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2
31	Abuso de privilegios de acceso	1	1	1	1	1	1	1	1	1	1	1	1	3	3	3	2	2	1	1	1	1	1	1	1	1	1
32	Manipulación de equipos	1	1	1	1	1	2	1	1	1	1	1	1	3	3	2	1	2	1	1	1	1	1	2	1	2	1
33	Manipulación de configuración	1	2	2	2	3	3	1	2	2	1	2	2	2	2	2	1	1	1	1	1	1	1	2	1	2	1
34	Alteración de la información	1	1	2	2	3	3	1	1	2	1	2	2	3	3	3	2	1	2	1	1	1	1	2	1	2	1

Impacto	Valor
No hay consecuencias	0
No hay consecuencias relevantes	1
Consecuencias relevantes	2
Hay consecuencias graves	3

N°	ACTIVO / AMENAZA	EQUIPOS INFORMÁTICOS											REDES DE COMUNICACIONES					SOPORTE DE INFORMACIÓN				EQUIPAMIENTO AUXILIAR					
		Tester	Servidores de torre HP Gen6	Switch de rack Cisco	Switch de rack Dlink	Switch de rack Huawei	Servidores de torre IBM	Servidor UTM	Servidor Firewall	Servidor de Backup	Computadoras de Escritorio (10)	Laptop (2)	Motorolas	Routers AP	Router Prueba	VOIP	Vlans	Discos Duros	Almacenamiento en Red	Disco Duro Externo	Back up de archivos	Fuentes de alimentación	generadores eléctricos	UPS	Cable UTP	Cable de Fibra	Reguladores de Voltaje
16	Agotamiento de recursos	0	1	2	2	2	1	1	1	1	1	3	2	1	2	1	1	1	1	1	1	1	1	1	2	3	1
17	Errores de los usuarios	0	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
18	Errores del administrador	0	2	2	2	2	2	2	2	1	1	1	2	1	0	1	3	1	1	1	1	1	1	1	2	3	1
19	Errores de configuración	0	2	2	2	2	2	3	2	1	1	1	2	1	0	1	3	1	1	1	1	1	1	1	1	2	1
20	Degradación de los soportes de almacenamiento de la información	0	1	1	1	1	1	1	1	1	2	2	1	1	1	1	1	2	2	2	1	1	1	1	1	1	1
21	Difusión de software dañino	0	2	2	2	2	2	3	3	1	2	2	1	1	1	1	1	2	2	2	2	1	1	1	1	1	1
22	Errores de mantenimiento / actualización de programas (software)	0	2	2	2	2	2	3	3	1	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
23	Errores de mantenimiento / actualización de equipos (hardware)	0	2	2	2	2	2	3	3	1	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
24	Caída del sistema por sobrecarga	0	3	3	3	3	3	3	3	2	2	1	1	1	0	1	3	1	1	1	1	1	1	1	2	2	1
25	Denegación de servicio	0	2	2	2	2	2	3	3	1	1	1	1	1	1	1	2	1	1	1	1	1	1	1	2	2	1
26	Robo	0	2	2	2	2	2	3	2	2	2	2	1	1	1	1	1	2	1	1	1	1	1	1	2	2	1
27	Ataques destructivos	0	2	2	2	2	2	3	3	2	2	1	1	1	1	1	2	1	1	1	1	1	1	1	2	2	1
28	Extorsión	0	2	2	2	2	2	3	2	3	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
29	Ingeniería social	0	2	2	2	2	2	3	3	2	1	1	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1
30	Manipulación de logs	0	1	1	1	1	1	2	1	1	1	1	1	1	1	1	2	1	1	1	1	0	0	0	0	0	0
31	Abuso de privilegios de acceso	0	2	2	2	2	2	3	2	2	1	1	1	1	0	1	2	1	1	1	1	1	1	1	1	1	1
32	Manipulación de equipos	0	2	2	2	2	2	3	3	2	1	1	2	1	1	1	2	1	1	1	1	1	1	1	2	2	1
33	Manipulación de configuración	0	2	2	2	2	2	3	3	2	1	1	1	1	1	1	2	1	1	1	1	1	1	1	2	2	1
34	Alteración de la información	0	2	2	2	2	2	3	3	2	1	1	1	1	1	1	2	1	1	1	1	1	1	1	2	2	1

Impacto	Valor
No hay consecuencias	0
No hay consecuencias relevantes	1
Consecuencias relevantes	2
Hay consecuencias graves	3

N°	ACTIVO / AMENAZA	REDES DE COMUNICACIONES					SOPORTE DE INFORMACIÓN				EQUIPAMIENTO AUXILIAR						INSTALACIONES							PERSONAL				
		Motorolas	Routers AP	Router Prueba	VOIP	Vlans	Discos Duros	Almacenamiento en Red	Disco Duro Externo	Back up de archivos	Fuentes de alimentación	generadores eléctricos	UPS	Cable UTP	Cable de Fibra	Reguladores de Voltaje	Central Telefonica	Cuarto de Servidores	Comunicaciones	Area de Procesamiento de la informacion	Area de Electronica	Area de Informatica	Area de Telefonia	Soporte Técnico	Redes	Seguridad de la Información	Centro Procesamiento de la Información	RadioComunicaciones
16	Agotamiento de recursos	2	1	2	1	1	1	1	1	1	1	1	1	2	3	1	1	1	1	1	1	2	1	3	3	2	2	2
17	Errores de los usuarios	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2	2	1
18	Errores del administrador	2	1	0	1	3	1	1	1	1	1	1	1	2	3	1	2	2	2	2	1	2	1	1	2	2	2	1
19	Errores de configuración	2	1	0	1	3	1	1	1	1	1	1	1	1	2	1	2	2	2	2	1	2	1	2	2	2	2	1
20	Degradación de los soportes de almacenamiento de la información	1	1	1	1	1	2	2	2	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	2
21	Difusión de software dañino	1	1	1	1	1	2	2	2	2	1	1	1	1	1	1	2	2	2	3	1	2	1	1	2	3	3	2
22	Errores de mantenimiento / actualización de programas (software)	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	2	1	2	1	1	2	2	2	2
23	Errores de mantenimiento / actualización de equipos (hardware)	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1
24	Caída del sistema por sobrecarga	1	1	0	1	3	1	1	1	1	1	1	1	2	2	1	2	3	2	2	1	2	1	1	2	3	3	1
25	Denegación de servicio	1	1	1	1	2	1	1	1	1	1	1	1	2	2	1	2	2	2	2	1	2	1	1	2	2	2	1
26	Robo	1	1	1	1	1	2	1	1	1	1	1	1	2	2	1	2	2	2	3	1	2	1	1	2	3	3	1
27	Ataques destructivos	1	1	1	1	2	1	1	1	1	1	1	1	2	2	1	2	2	2	2	1	2	1	1	2	3	3	1
28	Extorsión	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	3	1	2	1	1	2	3	3	2
29	Ingeniería social	1	1	0	1	1	1	1	1	1	1	1	1	1	1	1	2	2	2	3	1	2	1	2	2	3	3	2
30	Manipulación de logs	1	1	1	1	2	1	1	1	1	0	0	0	0	0	0	1	1	2	2	1	2	1	1	2	1	1	1
31	Abuso de privilegios de acceso	1	1	0	1	2	1	1	1	1	1	1	1	1	1	1	2	2	2	2	1	2	1	2	2	3	3	2
32	Manipulación de equipos	2	1	1	1	2	1	1	1	1	1	1	1	2	2	1	2	2	2	3	1	2	1	2	2	3	3	1
33	Manipulación de configuración	1	1	1	1	2	1	1	1	1	1	1	1	2	2	1	2	2	2	2	1	2	1	2	2	3	3	2
34	Alteración de la información	1	1	1	1	2	1	1	1	1	1	1	1	2	2	1	2	2	2	3	1	2	1	2	2	3	3	2

Nota. Evaluación de la matriz de impacto. Fuente: (Amutio, Candau, & Mañas, 2012).

Fase 6: Tratar el riesgo

Para tratar el riesgo se tienen 4 elementos: Transferir, Eliminar, Asumir y Mitigar. Para organizar los activos se tomó como guía al CIS (Critical Security Controls), CIS es una organización con el objetivo de desarrollar buenos ejemplos de soluciones en la ciberseguridad. Se desarrollaron los primeros 6 controles, en una columna se definió que va a realizar el control.

Figura 15

Controles CIS

CONTROLES	
CIS Control 1: Inventario de Dispositivos autorizados y no autorizados	Gestione activamente todo dispositivo hardware en la red (inventario, seguimiento y corrección), de tal manera que solo los dispositivos autorizados obtengan acceso y que los dispositivos no autorizados y no gestionados sean detectados y se prevenga que obtengan acceso.
CIS Control 2: Inventario de Software autorizados y no autorizados	Gestione activamente todo software en la red (inventario, seguimiento y corrección), de tal manera que solo software autorizado esté instalado y pueda ejecutarse, y que el software no autorizado y no gestionado sea encontrado y se prevenga su instalación y ejecución.
CIS Control 3: Gestión continua de vulnerabilidades	Adquirir, evaluar y tomar medidas continuamente sobre nueva información para identificar vulnerabilidades, remediar y minimizar la ventana de oportunidad para los atacantes.
CIS Control 4: Uso controlado de privilegios administrativos	Los procesos y herramientas utilizados para rastrear, controlar, prevenir y corregir el uso, la asignación y la configuración de privilegios administrativos en computadoras, redes y aplicaciones.
CIS Control 5: Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores	Establezca, implemente y gestione activamente (rastree, informe, corrija) la configuración de seguridad de dispositivos móviles, computadoras portátiles, servidores y estaciones de trabajo utilizando una rigurosa gestión de configuraciones y un proceso de control de cambios para evitar que los atacantes exploten servicios y configuraciones vulnerables.
CIS Control 6: Mantenimiento, monitoreo y análisis de logs de auditoría	Reúna, administre y analice registros de auditoría de eventos que podrían ayudar a detectar, comprender o recuperarse de un ataque

Controles CIS

CIS Control 1: Inventario de dispositivos autorizados y no autorizados

a. CIS control 1

Sub-Control	Activo	Tipo de Activo	Función de Seguridad	Control	Descripción	Clasificación
1,1	Computadoras de Escritorio (10)	Equipos	Proteger	Utilizar sistema de loggin del Sistema Operativo	Utilizar sistema de loggin que posee el Sistema Operativo, como PIN y contraseña con su respectivo estandar de seguridad	Mitigar
1,2	Discos Duros	Equipos	Responder	Gestionar activos no autorizados	Asegurar que activos daniños se procesen a cuarentena o se elimen directamente	Mitigar
1,3	VozIP	Equipos	Identificar	Mantener el control de acceso y configuración	Asegurar que la configuración de equipos tenga la información completa, como el usuario, dirección ip, departamento, etc. Así como el uso correcto del equipo	Mitigar
1,4	Router AP	Equipos	Identificar	Utilizar DHCP Logging para tener el registro del ingreso al router	Utilizar el sistema de Loggin de DHCP para tener el registro de los ingresos al router.	Mitigar
1,5	Discos Duros Externos	Equipos	Responder	Mantener el control de acceso y configuración	Asegurar que activos daniños se procesen a cuarentena o se elimen directamente	Mitigar
1,6	Documentos Ordinarios	Equipos	Proteger	Gestionar respaldos	Asegurar de tener respaldos para sustento por cualquier modificación, daño o robo. (Mejorar control de acceso por hardware, software y a traves de politicas)	Mitigar

CIS Control 2: Inventario de Software autorizados y no autorizados

b. CIS control 2

Sub-Control	Activo	Tipo de Activo	Función de Seguridad	Control	Descripción	Clasificación
2,1	Apache	Aplicaciones	Identificar	Utilizar Mod_Security	Utilizar Mod_Security que actua como firewall, monitorea el tráfico en tiempo real y ayuda contra ataques de fuerza bruta	Mitigar
2,2	Office	Aplicaciones	Responder	Utilizar aplicativo con licenciamiento original	Utilizar aplicativo con licenciamiento original, para que no se cree brechas de seguridad al parchar el aplicativo (Siempre tener parchado)	Mitigar
2,3	Windows	Aplicaciones	Proteger	Utilizar sistema de loggin del Sistema Operativo	Utilizar sistema de loggin que posee el Sistema Operativo, como PIN y contraseña con su respectivo estandar de seguridad	Mitigar
2,4	Almacenamiento en Red	Aplicaciones	Responder	Mantener el control de acceso y configuración	Asegurar que activos daniños se procesen a cuarentena o se elimen directamente	Mitigar
2,6	Internet	Aplicaciones	Proteger	Utilizar lista blanca de paginas	Utilizar lista blanca de paginas que pueden acceder los usuarios	Mitigar

CIS Control 3: Gestión continua de vulnerabilidades

c. CIS control 3

Sub-Control	Activo	Tipo de Activo	Función de Seguridad	Control	Descripción	Clasificación
3,1	Apache	Aplicaciones	Detectar	Utilizar Mod_Evasive	Utilizar Mod_Evasive que detecta varias peticiones de paginas o direcciones IP, deteniendo la petición y bloqueandola	Mitigar
3,2	Office	Aplicaciones	Proteger	Administración Vulnerabilidad Microsoft 365	Asegurarse de que el agente de seguridad de Microsoft 365 se encuentre instalado ya que usa software para ataques informaticos	Transferir
3,3	Windows	Aplicaciones	Proteger	Implementar herramientas de gestión automatizada de parches	Implementar herramamientas, asegurarse de que actualizaciones automaticas se encuentren activas para que cuenten con las ultimas actualizaciones de seguridad provistas por el Sistema Operativo	Mitigar
3,4	Almacenamiento en Red	Aplicaciones	Detectar	Realizar análisis de vulnerabilidad autenticados	Realizar escaneos de vulnerabilidad con agentes que se ejecutan localmente en cada sistema o con escaneres remotos	Mitigar
3,6	Internet	Aplicaciones	Detectar	Realizar análisis de vulnerabilidad	Realizar escaneos de vulnerabilidad con agentes que se ejecutan localmente, controlar o con escaneres remotos	Mitigar

CIS Control 4: Uso controlado de privilegios administrativos

d. CIS control 4

Sub-Control	Activo	Tipo de Activ	Función de Seguridad	Control	Descripción	Clasificación
4,1	Computadoras de Escritorio (10)	Equipos	Proteger	Asegurar el uso de cuenta administrativa	Asegurarse que las cuentas administrativas sean las unicas para cambiar configuraciones con respecto al	Mitigar
4,2	Discos Duros	Equipos	Proteger	Herramienta Bitlocker	Implementar la herramienta Bitlocker para que se pueda acceder a la información personas con autorización	Mitigar
4,3	VozIP	Equipos	Identificar	Registrar y alertar cambios de miembros en grupos administrativos	Configure los sistemas para que generen una entrada de registro y una alerta cuando se agregue o elimine una cuenta a cualquier grupo que tenga asignados privilegios administrativos.	Mitigar
4,4	Router AP	Equipos	Proteger	Cambiar contraseñas por defecto	Cambiar contraseñas, nombres y configuración antes de implementar el	Mitigar
4,5	Discos Duros Externos	Equipos	Responder	Usar metodo de autenticación	Usar herramienta de contraseña para el visualizar la información y la instalación de programas	Mitigar
4,6	Documentos Ordinarios	Equipos	Proteger	Limitar el acceso a los documentos	Limitar el acceso al personal a documentos que no tienen autorización	Mitigar
4,11	Apache	Aplicaciones	Detectar	Registrar y alertar los inicios de sesión fallidos	Configurar para que el ingreso fallido se guarde en los registros, para determinar y bloquear dispositivos	Mitigar
4,12	Office	Aplicaciones	Proteger	Uso de cuentas administrativas	Usar la administración que ofrece Microsoft 365 para la configuración de las cuentas y creación de reglas para menorar los riesgos en ataques informaticos	Transefir
4,13	Windows	Aplicaciones	Detectar	Mantener inventario de las cuentas de los usuarios	Usar herramientas administrativas en el dominio, para tener un ingreso controlado con los usuarios respectos al uso de los	Mitigar
4,14	Almacenamiento en Red	Aplicaciones	Proteger	Perfiles de seguridad	Asegurarse que perfiles de seguridad esten creados para que dispositivos seleccionados accedan a la información	Mitigar
4,16	Internet	Aplicaciones	Proteger	Perfiles de seguridad	Asegurarse del perfil de seguridad para el acceso al internet, limitar el uso de paginas inncesarias	Mitigar

CIS Control 5: Configuración segura para hardware y software en dispositivos móviles, computadoras portátiles, estaciones de trabajo y servidores

e. CIS control 5

Sub-Control	Activo	Tipo de Activo	Función de Segurida	Control	Descripción	Clasificación
5,1	Computadoras de Escritorio (10)	Equipos	Proteger	Establecer configuraciones seguras	Mantener estandares de configuración de se guridad, documentados para todos los sistemas operativos y software	Mitigar

CIS Control 6: Mantenimiento, monitoreo y análisis de logs de auditoría.

f. CIS control 6

Sub-Control	Activo	Tipo de Activo	Función de Seguridad	Control	Descripción	Clasificación
6,1	Computadoras de Escritorio (10)	Equipos	Identificar	Activación de LOGS	Activar el registro de actividades o cualquier configuración que nos de logs	Mitigar
6,2	Discos Duros	Equipos	Identificar	Activación de LOGS	Activar el registro de actividades o cualquier configuración que nos de logs	Mitigar
6,3	VozIP	Equipos	Identificar	Activación de LOGS	Activar el registro de actividades o cualquier configuración que nos de logs	Mitigar
6,4	Router AP	Equipos	Identificar	Activación de LOGS	Activar el registro de actividades o cualquier configuración que nos de logs	Mitigar
6,5	Discos Duros Externos	Equipos	Identificar	Activación de LOGS	Activar el registro de actividades o cualquier configuración que nos de logs	Mitigar
6,6	Documentos Ordinarios	Equipos	Identificar	Activación de LOGS	Activar el registro de actividades o cualquier configuración que nos de logs	Mitigar
6,7	Apache	Aplicaciones	Identificar	Activación de LOGS	Activar el registro de actividades o cualquier configuración que nos de logs	Mitigar
6,8	Office	Aplicaciones	Identificar	Activación de LOGS	Activar el registro de actividades o cualquier configuración que nos de logs	Mitigar
6,9	Windows	Aplicaciones	Identificar	Activación de LOGS	Activar el registro de actividades o cualquier configuración que nos de logs	Mitigar
6,10	Almacenamiento en Red	Aplicaciones	Identificar	Activación de LOGS	Activar el registro de actividades o cualquier configuración que nos de logs	Mitigar
6,11	Internet	Aplicaciones	Identificar	Activación de LOGS	Activar el registro de actividades o cualquier configuración que nos de logs	Mitigar

Nota. Tratar el riesgo con controles CIS. Fuente: (CIS, 2018)

CAPÍTULO IV

PLAN DE RECUPERACIÓN DE DESASTRES

Realizar una evaluación de riesgos

Una amenaza es cualquier elemento que, por su impacto y nivel de incidencia, pueda comprometer la seguridad del departamento de TIC de la FAEBMS, así como su continuidad o sostenibilidad, las amenazas que se tomaran en cuenta para el plan de recuperación de desastres son las siguientes:

- Fuego.
- Daños por agua.
- Desastres naturales.
- Corte del suministro eléctrico.
- Condiciones inadecuadas de temperatura o humedad.
- Fallo de servicios de comunicaciones.
- Desastres industriales.
- Fuga de información.
- Introducción de falsa información.
- Acceso no autorizado.
- Vulnerabilidad de programas (software).
- Corrupción de la información.
- Destrucción de información.
- Interceptación de información (escucha).
- Indisponibilidad del personal.
- Agotamiento de recursos.
- Errores de los usuarios.

- Errores del administrador.
- Errores de configuración.
- Degradación de los soportes de almacenamiento de la información.
- Difusión de software dañino.
- Errores de mantenimiento / actualización de programas (software).
- Errores de mantenimiento / actualización de equipos (hardware).
- Caída del sistema por sobrecarga.
- Denegación de servicio.
- Robo.
- Ataques destructivos.
- Extorsión.
- Ingeniería social.
- Manipulación de logs.
- Abuso de privilegios de acceso.
- Manipulación de equipos.
- Manipulación de configuración.
- Alteración de la información.

Mediante un mapa de calor de riesgos se pueden apreciar los activos más vulnerables a las amenazas, por ende, se decidió elaborar un plan de contingencia y recuperación de desastres con los activos que están en nivel crítico, identificador por los colores rojo y naranja.

Figura 16

Matriz de riesgos

Nota. Mapa de calor del impacto de los riesgos. Fuente: (Amutio, Candau, & Mañas, 2012).

Realizar un análisis de impacto al negocio (BIA) y desarrollar estrategias de recuperación y continuidad del negocio.

En el análisis del impacto se tiene dos componentes claves, el RTO y RPO. El RTO es el tiempo que tolera la institución sobre la pérdida de información y el desastre, el valor es el estado operacional del servicio. El RPO es el tiempo que transcurre desde la interrupción y recuperación de los servicios (Alexander, 2015).

Figura 17

Matriz de recuperación de desastres

ACTIVO	VULNERABILIDAD	RTO	RPO	RECOMENDACIÓN	Area Responsable
Internet	No hay un cifrado o esté es inseguro en las comunicaciones que realizan los dispositivos con la nube, el servidor o el usuario	2 horas	1 hora	Es recomendable que la información que contenga o reciba el dispositivo esté cifrada para evitar el robo, la manipulación o la modificación de las acciones a realizar.	Redes
Office	Programas de Office que no cuenta con licenciamiento, se puede dar el caso de que no reciban las últimas actualizaciones de seguridad. Esto podría dejar expuesto el equipo como tal y las más recientes vulnerabilidades descubiertas.	1 hora	1 hora	Al tener licenciamiento las actualizaciones de seguridad son automaticas, se tiene un mayor respaldo ante ataques informaticos.	Soporte Técnico
Apache	Código que se ejecuta en procesos o subprocesos secundarios con pocos privilegios podría permitir a un atacante ejecutar código arbitrario con los privilegios de root manipulando el marcador.	2 horas	1 hora	Tener actualizado la versión de apache que ya corrige este error e igual el acceso a este recurso ser limitidado y controlado	Redes
Windows	No hay un cifrado o esté es inseguro en las comunicaciones que realizan los dispositivos con la nube, el servidor o el usuario	1 hora	1 hora	Es recomendable que la información que contenga o reciba el dispositivo esté cifrada para evitar el robo, la manipulación o la modificación de las acciones a realizar.	Soporte Técnico
Computadoras de Escritorio(10)	Una vulnerabilidad que no se controla es el uso de dispositivos de almacenamiento por los usuarios(USB, Discos Externos, etc). Los dispositivos al conectarse en otros lugares pueden tener virus	1 hora	1 día	Se debe dar limitaciones para el uso de dispositivos de almacenamiento(USB, Discos Externos, etc). Usar almacenamiento en la nube	Soporte Técnico
Discos Duros	No hay un cifrado o esté es inseguro por lo que cualquier persona puede ver la información que contiene el disco sin autorización	1 hora	1 día	Una opción es usar bitlocker, el cifrado ayuda a proteger los datos en tu dispositivo para que solo puedan acceder a ellos personas con autorización	Seguridad de la Información
VoIP	Pérdida de privacidad. La mayor parte del tráfico de VoIP no está cifrado, lo que facilita a que intrusos escuchen sus conversaciones de VoIP.	1 día	1 día	Activar las funciones de autenticación y cifrado que se encuentran disponibles con el sistema de VoIP. Esto mantendrá a las personas no autorizadas sin acceso a la red y protegerá la privacidad de las llamadas	RadioComunicaciones
Routers AP	Al conectarse la red la contraseña usualmente es guardada por todos los dispositivos conectados. Si un trabajador deja la organización, o si se pierde o roba un dispositivo Wi-Fi, pueden hacer uso de la conexión que se tiene a la red	1 dia	1 hora	Cambiar periodicamente la contraseña con estandares recomendados.	Redes/Soporte Técnico
Discos Duros Externos	Una vulnerabilidad que no se controla es el uso de dispositivos de almacenamiento por los usuarios(USB, Discos Externos, etc). Los dispositivos al conectarse en otros lugares pueden tener virus	3 días	3 horas	Se debe dar limitaciones para el uso de dispositivos de almacenamiento(USB, Discos Externos, etc). Usar almacenamiento en la nube	Seguridad de la Información
Almacenamiento en Red	No se tiene perfiles de seguridad por lo que la información puede ser copiada, transmitida, visualizada, robada, destruida, alterada o se puede usar de forma no autorizada	1 día	1 día	Limitar el acceso a los documentos, crear prefiles de seguridad	Seguridad de la Información
Documentos Ordinarios	La información puede ser copiada, transmitida, visualizada, robada, destruida, alterada o se puede usar de forma no autorizada	1 día	1 día	Limitar el acceso a los documentos, crear prefiles de seguridad	Seguridad de la Información

Nota. Análisis de impacto y estrategias de recuperación. Adaptado de INCIBE Instituto Nacional de Ciberseguridad, 2017, (https://normas-apa.org/wp-content/uploads/Guia-Normas-APA-7ma-edicion.pdf).

Concientizar, capacitar y probar los planes

Es importante proveer la información necesaria a todo el personal, el cual está encargado por el Capt. Téc. Avc. Diego Valencia, ya que así estarían capacitados para resolver cualquier problema que se presente en situaciones imprevistas.

Mantener y mejorar el plan de recuperación ante desastres

Para un mejor desempeño laboral es de vital importancia dar un seguimiento constante al plan de recuperación de desastres para poder verificar si existen nuevas amenazas que puedan poner en riesgo a la institución e implementar posibles mejoras que satisfagan o permitan brindar una solución inmediata.

CAPÍTULO V

ANÁLISIS DE COSTO BENEFICIO

El análisis de costo-beneficio (CBA) es una herramienta para analizar el equilibrio entre los costos y beneficios de un proyecto. ABC se puede aplicar a proyectos públicos y privados (Castro, Rosales, & Rahal, 2008). En este apartado los valores del costo de pérdida no están basados en datos estadísticos o históricos, son valores entregados por el supervisor Sgos. Loachamin Fernando, los cuales se tomaron como referencia para el cuadro de análisis costo beneficio.

Figura 18

Análisis costo beneficio

a. Análisis de retorno sobre la inversión en seguridad (ROSI)

ACTIVO	VULNERABILIDAD	COSTO DE PERDIDA	ROSI	% ROSI
Internet	No hay un cifrado o esté es inseguro en las comunicaciones que realizan los dispositivos con la nube, el servidor o el usuario	50000.00	7	700%
Office	Programas de Office que no cuenta con licenciamiento, se puede dar el caso de que no reciban las últimas actualizaciones de seguridad. Esto podría dejar expuesto el equipo como tal y las más recientes vulnerabilidades descubiertas.	5000.00	3.75	375%
Apache	Código que se ejecuta en procesos o subprocesos secundarios con pocos privilegios podría permitir a un atacante ejecutar código arbitrario con los privilegios de root manipulando el marcador.	15000.00	9.625	963%
Windows	No hay un cifrado o esté es inseguro en las comunicaciones que realizan los dispositivos con la nube, el servidor o el usuario	15000.00	0.425	43%
Computadoras de Escritorio(10)	Una vulnerabilidad que no se controla es el uso de dispositivos de almacenamiento por los usuarios(USB, Discos Externos, etc). Los dispositivos al conectarse en otros lugares pueden tener virus	1000.00	-0.64	-64%
Discos Duros	No hay un cifrado o esté es inseguro por lo que cualquier persona puede ver la información que contiene el disco sin autorización	1000.00	-0.55	-55%
VoIP	Pérdida de privacidad. La mayor parte del tráfico de VoIP no está cifrado, lo que facilita a que intrusos escuchen sus conversaciones de VoIP.	5000.00	7	700%
Routers AP	Al conectarse la red la contraseña usualmente es guardada por todos los dispositivos conectados. Si un trabajador deja la organización, o si se pierde o roba un dispositivo Wi-Fi, pueden hacer uso de la conexión que se tiene a la red	5000.00	1.25	125%
Discos Duros Externos	Una vulnerabilidad que no se controla es el uso de dispositivos de almacenamiento por los usuarios(USB, Discos Externos, etc). Los dispositivos al conectarse en otros lugares pueden tener virus	5000.00	7	700%
Almacenamiento en Red	No se tiene perfiles de seguridad por lo que la información puede ser copiada, transmitida, visualizada, robada, destruida, alterada o se puede usar de forma no autorizada	25000.00	0.830215189	83%
Documentos Ordinarios	La información puede ser copiada, transmitida, visualizada, robada, destruida, alterada o se puede usar de forma no autorizada	3000.00	1.112375533	111%
TOTAL		130000.00	36.80259072	3680%

b. Parámetros para el cálculo ROSI

EXPOSICIÓN DEL RIESGO	% MITIGACIÓN	COSTE DE SOLUCIÓN	SOLUCIÓN
50000.00	80%	5000.00	Dispositivo de seguridad
5000.00	95%	1000.00	Licenciamiento Original
15000.00	85%	1200.00	Dispositivo de seguridad
15000.00	95%	10000.00	Licenciamiento Original
1000.00	90%	2500.00	Software de restauración del sistema
1000.00	90%	2000.00	Software de restauración del sistema
5000.00	80%	500.00	VPN
5000.00	90%	2000.00	Dispositivo de seguridad
5000.00	80%	500.00	Administración Bitlocker
25000.00	99%	13523.00	Servicio nube (3 años de reserva)
3000.00	99%	1406.00	Servicio nube (3 años de reserva)

Nota. Análisis de costo beneficio, mediante el cálculo ROSI.

Como se observa en la figura 18 sección b, se tomaron los valores para el cálculo ROSI, se tomaron los activos con el nivel más alto de riesgo para sugerir una solución con su costo y el porcentaje de mitigación que tiene. Los valores obtenidos del cálculo ROSI son porcentajes elevados, ya que los costos de pérdida superan en gran cantidad a los costos de solución, como resultado se tiene 9 activos con un porcentaje favorable de los 11 en total, evidenciando un beneficio en la mayoría de los activos de información con un nivel de alto riesgo.

CAPÍTULO VI

CONCLUSIONES

1. Al desarrollar el plan de contingencia se determinan los activos de información clasificándolos con un umbral tomando los mayores que 1, de resultado un total de 11 activos; se evidenció que no se tienen establecidos estándares ante riesgos informáticos.
2. La metodología MAGERIT permite realizar un análisis a los activos de información, tomando en cuenta cada fase para establecer controles determinando la acción de transferir, eliminar, asumir o mitigar, logrando reducir en un 65% las amenazas, vulnerabilidades y riesgos informáticos en el departamento de TIC de la FAEBMS.
3. Al desarrollar el plan de recuperación de desastres se sustentó en vulnerabilidades que no están dentro de las amenazas establecidas, reduciendo otros riesgos informáticos con estrategias de recuperación y continuidad del negocio, estableciendo tiempos de RTO y RPO que pueda asumir el departamento de TIC de la FAEBMS.
4. El plan de continuidad del negocio, no solo se enfoca en la parte tecnológica también con la parte administrativa para la recuperación efectiva y coordinada ante amenazas, vulnerabilidades y riesgos informáticos.
5. Dentro del análisis de costo/beneficio se determina que el coste de la solución es menor al coste de la exposición del riesgo, logrando tener un porcentaje del cálculo de ROSI del 3680% en los activos de información, teniendo como resultado que la implementación de las soluciones propuestas son factibles en los 9 de los 11 activos con un nivel de alto riesgo.

RECOMENDACIONES

1. La propuesta del plan de contingencia se debe mantener en constante mejora, actualizando planes, activos y todo lo que conlleva para minimizar efectivamente los riesgos; se debe actualizar al menos una vez por año.
2. Capacitar de manera correcta a todo el personal involucrado en el departamento de TIC de la FAEBMS; si se realiza cambios se deben informar y actualizar para eficazmente realizar los procedimientos recomendados en los activos de información.

LISTA DE REFERENCIAS

Artículo de revista

Alexander, J. (2015). Diseño de un Sistema de Gestión de Seguridad y Privacidad de la Información.

Alvarado-Zabala, J., Pacheco-Guzmán, J., & Martillo-Alchundia, I. (2018). EL ANÁLISIS Y GESTIÓN DE RIESGOS EN GOBIERNOS DE TI DESDE EL ENFOQUE DE LA METODOLOGÍA MAGERIT. CCCSS Contribuciones a las Ciencias Sociales, 1.

Análisis de riesgos. (2017). INCIBE, 7-8.

Casas, J. (2003). La encuesta como técnica de investigación. Elaboración de cuestionarios y tratamiento estadístico de los datos. 527-538.

Jiménez, J. (2018). Seguridad y Privacidad de la Información. Plan de Recuperación de Desastres, 6-7.

L, R. Q., & Castaño, C. (2002). Introducción a la metodología de investigación cualitativa. Revista de Psicodidáctica, 8-9.

Solarte Solarte , F. N., Enriquez Rosero , E. R., & Benavides Ruano, M. d. (diciembre de 2015). Metodología de análisis y evaluación de riesgos aplicados a la seguridad informática y de información bajo la norma ISO/IEC 27001. Revista Tecnológica ESPOL-RTE, 28(5), 507. Recuperado el 11 de noviembre de 2020, de http://www.rte.espol.edu.ec/index.php/tecnologica/article/view/456

Libro

Amutio, M., Candau, J., & Mañas, J. (2012). : MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid: Ministerio de Hacienda y Administraciones Públicas.

Castillo Reina, S., Cardenas Prado, J., Quezada Ancajima, J., Roncal Mejia, M., & Villanueva León, M. (2013). "Mapa de riesgos de la financiera Edyficar" Trujillo-La Libertad. Perú, Trujillo, Perú: Universidad Privada Antenor Orrego. Recuperado el 13 de marzo de 2021, de https://es.scribd.com/document/265576097/mapaderiesgosedyficar-131021144345-phpapp02

Castro, R., Rosales, R., & Rahal, A. (2008). Metodologías de preparación y evaluación de proyectos de inversión pública. Bogotá: C. Facultad de Economía.

Viteri Silva, C. F. (2015). Evaluación de riesgos tecnológicos del centro de datos de la universidad Nacional de Chimborazo usando los procesos de TI basados en Coby y MAGERIT. Sangolqui, Pichincha, Ecuador: ESPE. Recuperado el 14 de abril de 2021, de https://repositorio.espe.edu.ec/bitstream/21000/10826/4/T-ESPE-049506.pdf

Página web

Amutio, M., Candau, J., & Mañas, J. (2012). : MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Madrid: Ministerio de Hacienda y Administraciones Públicas.

CIS. (2018). Obtenido de Center for Internet Security: https://www.cert.gov.py/application/files/7415/3625/3112/CIS_Controls_Version_7_Spanish_Translation.pdf