UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

Tema:

PLAN DE CONTINGENCIA INFORMÁTICO BASADO EN LA NORMA ISO 24762:2008 PARA EL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE LA MUNICIPALIDAD DE AMBATO

Trabajo de Titulación Modalidad: Proyecto de Investigación, presentado previo a la obtención del título de Ingeniera en Sistemas Computacionales e Informáticos

ÁREA: Administrativas informáticas

LÍNEA DE INVESTIGACIÓN: Administración de recursos

AUTOR: Adriana Cristina Nuñez Santamaría

TUTOR: Ing. Julio Balarezo, PhD

Ambato - Ecuador

marzo – 2022

APROBACIÓN DEL TUTOR

En calidad de tutor del Trabajo de Titulación con el tema: PLAN DE CONTINGENCIA INFORMÁTICO BASADO EN LA NORMA ISO 24762:2008 PARA EL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE LA MUNICIPALIDAD DE AMBATO, desarrollado bajo la modalidad Proyecto de Investigación por la señorita Núñez Santamaría Adriana Cristina, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, me permito indicar que la estudiante ha sido tutorada durante todo el desarrollo del trabajo hasta su conclusión, de acuerdo a lo dispuesto en el Artículo 15 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y el numeral 7.4 del respectivo instructivo.

Ambato, marzo 2022.

Firmado electrónicamente por:
JULIO ENRIQUE BALAREZO LOPEZ

Ing. Julio Balarezo, PhD.

TUTOR

AUTORÍA

El presente Proyecto de Investigación titulado: PLAN DE CONTINGENCIA INFORMÁTICO BASADO EN LA NORMA ISO 24762:2008 PARA EL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE LA MUNICIPALIDAD DE AMBATO, es absolutamente original, auténtico y personal. En tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, marzo 2022.

Adriana Cristina Nuñez Santamaría

C.C 1804576013

AUTOR

APROBACIÓN TRIBUNAL DE GRADO

En calidad de par calificador del Informe Final del Trabajo de Titulación presentado por la señorita Adriana Cristina Nuñez Santamaría, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, bajo la Modalidad Proyecto de Investigación, titulado PLAN DE CONTINGENCIA INFORMÁTICO BASADO EN LA NORMA ISO 24762:2008 PARA EL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO DE LA MUNICIPALIDAD DE AMBATO, nos permitimos informar que el trabajo ha sido revisado y calificado de acuerdo al Artículo 17 del Reglamento para obtener el Título de Tercer Nivel, de Grado de la Universidad Técnica de Ambato, y al numeral 7.6 del respectivo instructivo. Para cuya constancia suscribimos, conjuntamente con la señora Presidenta del Tribunal.

Ambato, marzo 2022.

Firmado electrónicamente por:
ELSA PILAR URRUTIA

Ing. Pilar Urrutia, Mg.
PRESIDENTA DEL TRIBUNAL

Firmado electrónicamente por:
LEONARDO DAVID TORRES VALVERDE

Ing. Leonardo Torres
PROFESOR CALIFICADOR

Firmado electrónicamente por:
OSCAR FERNANDO IBARRA TORRES

Ing. Fernando Ibarra
PROFESOR CALIFICADOR

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación en favor de la Universidad Técnica de Ambato, con fines de difusión pública. Además, autorizo su reproducción total o parcial dentro de las regulaciones de la institución.

Ambato, marzo 2022.

Adriana Cristina Nuñez Santamaría

C.C 1804576013

AUTOR

DEDICATORIA

El presente proyecto se lo dedico primeramente a Dios, pues es él quien me ha dado la capacidad suficiente para culminar mis estudios superiores.

A mi madre por su constante perseverancia para alcanzar mi objetivo y por cuidarme siempre en cada una de sus oraciones.

A mi padre que me guia y me cuida desde el cielo, por enseñarme principios y valores para ser una buena persona.

A mi esposo por su apoyo incondicional a lo largo de estos años de estudio universitario.

A mi hija quien es mi mayor inspiración para ser mejor cada dia.

A mis amigos de carrera por sus conocimientos y enseñanzas.

Nuñez Santamaría Adriana Cristina

AGRADECIMIENTO

A la Universidad Técnica de Ambato por brindarme la oportunidad de formarme profesionalmente.

A toda mi familia, esposo, hija, madre y hermanas por cada uno de sus consejos para poder culminar mi carrera universitaria.

A mi tutor Ing. Julio Balarezo por compartir sus conocimientos en la elaboración del presente proyecto.

Al personal del departamento de TI del Gobierno Autónomo Descentralizado de la Municipalidad de Ambato, por brindarme información necesaria para culminar el proyecto.

A mis amigos por todos los momentos compartidos a lo largo de mi carrera universitaria.

Nuñez Santamaria Adriana Cristina

ÍNDICE

APROBACIÓN DEL TUTOR ii
AUTORÍA iii
APROBACIÓN TRIBUNAL DE GRADO iv
DERECHOS DE AUTOR v
DEDICATORIA vi
AGRADECIMIENTO vii
CAPITULO 1 1
1.1 Tema de Investigación 1
1.2 Antecedentes Investigativos 1
1.2.1 Contextualización del problema 2
1.2.2 Fundamentación Teórica 3
1.3 Objetivos 6
1.3.1 General 6
1.3.2 Específicos 6
CAPÍTULO 2 8
2.1 Materiales 8
2.1.1 Humanos 8
2.1.2 Institucionales 8
2.1.3 Otros 8
2.2 Métodos 9
2.2.1 Análisis de riesgos mediante la metodología MAGERIT 14
2.2.1.1 Identificación de Activos 15
2.2.1.2 Valoración de Activos 16
2.2.1.3 Identificación de amenazas 23
2.2.1.4 Determinación del Impacto Potencial 31
2.2.1.5 Determinación del Riesgo Potencial 31
2.2.2 Modalidad de la Investigación 32
2.2.3 Recolección de Información 32
2.2.4 Procesamiento y Análisis de Datos 32
2.2.5 Desarrollo del proyecto 33
CAPÍTULO 3 34
3.1 Análisis y discusión de los resultados 34

3.1.1 Desarrollo de la propuesta 34
3.1.2 Planificación 34
3.1.3 Alcance 34
3.1.4 Información Gobierno Autónomo Descentralizado de Ambato 35
3.1.5 Organigrama Estructural del GAD Municipalidad de Ambato 38
3.1.6 Diagnóstico de la situación actual 40
3.1.7 Ubicación geográfica 41
3.1.8 Diseño topológico de la institución 46
3.1.9 Activos informáticos 46
3.1.10 Identificación de activos de información más relevantes 54
3.1.10.1 Servicios 54
3.1.10.2 Activos de Hardware 54
3.1.10.3 Activos de Software 55
3.1.10.4 Datos/ Información 56
3.1.10.5 Activo de Redes de Comunicación 57
3.1.11 Análisis de Riesgo con la metodología MAGERIT 57
3.1.11.1 Valoración de activos 57
3.1.11.2 Impacto de las amenazas sobre los activos 59
3.1.11.3 Matriz de Análisis de Riesgos 81
3.1.12 Cláusulas de la norma ISO 24762:2008 102
3.1.13 Categorización de riesgos y aplicabilidad de la norma ISO 24762:2008 .. 107
3.2 Diseño del Plan de Contingencia Informático 141
CAPÍTULO 4 197
4.1 Conclusiones 197
4.2 Recomendaciones 198
Bibliografía 199
ANEXOS 202

ÍNDICE DE TABLAS

Tabla 2.1 Recursos económicos 8
Tabla 2.2 Representación de la norma ISO 27002:2005 e ISO 24762:2008 11
Tabla 2.3 Tipos de activos según MAGERIT 15
Tabla 2.4 Criterios de valoración según MAGERIT 17
Tabla 2.5 Información de carácter personal 17
Tabla 2.6 Obligaciones legales 18
Tabla 2.7 Seguridad 18
Tabla 2.8 Intereses comerciales o económicos 18
Tabla 2.9 Interrupción del servicio 19
Tabla 2.10 Orden público 20
Tabla 2.11 Operaciones 20
Tabla 2.12 Administración y gestión 21
Tabla 2.13 Pérdida de confianza (reputación) 21
Tabla 2.14 Persecución de delitos 22
Tabla 2.15 Tiempo de recuperación del servicio 22
Tabla 2.16 Información clasificada 22
Tabla 2.17 Información clasificada (Unión Europea) 23
Tabla 2.18 Ponderación de Criterios de valoración 23
Tabla 2.19 Amenazas al tipo de activo Hardware [HW] 24
Tabla 2.20 Amenazas al tipo de activo Software [SW] 25
Tabla 2.21 Amenazas al activo Servicios [S] 25
Tabla 2.22 Amenazas al activo Datos [D] 26
Tabla 2.23 Amenazas al activo Redes de Comunicación [COM] 26
Tabla 2.24 Amenazas al activo Soportes de Información [Media] 27
Tabla 2.25 Amenazas al activo Equipamiento Auxiliar [AUX] 28
Tabla 2.26 Amenazas al activo Instalaciones [L] 29
Tabla 2.27 Amenazas al activo Personal [P] 29
Tablas 2.28 Degradación del valor del activo 30
Tabla 2.29 Probabilidad de ocurrencia 30
Tabla 2.30 Riesgo en función del impacto y la probabilidad 31
Tabla 3.1 Principios Institucionales 35

Tabla 3.2 Valores institucionales 36
Tabla 3.3 Análisis FODA de departamento de TI 41
Tabla 3.4 Eventos catastróficos 42
Tabla 3.5 Principales servicios de GAD Municipalidad de Ambato 48
Tabla 3.6 Servicios 54
Tabla 3.7 Activos de Hardware 55
Tabla 3.8 Activos de Software 55
Tabla 3.9 Activos de Información 56
Tabla 3.10 Activo de Redes de Comunicación 57
Tabla 3.11 Valoración de activos 57
Tabla 3.12 Impacto en Servicios 60
Tabla 3.13 Impacto en activos Software 64
Tabla 3.14 Impacto en activos Hardware 74
Tabla 3.15 Impacto en activos Datos 80
Tabla 3.16 Impacto en activo Redes de Comunicación 81
Tabla 3.17 Riesgo en Servicios 82
Tabla 3.18 Riesgos en Software 86
Tabla 3.20 Riesgos en Hardware 95
Tabla 3.21 Riesgo en Datos 101
Tabla 3.22 Riesgos en Redes de Comunicación 102
Tabla 3.23 Cláusulas de la norma ISO 24762:2008 102
Tabla 3.24 Categorización de riesgos y aplicabilidad de la norma ISO 24762:2008 107

ÍNDICE DE FIGURAS

1Figura 2.1 Elementos del análisis del riesgo potencial 14
2Figura 3.1 Organigrama estructura del GADMA 39
3Figura 3.2 Afectación por inundación Ambato-2015 43
4Figura 3.3 Amenazas por movimiento de masa 44
5Figura 3.4 Ubicación geográfica del GADMA 45
6Figura 3.5 Diseño Topológico del GADMA 46

RESUMEN EJECUTIVO

Un plan de contingencia informático para el departamento de TI (Tecnologías de Información) del Gobierno Autónomo Descentralizado de la Municipalidad de Ambato pretende identificar los riesgos, ya sean de origen natural o humano que puedan ocurrir y causen algún perjuicio a los activos más importantes, por medio de este, se podrá disminuir o mitigar los riesgos y de esta manera poder proteger la información para garantizar su confidencialidad, integridad y disponibilidad, para el normal funcionamiento de las actividades que brinda la institución a toda la ciudadanía.

El departamento de TI es el encargado de administrar y gestionar de la mejor manera la información y servicios de la institución, la cual puede estar expuesta a amenazas que perjudiquen su confidencialidad, integridad y disponibilidad, interrumpiendo de forma parcial o total las operaciones de la institución, por tal motivo se debe contar con un plan de contingencia informático actualizado para disminuir las eventualidades informáticas que se puedan presentar, para que la institución siga operando.

El presente proyecto de investigación plantea el Diseño de un Plan de Contingencia Informático basado en la norma ISO 24762:2008, que describe las directrices ante desastres de Tecnología de Información y Comunicaciones. El plan describirá que acciones tomar ante un evento catastrófico que afecte la continuidad de las actividades de la institución, reduciendo el impacto por medidas de mitigación antes, durante y después ante la materialización de las amenazas, y así prevenir la pérdida de información valiosa para la institución.

PALABRAS CLAVE: Confidencialidad, integridad, disponibilidad, amenazas, activos informáticos, riesgo, plan de contingencia informático, servicios, ISO 24762

ABSTRACT

A computer contingency plan for the IT department (Information Technologies) of the Autonomous Decentralized Government of the Municipality of Ambato aims to identify risks, whether of natural or human origin that may occur and cause damage to the most important assets, for By means of this, the risks may be reduced or mitigated and in this way to be able to protect the information to guarantee its confidentiality, integrity and availability, for the normal functioning of the activities that the institution offers to all citizens.

The IT department is in charge of administering and managing in the best way the information and services of the institution, which may be exposed to threats that harm its confidentiality, integrity and availability, partially or totally interrupting the operations of the institution. For this reason, an updated IT contingency plan must be in place to reduce any IT eventualities that may arise, so that the institution continues to operate.

This research project proposes the Design of a Computer Contingency Plan based on the ISO 24762: 2008 standard, which describes the guidelines for Information and Communications Technology disasters. The plan will describe what actions to take in the event of a catastrophic event that affects the continuity of the institution's activities, reducing the impact of mitigation measures before, during and after the materialization of threats, and thus prevent the loss of valuable information for the institution. institution.

KEYWORDS: Confidentiality, integrity, availability, threats, IT assets, risk, IT contingency plan, services, ISO 24762

CAPITULO 1

MARCO TEÓRICO

1.1 Tema de Investigación

Plan de contingencia informático basado en la norma ISO 24762:2008 para el Departamento de Tecnologías de la Información del Gobierno Autónomo Descentralizado de la Municipalidad de Ambato.

1.2 Antecedentes Investigativos

Como antecedentes se puede mencionar:
Según el proyecto de titulación de los autores Chamba Mera Jhon José y Delgado Álvarez Luis Ignacio titulado "Desarrollo de un plan de recuperación ante desastres (DRP) para la Unidad de T.I. de la Corporación AMCO" [1]**.** El presente proyecto menciona la importancia de identificar correctamente los riesgos, así como su impacto, para el análisis y posterior aplicación de medidas correctivas.

Según el proyecto de titulación de Andrés Fernando Hernández Álvarez, titulado "Elaboración de un Plan de Contingencia para las Tecnologías de Información - Caso de Estudio Banco del Estado" [2]**.** El trabajo menciona la importancia de considerar como prioridad el desarrollo de un plan de contingencia para estar preparados ante cualquier incidente que se pueda presentar y perjudicar los principales procesos.

Según el trabajo de titulación de Lara Santán Romel Delti, titulado "Plan de Contingencia Informático para el conjunto de bodegas Parkenor" [3]**.** El trabajo concluye que mediante el desarrollo de un plan de contingencia permite disminuir el impacto y los efectos de una catástrofe, además identificar oportunamente las áreas vulnerables para evitar accidentes.

Según el trabajo de titulación de Mero Suárez Carlos Renán, titulado "Plan de Contingencias Informáticas y la Seguridad de la Información en el Consejo Nacional

Electoral de la Provincia de Santa Elena" [4]. El trabajo tiene como objetivo fundamental salvaguardar la información, un plan de contingencia permite a la institución el correcto funcionamiento de esta cuando ocurra un accidente interno o externo.

1.2.1 Contextualización del problema

"Para América Latina y el Caribe la convergencia de las tecnologías de la información con la tecnología operativa y los sistemas heredados ya plantea grandes desafíos en todo el ecosistema digital, por un lado, ofrecen inmensas oportunidades de eficiencia e innovación, pero también amplifican la superficie de ataque y pueden crear riesgos de seguridad y privacidad de datos" [5]**.**

"Los despliegues de telecomunicaciones de emergencia de la Unión Internacional de Telecomunicaciones (UIT) son parte del Marco para la Cooperación en Emergencias (IFCE). El cual proporciona servicios de telecomunicaciones para la mitigación de desastres, así como movilización de recursos inmediatamente después de un desastre para asegurar la continuidad de las comunicaciones" [6]**.** Es importante para cualquier organización recuperar la información en un lapso corto de tiempo.

"Comúnmente, se suele asociar los tipos de riesgos tecnológicos solamente con las instalaciones industriales o equipamientos de alta tecnología. No obstante, la experiencia de accidentabilidad en provincias, como es el caso de Pichincha, deja distinguir diversos eventos en el sector residencial y a nivel de obras civiles. Además, otros accidentes muy puntuales vinculados con obras civiles han sido reportados por vulnerabilidades intrínsecas" [7]**.** Las amenazas a la información pueden surgir de diferentes formas tanto de origen natural (terremotos, inundaciones, etc.), de origen humano (competencia, problemas laborales, entre otros), como de origen técnico (fallas del hardware, del software, etc.). Estos tipos de amenazas son conocidos en la temática de seguridad de la información.

"En la ciudad de Ambato el Gobierno Autónomo Descentralizado, es una institución que promueve el desarrollo sostenible del cantón, a través de la prestación de servicios

accesibles, óptimos y oportunos, la implementación de políticas públicas incluyentes, la mejora continua e innovación de sus procesos y servicios, el uso de tecnologías, y el fomento de la participación ciudadana, para mejorar la calidad de vida de sus ciudadanos. Tener un plan de contingencia informático actualizado, ayudará satisfactoriamente a continuar con los distintos servicios que presta dicha institución, en caso de presentarse algún evento catastrófico" [8]**.**

"Los riesgos de la información están presentes cuando coinciden dos elementos: amenazas y vulnerabilidades. Las amenazas y vulnerabilidades están íntimamente ligadas, y no puede haber ninguna consecuencia sin la presencia conjunta de éstas. Las amenazas deben tomar ventaja de las vulnerabilidades y pueden venir de cualquier parte, interna o externa, relacionada con el entorno de las organizaciones" [9]**.**

1.2.2 Fundamentación Teórica

Plan de Contingencia: "Un plan de contingencia permite identificar los riesgos (de origen natural o humano) a sistemas o recursos informáticos, para mantener la continuidad del negocio de la organización recuperando la totalidad de su funcionalidad en el menor tiempo posible, proteger la información es primordial, para garantizar su integridad, confidencialidad y disponibilidad" [10]**.**

Norma ISO: "Organización Internacional de Estandarización es una entidad compuesta por organismos nacionales de normalización, estructurada en comités técnicos que tienen como misión la elaboración de normas internacionales en temas específicos" [11]**.**

Seguridad Informática: "Es la disciplina que se ocupa de diseñar las normas, procedimientos, métodos y técnicas destinados a conseguir un sistema de información seguro y confiable.

Para que un sistema sea considerado como seguro, se debe cumplir con las siguientes propiedades:

- **Integridad:** Garantiza la autenticidad y precisión de la información, sin importar el momento en que esta se solicita

- **Confidencialidad:** Hace relación al hecho de que los datos o la información estén únicamente al alcance del conocimiento de las personas, entidades o mecanismos autorizados, en momentos autorizados y de manera autorizada.
- **Disponibilidad:** Grado en el que un dato está en el lugar, momento y forma en el que es requerido por el usuario autorizado. Situación que se produce cuando se puede acceder a un sistema de información en un periodo de tiempo considerado aceptable. La disponibilidad está asociada a la fiabilidad técnica de los componentes del sistema de información" [12]**.**

"El objetivo primario de la seguridad informática es el de mantener al mínimo los riesgos sobre los recursos informáticos, todos los recursos y garantizar así la continuidad de las operaciones de la organización al tiempo que se administra ese riesgo informático a un cierto costo aceptable" [13].

Políticas de Seguridad: "Recoge las directrices u objetos de una organización con respecto a la seguridad de la información, el contenido depende de las necesidades y la realidad de la organización.
Generalmente se engloba en los siguientes grupos:

1. Identificar las necesidades de seguridad y los riesgos que amenazan al sistema, así como evaluar los impactos ante un eventual ataque.
2. Relacionar todas las medidas de seguridad que deben implantarse para afrontar los riesgos de cada activo o grupo de activos.
3. Proporcionar una perspectiva general de las reglas y los procedimientos que deben aplicarse para afrontar los riesgos identificados en los diferentes departamentos de la organización.
4. Detectar todas las vulnerabilidades del sistema de información y controlar los fallos que se producen en los activos, incluidas las aplicaciones instaladas.
5. Definir un plan de contingencias" [12]**.**

Tecnologías de la Información y Comunicación: "Rama de la tecnología que se dedica al estudio, aplicación y procesamiento de data, lo cual involucra la obtención,

creación, almacenamiento, administración, modificación, manejo, movimiento, control, visualización, distribución, intercambio, transmisión o recepción de información de forma automática, así como el desarrollo y uso de *hardware*, *firmware*, *software*, cualquiera de sus componentes y todos los procedimientos asociados con el procesamiento de data" [14].

Activo: "En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de la misma (sistemas, soportes, edificios, personas...) que tenga valor para la organización" [15].

Amenazas: "Presencia de uno o más factores de diversa índole (personas, maquinas o sucesos), que de tener la oportunidad atacarían al sistema produciendo daños aprovechándose de su nivel de vulnerabilidad.
Las amenazas se clasifican en cuatro grupos:

- De interrupción: El objetivo de la amenaza es deshabilitar el acceso a la información.
- De interceptación: Personas, programas o equipos no autorizados podrían acceder a un determinado recurso del sistema y captar información confidencial de la organización
- De modificación: Personas, programas o equipos no autorizados no solamente accederían a los programas y datos de un sistema de información, sino que además los modificaría.
- De fabricación: Agregarían información falsa en el conjunto de información del sistema.

Según su origen se clasifican:

- Accidentales: Accidentes meteorológicos, incendios, inundaciones, fallos en los equipos, en las redes, en los sistemas operativos, errores humanos.
- Intencionadas: Son debidas siempre a la acción humana, como la introducción de software malicioso, malware, intrusión informática, robos o hurtos, estas amenazas pueden tener su origen en el exterior de la organización o incluso en el personal de la misma" [16].

Vulnerabilidad: "Constituye un hecho o una actividad que permite concretar una amenaza. Se es vulnerable en la medida en que no hay suficiente protección como para evitar que llegue a suceder una amenaza.

- **Ataques no intencionados:** Cuando un hecho perjudica a la información, a la TI o a la empresa sin que ocurra por las acciones intencionadas de alguien. Por ejemplo, un incendio accidental, una inundación debida al mal tiempo, la falla de suministro de energía eléctrica por la caída de un rayo, una falla en un satélite de comunicación, errores y equivocaciones de usuarios, entre muchos más.
- **Ataques intencionados:** Los ataques lógicos a los sistemas de información vienen del exterior de la empresa, otros pueden provenir del interior de la propia empresa, estos son causados por empleados descontentos, ingenuos o conocimiento insuficiente, ya que, sobre estos, se aplica la ingeniería social" [17]**.**

Riesgo: El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización [15].

1.3 Objetivos

1.3.1 General

Diseñar un plan de contingencia informático basado en la norma ISO 24762:2008 para el Departamento de Tecnologías de la Información del Gobierno Autónomo Descentralizado de la Municipalidad de Ambato.

1.3.2 Específicos

- Analizar la información respectiva del Data Center del departamento de Tecnologías de la Información del GAD de Ambato.

- Identificar los posibles riesgos de origen natural o humano que se pueden presentar en el departamento de Tecnologías de la Información del GAD de Ambato.
- Investigar la norma ISO 24762:2008 y proponer un plan de contingencia informático de acuerdo a la evaluación realizada en la institución.

CAPÍTULO 2

METODOLOGÍA

2.1 Materiales

2.1.1 Humanos

- Docente Tutor del Proyecto
- Tutor del GAD de la Municipalidad de Ambato.
- Autor del Proyecto.

2.1.2 Institucionales

- Repositorio Institucional.
- Biblioteca Digital.
- GAD de la Municipalidad de Ambato.

2.1.3 Otros

En el proyecto de investigación el encargado del financiamiento en su totalidad será del investigador. En la siguiente tabla se detalla el presupuesto:

Tabla 2.1 Recursos económicos

No.	Detalle	Unidad	Cantidad	Valor Unitario	Valor Total
1	Internet	Horas	200	$0.80	160
2	Resma de papel boom	c/u	1	$5.00	5.00
3	Carpetas	c/u	3	$1.00	3.00
4	Impresiones	c/u	200	$0.05	10.00

5	Medios de almacenamiento	c/u	2	$10.00	20.00
6	Computador	c/u	1	$800	800
7	Esferos	c/u	3	$0.60	1.80
8	Lápices	c/u	3	$0.60	1.80
9	Borrador	c/u	1	$0.35	0.35
10	Cuaderno	c/u	1	$1.50	1.50
11	Transporte	Semanal	25	$5	125
				Subtotal	1128.45
				Imprevistos (10%)	112.845
				Total	1241.295

Fuente: Elaborado por el investigador

2.2 Métodos

El presente trabajo de investigación se centra en el diseño de un plan de contingencia informático, ya que con el mismo se podría mitigar los riesgos que se presentan de manera interna o externa, para ello utilizaremos las siguientes metodologías:

Método Delphi

"El método Delphi es muy adecuado para aquellos problemas en donde la mejor información disponible es la opinión de los expertos en la materia. Además, debido a su flexibilidad, que mejor se adapta a la exploración de elementos que supongan una mezcla de evidencia científica y valores sociales. Pretende obtener una visión colectiva de expertos sobre un tema a partir de rondas repetidas de preguntas, siendo un método capaz de obtener y depurar los juicios de grupo. La operativa del método Delphi consiste en el envío de encuestas sucesivas a un grupo de expertos previamente elegidos" [18].

Metodología MAGERI

"MAGERIT es la metodología de análisis y gestión de riesgos elaborada por el antiguo Consejo Superior de Administración Electrónica (actualmente Comisión de Estrategia TIC), como respuesta a la percepción de que la Administración, y, en general, toda la sociedad, dependen de forma creciente de las tecnologías de la información para el cumplimiento de su misión. La razón de ser de MAGERIT está directamente relacionada con la generalización del uso de las tecnologías de la información, que supone unos beneficios evidentes para los ciudadanos; pero también da lugar a ciertos riesgos que deben minimizarse con medidas de seguridad que generen confianza" [19].

ISO / IEC 24762: 2008

"Proporciona directrices sobre la provisión de servicios de recuperación de desastres de tecnología de la información y las comunicaciones (DR de TIC) como parte de la gestión de la continuidad del negocio, aplicable a proveedores de servicios de DR de TIC *internos* y *subcontratados* de instalaciones físicas y servicios.
Esta norma internacional especifica:

- Los requisitos para implementar, operar, monitorear y mantener los servicios e instalaciones de recuperación de desastres de TIC.
- Las capacidades que deben poseer los proveedores de servicios de recuperación de desastres de TIC subcontratados y las prácticas que deben seguir, a fin de proporcionar entornos operativos básicos seguros y facilitar los esfuerzos de recuperación de las organizaciones.
- La guía para la selección del sitio de recuperación.
- La guía para que los proveedores de servicios de DR de TIC mejoren continuamente sus servicios de DR de TIC" [20].

Tabla 2.2 Representación de la norma ISO 27002:2005 e ISO 24762:2008

ISO/IEC 24762:2008	ISO/IEC 27002:2005
Cláusula 5 **Recuperación de desastres TIC5**	
5.1 General	
5.2 Estabilidad ambiental	
5.3 Gestión de activos	Controles enumerados en la Cláusula 7 (ASSET GESTIÓN)
5.4 Proximidad del sitio	
5.5 Gestión de proveedores	6.2.3 Abordar la seguridad en acuerdos de terceros Controles enumerados en la Cláusula 8 (Seguridad de Recursos Humanos) 12.1.1 Análisis y especificación de requisitos de seguridad
5.6 Acuerdos de externalización	Controles enumerados en la subcláusula 10.2 (TERCERO GESTIÓN DE ENTREGA DE SERVICIOS)
5.7 Seguridad de la información	10.1.3 Segregación de funciones 13.1.1 Informar de eventos de seguridad de la información
5.8 Activación del plan de recuperación ante desastres	6.1.3 Asignación de responsabilidades de seguridad de la información 14.1.4 Marco de planificación de continuidad del negocio
5.9 Formación y educación	8.2.2 Sensibilización, educación y formación en seguridad de la información
5.10 Pruebas en sistemas TIC	10.1.2 Gestión del cambio 10.3.2 Aceptación del Sistema 10.5.1 Copia de seguridad de la información 14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad del negocio
5.11 Planificación de continuidad del negocio para los proveedores de servicios de ICT DR	Controles enumerados en la Cláusula 14 (Business Gestión De Continuidad)
5.12 Documentación y revisión periódica	
CLÁUSULA 6 **Instalaciones de recuperación ante desastres TIC**	
6.1 General	
6.2 Ubicación del sitio de recuperación	10.5.1 Copia de seguridad de la información

6.3 Controles de acceso físico	9.1.1 Perímetro de seguridad física 9.1.2 Controles de entrada físicos
6.4 Seguridad física de las instalaciones	
6.5 Áreas dedicadas	
6.6 Controles ambientales	
6.7 Telecomunicaciones	9.2.2 Servicios públicos de apoyo 9.2.3 Seguridad de cableado
6.8 Fuente de alimentación	
6.9 Gestión de cables	
6.10 Protección contra incendios	
6.11 Centro de operaciones de emergencia (EOC)	
6.12 Instalaciones restringidas	
6.13 Servicios de no recuperación	
6.14 Instalaciones físicas y ciclo de vida del equipo de apoyo	
6.15 Pruebas	
CLÁUSULA 7 Capacidad del proveedor de servicios externalizados	
7.1 General	
7.2 Revisar el estado de recuperación ante desastres de la organización	(Para organizaciones que van a utilizar servicios profesionales des) Controles enumerados en la Cláusula 14 (BUSINESS GESTIÓN DE CONTINUIDAD)
7.3 Requisitos de instalaciones *(*Nota: Esta expectativa es para los proveedores de servicios en general, y no limitado para los proveedores de servicios profesionales*)*	
7.4 Experiencia	
7.5 Control de acceso lógico	
7.6 Equipos TIC y preparación para operaciones	
7.7 Soporte de recuperación simultáneo	
7.8 Niveles de servicio	(Para organizaciones que utilizan servicios profesionales de DRS) Controles enumerados en la subcláusula 10.2 (TERCERO GESTIÓN DE ENTREGA DE SERVICIOS)
7.9 Tipos de servicio	10.3.1 Gestión de capacidad
7.10 Proximidad de servicios	
7.11 Relación de suscripción para servicios compartidos	15.1.4 Protección de datos y privacidad de la información personal

7.12 Activación de servicios suscritos	14.1.4 Marco de planificación de continuidad del negocio
7.13 Pruebas de la Organización	14.1.5 Pruebas, mantenimiento y reevaluación de planes de continuidad del negocio
7.14 Cambios en la capacidad	12.1.1 Análisis y especificación de requisitos de seguridad 12.5.1 Cambiar los procedimientos de control
7.15 Plan de respuesta a emergencias	13.2.1 Responsabilidades y procedimientos Controles enumerados en la Cláusula 14 (Business Gestión De Continuidad)
7.16 Autoevaluación	

Fuente: Elaborador por el investigador en base a [20].

Norma 410-11 de la Contraloría General del Estado del Ecuador

"Corresponde a la Unidad de Tecnología de Información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado.

Los aspectos para considerar son:

1. Plan de respuesta a los riesgos que incluirá la definición y asignación de roles críticos para administrar los riesgos de tecnología de información, escenarios de contingencias, la responsabilidad específica de la seguridad de la información, la seguridad física y su cumplimiento.
2. Definición y ejecución de procedimientos de control de cambios, para asegurar que el plan de continuidad de tecnología de información se mantenga actualizado y refleje de manera permanente los requerimientos actuales de la organización.
3. Plan de continuidad de las operaciones que contemplará la puesta en marcha de un centro de cómputo alterno propio o de uso compartido en un Data Center Estatal, mientras dure la contingencia con el restablecimiento de las comunicaciones y recuperación de la información de los respaldos.
4. Plan de recuperación de desastres que comprenderá:
   - Actividades previas al desastre (bitácora de operaciones).
   - Actividades durante el desastre (plan de emergencias, entrenamiento).

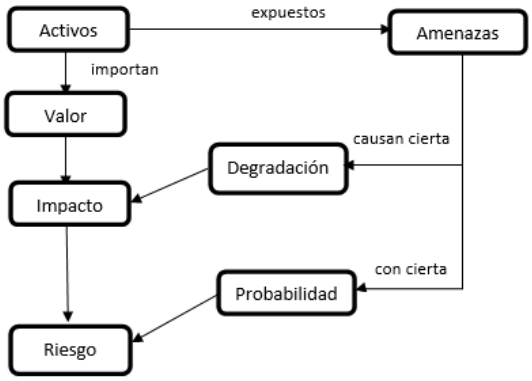
- Actividades después del desastre.

5. Es indispensable designar un comité con roles específicos y nombre de los encargados de ejecutar las funciones de contingencia en caso de suscitarse una emergencia.
6. El plan de contingencias será un documento de carácter confidencial que describa los procedimientos a seguir en caso de una emergencia o fallo computacional que interrumpa la operatividad de los sistemas de información. La aplicación del plan permitirá recuperar la operación de los sistemas en un nivel aceptable, además de salvaguardar la integridad y seguridad de la información.
7. El plan de contingencias aprobado será difundido entre el personal responsable de su ejecución y deberá ser sometido a pruebas, entrenamientos y evaluaciones periódicas, o cuando se haya efectuado algún cambio en la configuración de los equipos o el esquema de procesamiento" [21].

2.2.1 Análisis de riesgos mediante la metodología MAGERIT

La información y servicios que se maneja en la Municipalidad de Ambato es de vital importancia para toda la ciudadanía, por lo que mediante la metodología MAGERIT, juntamente con el personal del departamento de TI se evaluará los riesgos a los que están expuesto los activos principales del departamento de TI.

Figura 2.1 Elementos del análisis del riesgo potencial



Fuente: Elaborado por el investigador, a partir de [22].

Pasos para el Análisis de Riesgos mediante la metodología MAGERIT

1. Determinar los activos relevantes para la Organización, su interrelación y su valor, en el sentido de qué perjuicio supondría su degradación.
2. Determinar a qué amenazas están expuestos aquellos activos.
3. Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.
4. Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.
5. Estimar el riesgo, definido como el impacto [23].

2.2.1.1 Identificación de Activos

En un Sistema de Información hay dos partes fundamentales: la ***información*** que se maneja y los ***servicios*** que prestan. Estos activos principales marcan los requisitos de seguridad para todos los demás componentes del sistema. Dentro de la información que se maneja, puede ser interesante considerar algunas características formales tales como si son de carácter personal, con requisitos legales, o si están sometidos a alguna clasificación de seguridad, con requisitos normativos [23].

En la siguiente tabla se muestra los tipo de activo según MAGERIT

Tabla 2.3 Tipos de activos según MAGERIT

TIPO	NOMBRE
[D]Datos/Información	La información es un activo abstracto, que permite a la organización prestar servicios.
[K]Claves criptográficas	Se emplea para autentificar las partes.
[S]Servicios	Función que satisface las necesidades de los usuarios.
[SW]Software/ Aplicaciones Informáticas	Las aplicaciones gestionan, analizan y transforman los datos para la prestación de servicios.
[HW]Hardware/ Equipamiento Informático	Medios físicos que soportan los servicios de la Organización.
[COM]Redes de Comunicación	Medios de transporte que llevan datos de un sitio a otro

[Media]Soporte de Información	Dispositivos físicos que permiten almacenar información de manera permanente o por largos periodos de tiempo.
[AUX]Equipamiento Auxiliar	Se considera a otros equipos que sirven de soporte a los sistemas de información.
[L]Instalaciones	Sitios donde se hospedan los sistemas de información y comunicaciones
[P]Personal	Personas relacionadas con el sistema de información

Elaborador por: el Investigador en base a [23]

2.2.1.2 Valoración de Activos

Una vez identificados los activos principales del departamento de TI del GAD Municipalidad de Ambato, se procede a la valoración de estos, pues cuanto más valor posee un activo, mayor nivel de protección requeriremos en las dimensiones de seguridad que sean adecuadas. Las dimensiones se utilizan para valorar los efectos de la materialización de una amenaza. La valoración que recibe un activo en una cierta dimensión es la medida del perjuicio para la organización si el activo es afectado en dicha dimensión. Cada uno de los activos tendrá un valor en las dimensiones de confidencialidad, integridad y disponibilidad para garantizar la seguridad de la información.

Confidencialidad: Se refiere al daño que causaría si se pierde la autorización de la información, los activos que obtiene un valor alto en esta dimensión, significan que provocaría daños graves a la organización.
Integridad: Se refiere a que la información no sufra alteraciones, es decir que los registros de las actividades no sufran cambios de manera intencionada o provocada.
Disponibilidad: Se refiere a que un activo debe permanecer trabajando, si en algún momento llegara a no estar disponible, podría causar daños graves a la organización.

Con los criterios de valoración que se describe en las siguientes tablas se podrá asignar un valor más específico a los activos.

Tabla 2.4 Criterios de valoración según MAGERIT

CÓDIGO	DESCRIPCIÓN
pi	Información de carácter personal
lro	Obligaciones legales
si	Seguridad
cei	Intereses comerciales o económicos
da	Interrupción del servicio
po	Orden público
olm	Operaciones
adm	Administración y gestión
lg	Pérdida de confianza (reputación)
crm	Persecución de delitos
tro	Tiempo de recuperación del servicio
lbl.nat	Información clasificada (nacional)
lbl.ue	Información clasificada (Unión Europea)

Fuente: Elaborado por el Investigador

Tabla 2.5 Información de carácter personal

[**pi] información de carácter personal**		
6	6.pi1	Probablemente afecte gravemente a un grupo de individuos
	6.pi2	probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
5	5.pi1	Probablemente afecte gravemente a un individuo
	5.pi2	Probablemente quebrante seriamente leyes o regulaciones
4	4.pi1	Probablemente afecte a un grupo de individuos
	4.pi2	Probablemente quebrante leyes o regulaciones
3	3.pi1	Probablemente afecte a un individuo
	3.pi2	Probablemente suponga el incumplimiento de una ley o regulación
2	2.pi1	Pudiera causar molestias a un individuo
	2.pi2	Pudiera quebrantar de forma leve leyes o regulaciones
1	1.pi1	Pudiera causar molestias a un individuo

Fuente: Libro II de MAGERIT [24]

Tabla 2.6 Obligaciones legales

[lro] Obligaciones legales		
9	9.lro	Probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7	7.lro	Probablemente cause un incumplimiento grave de una ley o regulación
5	5.lro	Probablemente sea causa de incumplimiento de una ley o regulación
3	3.lro	Probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
1	1.lro	Pudiera causar el incumplimiento leve o técnico de una ley o regulación

Fuente: Libro II de MAGERIT [24]

Tabla 2.7 Seguridad

[si] Seguridad		
10	10.si	Probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
9	9.si	Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
7	7.si	Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
3	3.si	Probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
1	1.si	Pudiera causar una merma en la seguridad o dificultar la investigación de un incidente

Fuente: Libro II de MAGERIT [24]

Tabla 2.8 Intereses comerciales o económicos

[cei]Intereses comerciales o económicos		
9	9.cei.a	De enorme interés para la competencia
	9.cei.b	De muy elevado valor comercial
	9.cei.c	Causa de pérdidas económicas excepcionalmente elevadas
	9.cei.d	Causa de muy significativas ganancias o ventajas para individuos u organizaciones

	9.cei.e	Constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
7	7.cei.a	De alto interés para la competencia
	7.cei.b	De elevado valor comercial
	7.cei.d	Proporciona ganancias o ventajas desmedidas a individuos u organizaciones
	7.cei.e	Constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
3	3.cei.a	De cierto interés para la competencia
	3.cei.b	De cierto valor comercial
	3.cei.c	Causa de pérdidas financieras o merma de ingresos
	3.cei.d	Facilita ventajas desproporcionadas a individuos u organizaciones
	3.cei.e	Constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
2	2.cei.a	De bajo interés para la competencia
	2.cei.b	De bajo valor comercial
1	1.cei.a	De pequeño interés para la competencia
	1.cei.b	De pequeño valor comercial
0	0.3	Supondría pérdidas económicas mínimas

Fuente: Libro II de MAGERIT [24]

Tabla 2.9 Interrupción del servicio

[da] Interrupción del servicio		
9	9.da	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
	9.da2	Probablemente tenga un serio impacto en otras organizaciones
7	7.da	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
	7.da2	Probablemente tenga un gran impacto en otras organizaciones

5	5.da	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	5.da2	Probablemente cause un cierto impacto en otras organizaciones
3	3.da	Probablemente cause la interrupción de actividades propias de la Organización
1	1.da	Pudiera causar la interrupción de actividades propias de la Organización

Fuente: Libro II de MAGERIT [24]

Tabla 2.10 Orden público

[po] Orden público		
9	9.pro	Alteración seria del orden publico
6	6.ptro	Probablemente cause manifestaciones, o presiones significativas
3	3pro	Causa de protestas puntuales
1	1.pro	Pudiera causar protestas puntuales

Fuente: Libro II de MAGERIT [24]

Tabla 2.11 Operaciones

[olm] Operaciones		
10	10.olm	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística
9	9.olm	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
7	7.olm	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
5	5.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
3	3.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
1	1.olm	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)

Fuente: Libro II de MAGERIT [24]

Tabla 2.12 Administración y gestión

[adm] Administración y gestión		
9	9.adm	Probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
7	7.adm	Probablemente impediría la operación efectiva de la Organización
5	5.adm	Probablemente impediría la operación efectiva de más de una parte de la Organización
3	3.adm	Probablemente impediría la operación efectiva de una parte de la Organización
1	1.adm	Pudiera impedir la operación efectiva de una parte de la Organización

Fuente: Libro II de MAGERIT [24]

Tabla 2.13 Pérdida de confianza (reputación)

[Ig] Pérdida de confianza (reputación)		
9	9.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
	9.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones con el público en general
7	7.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
	7.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
5	5.lg.a	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones
	5.lg.b	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público
3	3.lg	Probablemente afecte negativamente a las relaciones internas de la Organización
2	2.lg	Probablemente cause una pérdida menor de la confianza dentro de la Organización
1	1.lg	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	0.4	No supondría daño a la reputación o buena imagen de las personas u organizaciones

Fuente: Libro II de MAGERIT [24]

Tabla 2.14 Persecución de delitos

[crm] Persecución de delitos		
8	8.crm	Impida la investigación de delitos graves o facilite su comisión
4	4.crm	Dificulte la investigación o facilite la comisión de delitos

Fuente: Libro II de MAGERIT

Tabla 2.15 Tiempo de recuperación del servicio

[tro] Tiempo de recuperación del servicio		
7	7.rto	RTO < 4 horas
4	4.rto	4 horas < RTO < 1 día
1	1.rto	1 día < RTO < 5 días
0	0.rto	5 días < RTO

Fuente: Libro II de MAGERIT [24]

Tabla 2.16 Información clasificada

[lbl.nat] Información clasificada (nacional)		
10	10.lbl	Secreto
9	9.lbl	Reservado
8	8.lbl	Confidencial
7	7.lbl	Confidencial
6	6.lbl	Difusión limitada
5	5.lbl	Difusión limitada
4	4.lbl	Difusión limitada
3	3.lbl	Difusión limitada
2	2.lbl	Sin clasificar
1	1.lbl	Sin clasificar

Fuente: Libro II de MAGERIT [24]

Tabla 2.17 Información clasificada (Unión Europea)

[lbl.ue] Información clasificada (Unión Europea)		
10	10.ue	TRES SECRET UE
9	9.ue	SECRET UE
8	8.ue	CONFIDENTIEL UE
7	7.ue	CONFIDENTIEL UE
6	6.ue	RESTREINT UE
5	5.ue	RESTREINT UE
4	4.ue	RESTREINT UE
3	3.ue	RESTREINT UE

Fuente: Libro II de MAGERIT [24]

Una vez asignado el valor al activo, se utiliza como guía a la siguiente tabla, con niveles del 0 al 10, donde 0 toma un valor despreciable.

Tabla 2.18 Ponderación de Criterios de valoración

VALOR		**CÓDIGO**	**CRITERIO**
10	Extremo	E	Daño extremadamente grave
9	Muy Alto	MA	Daño muy grave
6-8	Alto	A	Daño grave
3-5	Medio	M	Daño importante
1-2	Bajo	B	Daño menor
0	Despreciable	D	Irrelevante a efectos prácticos

Fuente: Elaborado por el Investigador

2.2.1.3 Identificación de amenazas

Para cada tipo de activo existen ciertas amenazas, para ello, se ha considerado junto con el personal del departamento de TI, analizar mediante una dimensión de seguridad de la información como es la disponibilidad, puesto que si cualquier activo no se encuentra disponible por un lapso podría causar daños graves a la municipalidad.

En las siguientes tablas se detallas las amenazas para cada uno de los activos según la metodología MAGERIT.

Tabla 2.19 Amenazas al tipo de activo Hardware [HW]

TIPO	AMENAZAS
[N]Desastres Naturales	[N.1]Fuego
	[N.2]Daños de Agua
	[N*]Desastres Naturales 03 – CONTAMINACIÓN 04 - SINIESTRO MAYOR 06 - FENÓMENO CLIMÁTICO 07 - FENÓMENO SÍSMICO 08 - FENÓMENO DE ORIGEN VOLCÁNICO 09 - FENÓMENO METEOROLÓGICO 10 – INUNDACIÓN.
[I]De origen Industrial	[I.1]Fuego
	[I2]Daños por agua
	[I.*]Desastres Industriales
	[I.3]Contaminación mecánica
	[I.4]Contaminación electromagnética
	[I.5]Avería de origen físico o lógico
	[I.6]Corte de suministro eléctrico
	[I.7]Condiciones inadecuadas de temperatura o humedad
[E]Errores y fallos no intencionados	[E.2]Errores del administrador
	[E.23]Errores de mantenimiento/actualización de equipos (hardware)
	[E.24]Caída del sistema por agotamiento de recursos
[A]Ataques intencionados	[A.6]Abuso de privilegios de acceso
	[A.7]Uso no previsto
	[A.24]Denegación de servicio
	[A.25]Robo
	[A.26]Ataque destructivo

Fuente: Elaborador por el Investigador

Tabla 2.20 Amenazas al tipo de activo Software [SW]

TIPO	AMENAZA
[I]De origen Industrial	[I.5]Avería de origen físico o lógico
[E]Errores y fallos no intencionados	[E.1]Errores de los usuarios
	[E.2]Errores del administrador
	[E.8]Difusión de software dañino
	[E.18]Destrucción de información
	[E.20]Vulnerabilidades de los programas (software)
	[E.21]Errores de mantenimiento/actualización de programas(software)
[A]Ataques intencionados	[A.6]Abuso de privilegios de acceso [A.7]Uso no previsto
	[A.8]Difusión de software dañino
	[A.18]Destrucción de información
	[A.22]Manipulación de programas

Fuente: Elaborador por el Investigador

Tabla 2.21 Amenazas al activo Servicios [S]

TIPO	AMENAZAS
[E]Errores y fallos no intencionados	[E.1] Errores de los usuarios
	[E.2] Errores del administrador
	[E.18] Destrucción de información
	[E.19] Fugas de información
	[E.24] Caída del sistema por agotamiento de recursos
[A]Ataques intencionados	[A.6] Abuso de privilegios de acceso
	[A.7] Uso no previsto
	[A.18] Destrucción de información
	[A.24] Denegación de servicio

Fuente: Elaborador por el Investigador

Tabla 2.22 Amenazas al activo Datos [D]

TIPO	AMENAZA
[E]Errores y fallos no intencionados	[E.1]Errores de los usuarios
	[E.2]Errores del administrador
	[E.18]Destrucción de información
[A]Ataques intencionados	[A.4]Manipulación de la configuración [D.log]registros de actividad
	[A.6]Abuso de privilegios de acceso
	[A.18]Destrucción de información

Fuente: Elaborador por el Investigador

Tabla 2.23 Amenazas al activo Redes de Comunicación [COM]

TIPO	AMENAZA
[I]De origen industrial	[I.8]Fallo de servicios de comunicaciones
[E]Errores y fallos no intencionados	[E.2]Errores del administrador
	[E.18]Destrucción de información
	[E.24]Caída del sistema por agotamiento de recursos
[A]Ataques intencionados	[A.6]Abuso de privilegio de acceso
	[A.7]Uso no previsto
	[A.24]Denegación de servicio

Fuente: Elaborador por el Investigador

Tabla 2.24 Amenazas al activo Soportes de Información [Media]

TIPO	AMENAZA
[N]Desastres Naturales	[N.1]Fuego
	[N.2]Daños por agua
	[N.*]Desastres Naturales 03 – CONTAMINACIÓN 04 - SINIESTRO MAYOR 06 - FENÓMENO CLIMÁTICO 07 - FENÓMENO SÍSMICO 08 - FENÓMENO DE ORIGEN VOLCÁNICO 09 - FENÓMENO METEOROLÓGICO 10 - INUNDACIÓN
[I]De origen industrial	[I.1]Fuego
	[I.2]Daños por agua
	[I.*]Desastres industriales
	[I.3]Contaminación mecánica
	[I.4]Contaminación electromagnética
	[I.5]Avería de origen físico o lógico
	[I.6]Corte de suministro eléctrico
	[I.7]Condiciones inadecuadas de temperatura o humedad
	[I.10]Degradación de los soportes de almacenamiento de la información
[E]Errores y fallos no intencionados	[E.1]Errores de los usuarios
	[E.2]Errores del administrador
	[E.18]Destrucción de información
	[E.23]Errores de mantenimiento/actualización de equipos (hardware)
	[E.25]Pérdida de equipos
[A]Ataques intencionados	[A.7]Uso no previsto
	[A.18]Destrucción de información
	[A.23]Manipulación de los equipos
	[A.25]Robo
	[A.26]Ataque destructivo

Fuente: Elaborador por el Investigador

Tabla 2.25 Amenazas al activo Equipamiento Auxiliar [AUX]

TIPO	AMENAZA
[N]Desastres Naturales	[N.1]Fuego
	[N.2]Daños por agua
	[N.*]Desastres Naturales 03 – CONTAMINACIÓN 04 - SINIESTRO MAYOR 06 - FENÓMENO CLIMÁTICO 07 - FENÓMENO SÍSMICO 08 - FENÓMENO DE ORIGEN VOLCÁNICO 09 - FENÓMENO METEOROLÓGICO 10 - INUNDACIÓN
[I]De origen Industrial	[I.1]Fuego
	[I.2]Daños por agua
	[I.*]Desastres industriales
	[I.3]Contaminación mecánica
	[I.4]Contaminación electromagnética
	[I.5]Avería de origen físico o lógico
	[I.6]Corte de suministro eléctrico
	[I.7]Condiciones inadecuadas de temperatura y humedad
	[I.9]Interrupción de otros servicios y suministros esenciales
[E]Errores y fallos no intencionados	[E.23]Errores de mantenimiento/actualización de equipos
	[E.25]Pérdida de equipos
[A]Ataques intencionados	[A.7]Uso no previsto
	[A.23]Manipulación de equipos
	[A.25]Robo
	[A.26]Ataque destructivo

Fuente: Elaborador por el Investigador

Tabla 2.26 Amenazas al activo Instalaciones [L]

TIPO	AMENAZA
[N]Desastres Naturales	[N.1]Fuego
	[N.2]Daños por agua
	[N.*]Desastres Naturales 03 – CONTAMINACIÓN 04 - SINIESTRO MAYOR 06 - FENÓMENO CLIMÁTICO 07 - FENÓMENO SÍSMICO 08 - FENÓMENO DE ORIGEN VOLCÁNICO 09 - FENÓMENO METEOROLÓGICO 10 - INUNDACIÓN
[I]De origen industrial	[I.1]Fuego
	[I.2]Daños por agua
	[I.*]Desastres industriales
[E]Errores y fallos no intencionados	[E.18]Destrucción de información
[A]Ataques intencionados	[A.7]Uso no previsto
	[A.18]Destrucción de información
	[A.26]Ataque destructivo
	[A.27]Ocupación enemiga

Fuente: Elaborador por el Investigador

Tabla 2.27 Amenazas al activo Personal [P]

TIPO	AMENAZA
[E]Errores y fallos no intencionados	[E.28]Indisponibilidad del personal
[A]Ataques intencionados	[A.28]Indisponibilidad del personal
	[A.29]Extorsión
	[A.30]Ingeniería Social (picaresca)

Fuente: Elaborador por el Investigador

"Cuando un activo es víctima de una amenaza, no se ve afectado en todas sus dimensiones, ni en la misma cuantía. Una vez determinado que una amenaza puede perjudicar a un activo, hay que valorar su influencia en el valor del activo, en dos sentidos:

- **Degradación:** Cuán perjudicado resultaría el valor del activo.

- **Probabilidad:** Cuán probable o improbable es que se materialice la amenaza.

La degradación mide el daño causado por un incidente en el supuesto de que ocurriera, se suele caracterizar como una fracción del valor del activo y así aparecen expresiones como que un activo se ha visto *totalmente degradado*, o *degradado en una pequeña fracción.* Cuando las amenazas no son intencionales, probablemente baste conocer la fracción físicamente perjudicada de un activo para calcular la pérdida proporcional de valor que se pierde. Pero cuando la amenaza es intencional, no se puede pensar en proporcionalidad alguna pues el atacante puede causar mucho daño de forma selectiva" [23]

Asignaremos un valor cualitativo para cada activo mediante las siguientes tablas.

Tablas 2.28 Degradación del valor del activo

CÓDIGO	DESCRIPCIÓN
MA	Muy Alta
A	Alta
M	Media
B	Baja
MB	Muy Baja

Fuente: Elaborado por el Investigador

Tabla 2.29 Probabilidad de ocurrencia

CÓDIGO	VALOR	FRECUENCIA	TIEMPO
MA	100	Muy frecuente	A diario
A	10	Frecuente	Mensualmente
M	1	Normal	Una vez al año
B	1/10	Poco frecuente	Cada varios años
MB	1/100	Muy poco frecuente	Siglos

Fuente: Elaborador por el Investigador

2.2.1.4 Determinación del Impacto Potencial

"Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos en las dimensiones de (Confidencialidad, Integridad y Disponibilidad) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre la institución" [23].

Impacto acumulado: Se calcula con el valor propio más el valor acumulado de los activos que dependen de él, y las amenazas a los que están expuestos estos activos.
Al calcular el impacto permite establecer medidas de defensa para continuar con las actividades de la institución.

2.2.1.5 Determinación del Riesgo Potencial

El riesgo se determina mediante el impacto de las amenazas sobre los activos y la ocurrencia de probabilidad.

Para identificar el nivel de riesgos, sean estos Muy Altos (MA), Altos (A), Medios (M), Bajo (B) y Muy Bajo (MB) se utiliza la tabla 2.30, en donde:

- En la franja roja se encuentran los riesgos muy probables y de muy alto impacto.
- En la franja anaranjada se encuentran los riesgos con alto impacto.
- En la zona amarilla se encuentran los riesgos de impacto medio.
- En la zona gris y blanco de encuentra los riesgos de bajo y muy bajo impacto.

Tabla 2.30 Riesgo en función del impacto y la probabilidad

Riesgo		Probabilidad				
		MB	B	M	A	MA
Impacto	MA	A	MA	MA	MA	MA
	A	M	A	A	MA	MA
	M	B	M	M	A	A
	B	MB	B	B	M	M
	MB	MB	MB	MB	B	B

Fuente: Libro III de MAGERIT [25].

2.2.2 Modalidad de la Investigación

Modalidad bibliográfica: Se considera este método ya que permite a la investigación obtener diferentes fuentes de información derivadas de libros, artículos científicos, tesis de grado, entre otros, referente al tema, con el fin de un aporte teórico, el cual servirá como base a la investigación mediante las diferentes conclusiones de los autores derivados del problema.

Modalidad de campo: Esta modalidad es aplicada debido a que es necesario acudir al lugar de los hechos, donde se desarrollan las actividades informáticas dentro del departamento de TI de la Municipalidad de Ambato, con el fin de recolectar datos reales para la investigación.

Modalidad aplicada: En el presente proyecto se aplica dicha modalidad, porque se utiliza todos los conocimientos adquiridos durante los semestres de formación académica para poder diseñar un plan de contingencia informático ante la presencia de algún evento catastrófico que puede paralizar las actividades de la institución.

2.2.3 Recolección de Información

Las personas que proporcionarán información serán: Analistas de Seguridad y Administrativos del departamento de TI del GAD Municipalidad de Ambato, se recolectará información mediante entrevistas y encuestas al personal del departamento, utilizando el método Delphi. Además, se buscó información en internet basada en libros, artículos científicos, tesis de grado, todo ello, para alcanzar los objetivos planteados.

2.2.4 Procesamiento y Análisis de Datos

Para el procesamiento de los datos es fundamental seleccionar la información de manera correcta para el desarrollo de la investigación en relación con el problema, y así establecer conclusiones con datos reales. El análisis de datos se realizará desde el enfoque estadístico descriptivo, entrevistas, encuestas, que permitan la ejecución del plan de contingencia informático.

2.2.5 Desarrollo del proyecto

Para el desarrollo del proyecto se planearon las siguientes tareas:

- Analizar la situación actual del departamento de TI.
- Identificar de los activos informáticos más importantes.
- Analizar las amenazas en seguridad de la información.
- Evaluar los riesgos graves.
- Diseñar un plan de contingencia informático.

CAPÍTULO 3

RESULTADOS Y DISCUSIÓN

3.1 Análisis y discusión de los resultados

3.1.1 Desarrollo de la propuesta

El presente capítulo muestra de manera detallada las etapas de la elaboración del Plan de Contingencia basado en la norma ISO 24762:2008 para el departamento de TI del Gobierno Autónomo Descentralizado de la Municipalidad de Ambato, el cual contiene el diagnóstico de la situación actual del departamento, análisis de riesgos conforme a lo detallado anteriormente mediante la metodología MAGERIT.

3.1.2 Planificación

Recolectar la información necesaria mediante entrevistas al personal del departamento de TI, una vez obtenida la información se realizará un análisis de los riesgos, identificando los activos más relevantes, identificando las amenazas que afectan a esos activos, el impacto que generar las amenazas a los activos, utilizando la metodología MAGERIT. Mediante el análisis de riesgos obtenemos cuales son los riesgos muy altos y altos a los cuales se les da mayor importancia en el diseño del plan de contingencia informático basado en la norma ISO 24762:2008, en donde se detalla medidas de prevención, ejecución y recuperación ante la presencia de factores internos o externos para recuperarse en el menor tiempo posible

3.1.3 Alcance

El diseño del Plan de Contingencia Informático abarca los servicios y activos informáticos, el mismo se presentó al director del Departamento de Tecnologías de la Información del GAD Municipalidad de Ambato, en la elaboración del Plan de Contingencia no se realizará la fase de pruebas ni implementación de este, por

consiguiente, queda a cargo del personal del departamento de la institución una vez concluido el presente proyecto de titulación.

3.1.4 Información Gobierno Autónomo Descentralizado de Ambato

VISION

Al 2023 El GAD Municipalidad de Ambato será la institución formuladora y ejecutora de acciones que permitan hacer de Ambato un cantón seguro, digital, resiliente, inclusivo, sostenible, y saludable, con servicios de calidad; generadora de políticas que posicionen al cantón a nivel nacional como polo de desarrollo comercial y productivo, fundamentada en el capital intelectual y en el uso eficiente y transparente de sus recursos [26].

MISION

El GAD Municipalidad de Ambato es una institución que promueve el desarrollo sostenible del cantón, a través de la prestación de servicios accesibles, óptimos y oportunos, la implementación de políticas públicas incluyentes, la mejora continua e innovación de sus procesos y servicios, el uso de tecnologías, y el fomento de la participación ciudadana, para mejorar la calidad de vida de sus ciudadanos [26].

PRINCIPIOS INSTITUCIONALES

Tabla 3.1 Principios Institucionales

Cuidado Ambiental	Valor moral fundamental de todo funcionario público de la administración municipal que se basa en generar relaciones interpersonales consolidadas en la confianza y la sinceridad desde el cargo y hacia la comunidad.
Respeto	La administración basa su función en la consideración plena del ser humano sin miramientos de ninguna índole sino únicamente en su esencia misma como persona o institución sustentada en la lealtad y honorabilidad.
	Es el deber de exponer la información relativa a la gestión pública al análisis de la ciudadanía, respecto al manejo de los

Transparencia	recursos, a los criterios que sustentan la toma decisiones, y la conducta de los servidores públicos. Administrar los bienes públicos de forma clara y con actuaciones legales y legítimas, generando confianza de los ciudadanos.
Interculturalidad	Fundamento de libertad e igualdad, no hace distinciones por etnias, por el contrario, promueve el crecimiento y superación de forma igualitaria.
Justicia	Permite reconocer, respetar y hacer valer los derechos de todos los ciudadanos.
Equidad	Implica justicia e igualdad de oportunidades para todos, respetando la pluralidad de la sociedad.
Eficiencia	Capacidad de alcanzar los objetivos con la mejor utilización de los recursos.

Fuente: Elaborador por el investigador, a partir de [26].

VALORES INSTITUCIONALES

Tabla 3.2 Valores institucionales

Compromiso	Es la implicación intelectual y emocional de los miembros de la institución con ésta, y con ello su contribución personal al éxito de la misma.
Solidaridad	La administración persigue y promueve la colaboración en las causas justas de las personas o instituciones para alcanzar de manera objetiva y efectiva los objetivos, propósitos y metas propuestos.
Honestidad	Valor moral fundamental de todo funcionario público de la administración municipal que se basa en generar relaciones interpersonales consolidadas en la confianza y la sinceridad desde el cargo y hacia la comunidad.
Respeto	La administración basa su función en la consideración plena del ser humano sin miramientos de ninguna índole sino únicamente en su esencia misma como persona o institución sustentada en la lealtad y honorabilidad.

Diálogo Participativo	Es un método de democracia cuyo consenso permite la interacción con todos los sectores para generar una gobernanza que permita la integración de la comunidad en la gestión municipal.
Responsabilidad	Cumplimiento de la misión institucional basado en la doble aceptación de servir, servir para la función que le ha sido encomendada y desde esa servir a la ciudadanía para satisfacer sus necesidades.
Justicia	Permite reconocer, respetar y hacer valer los derechos de todos los ciudadanos.

Fuente: Elaborado por el investigador, a partir de [26].

POLÍTICAS

"El GAD Municipalidad de Ambato es reconocido por la calidad en la prestación de servicios, garantizando la transparencia, eficiencia, respeto y equidad en la atención integral, basados en el capital humano, innovación tecnológica y cuidado ambiental, para satisfacer las necesidades, requerimientos y expectativas, promoviendo el desarrollo sostenible, la productividad y gestión eficiente, orientada a mejorar la calidad de vida de sus ciudadanos. La gestión del GAD Municipalidad de Ambato se fundamenta en el cumplimiento de requerimientos legales y normativas aplicables, la mejora continua e innovación de sus procesos y servicios institucionales con un enfoque inclusivo" [26].

OBJETIVOS ESTRATÉGICOS

1. Promover el desarrollo social e intercultural fortaleciendo la salud, bienestar, igualdad de género, deporte y recreación; la conservación del patrimonio cultural, identidad, apropiación de tradiciones y costumbres de Ambato.

2. Promover el desarrollo urbano sostenible, mediante la transformación cultural, participación ciudadana, educación, capacitación, control mitigación, restauración de la transgresión ambiental, aplicando principios de movilidad sostenible, jerarquización de residuos, cuidado del agua, cuidado animal, cuidado ambiental, para el beneficio del cantón.

3. Impulsar el desarrollo productivo del cantón, mediante la optimización de sus diferentes sistemas formales de comercialización, en pro de su beneficio económico.

4. Optimizar las fuentes de financiamiento del presupuesto institucional, a través de recaudaciones propias, recursos fiscales, líneas de crédito y cooperación, para financiar la gestión municipal.

5. Garantizar la dotación de servicios públicos e infraestructura, mediante procesos sostenibles, para el beneficio de los habitantes del cantón.

6. Impulsar la innovación y competitividad del cantón, a través de la digitalización de servicios municipales, para el fortalecimiento de la gestión integral de la calidad institucional y la óptima interacción con los actores de interés y ciudadanía en general.

7. Fortalecer la administración interna institucional, a través de un modelo de gestión apropiado, la mejora continua e innovación de sus procesos y el uso de las tecnologías de información y comunicación, con el fin de alcanzar la excelencia del servicio.

8. Impulsar el desarrollo integral de Ambato, mediante normas que generen incentivos tributarios, un adecuado régimen de uso del suelo y un crecimiento urbano que sea ordenado, seguro, turístico, cultural, patrimonial, gastronómico, natural, inclusivo y sostenible, a fin de promover la inversión privada.

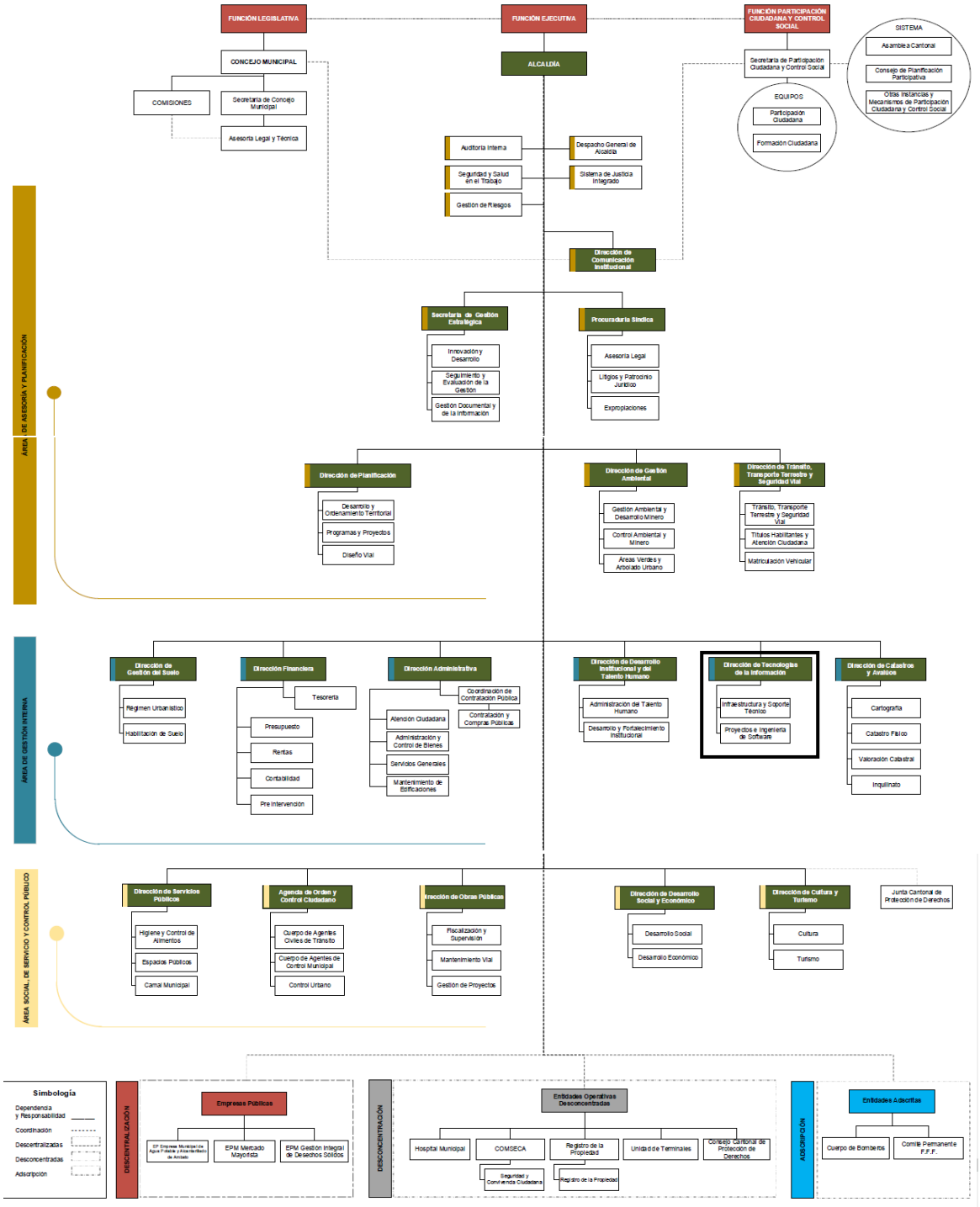
9. Fomentar la actualización y el cumplimiento de las ordenanzas y resoluciones de las competencias municipales acordes con las leyes y normas nacionales vigentes [26].

3.1.5 Organigrama Estructural del GAD Municipalidad de Ambato

"Por resolución administrativa se definió la estructura orgánica del Gobierno Autónomo Descentralizado Municipalidad de Ambato 2019 - 2023, con el fin de mejorar la prestación de servicios, la organización interna, la comunicación

institucional interna y externa, el incremento de la participación ciudadana, y la mejora continua en sus procesos" [27].

Figura 3.1 Organigrama estructura del GADMA



Fuente: Plan de Desarrollo y Ordenamiento Territorial

3.1.6 Diagnóstico de la situación actual

El Departamento de Tecnologías de la Información del GAD Municipalidad de Ambato posee dos Data Center, uno principal y otro alterno, los mismos que se conectan por medio de fibra óptica a 10 Gigabits, cuentan con un diseño topológico Físico y Lógico Check Point para proteger la información que se maneja, sin embargo, puede estar expuesta a amenazas que pueden desestabilizar las actividades que brinda la institución.

Para el respaldo de la información que maneja el Departamento de TI, se almacena cada 15 días en los servidores de la Base de Datos del Data Center Alterno, además utiliza un sistema biométrico para el acceso al Data Center, es decir solo tiene acceso el personal autorizado, cuenta con firewall, todo aquello para asegurar la información, el mismo no está totalmente seguro ante cualquier evento inesperado, sea natural o provocado por el hombre.

Al ser una institución pública cada año se adquiere equipos informáticos nuevos mediante la Norma de Contratación Pública verificado la vigencia tecnológica, para el mantenimiento de software se da soporte cada uno o dos años, además se utilizan licencias perpetuas.

Con el diseño del Plan de Contingencia Informático se pretende la pronta recuperación de los servicios previo a un análisis de riesgos, para enfocarse en los riesgos más altos siendo estos de mayor prioridad para la institución, debido al gran tamaño de información que se maneja de toda la ciudadanía de Ambato.

Análisis FODA del Departamento de Tecnologías de la Información del GAD Municipalidad de Ambato

Con la participación del personal de TI y la documentación pertinente, se realiza un análisis FODA del departamento, identificando las principales fortalezas, oportunidades, debilidades y amenazas presentes.

Tabla 3.3 Análisis FODA de departamento de TI

AMBIENTE INTERNO	AMBIENTE EXTERNO
FORTALEZAS	**OPORTUNIDADES**
• Personal con conocimiento necesario para resolver problemas informáticos. • Gran ancho de banda. • Licencias perpetuas para software. • Tecnología de punta en servidores. • Cuarto frio para servidores. • Infraestructura tecnológica. • Buen ambiente laboral.	• Respuesta inmediata para solventar problemas. • Avances tecnológicos.
DEBILIDADES	**AMENAZAS**
• Falta de capacitaciones al personal de TI. • Falta de personal para soporte. • No poseen políticas de seguridad. • No poseen planes de contingencia informático en base a una norma de estandarización. • Falta de charlas en seguridad informática.	• Cambio repentino de autoridades. • Falta de presupuesto para contratación de personal y equipos tecnológicos. • Pandemias. • Espacio físico inadecuado. • Falta de procesos definidos. • Mala planificación par proyectos.

Fuente: Elaborador por el Investigador en base a la información proporcionada por el departamento de TI

3.1.7 Ubicación geográfica

Las parroquias urbanas de Ambato, por su ubicación y por la tipología del depósito volcánico presente en el subsuelo de la ciudad, presenta amenazas relacionadas principalmente a" flujos de detritos" (deslizamiento o avalanchas de escombros, lahares secundarios), y en menor peso por caída de cenizas provenientes del volcán Tungurahua.

En la siguiente tabla se especifica los eventos catastróficos que se han registrado en la región, donde se observa que los fenómenos de mayor recurrencia son los sismos, con

lo cual, se tiene un proceso disparador muy importante para producir en el tiempo estas avalanchas, lahares, y deslizamientos, que son procesos de remoción en masa sensibles a las pendientes y a las condiciones hidro climatológicas prevalecientes en la región.

Tabla 3.4 Eventos catastróficos

FECHA	TIPO DE FENÓMENO	LUGAR AFECTADO	CONSECUENCIAS
1687	Terremoto	Ambato	Destrucción de Ambato, Latacunga y pueblos de la comarca – aprox. 7200 muertos
1698	Terremoto	Riobamba, Ambato y Latacunga	Gran destrucción de casas e Iglesias aprox. 7000 muertos.
1949	Terremoto	Ambato y Pelileo	Ciudad integralmente destruida, 6000 muertos y miles de heridos, 100.000 personas sin hogar, consecuencias socioeconómicas grandes y de larga duración. consecuencias socioeconómicas grandes y de larga duración.
2002	Temblor	Ambato	4.8 Richter
2012	Temblor	Pelileo	Sentido en Ambato, Baños, Patate, Mocha, Salcedo

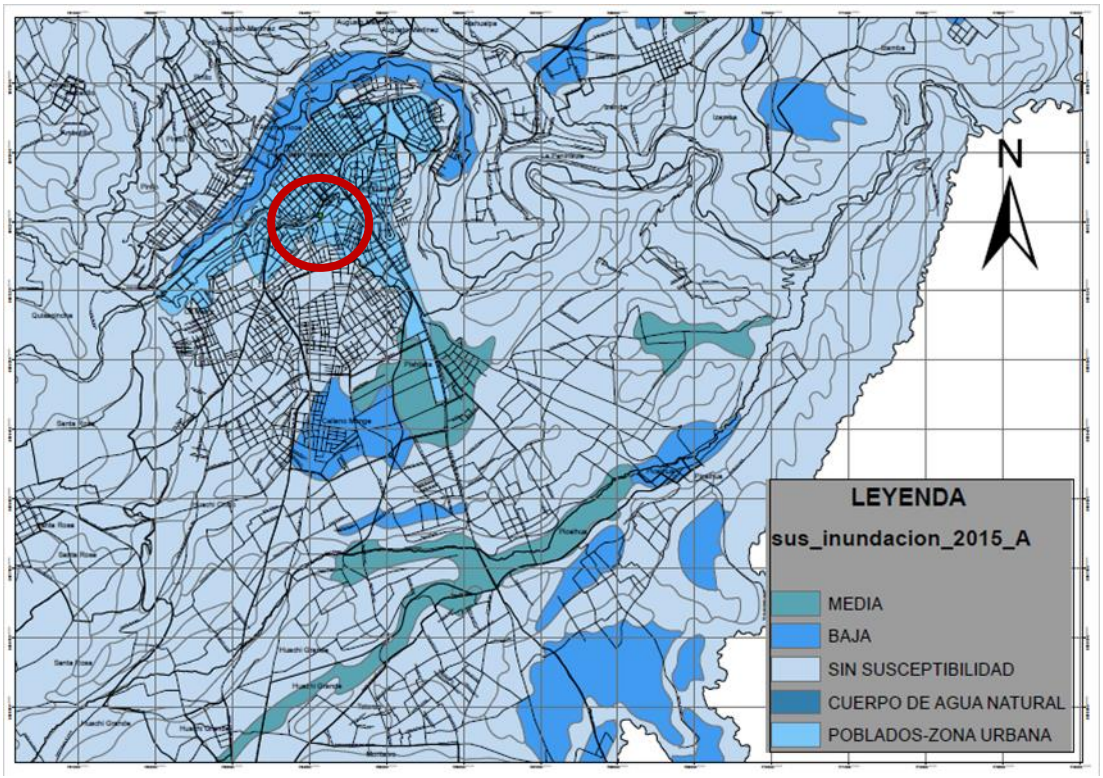
Fuente: Elaborado por el investigador, a partir de [27].

En el cantón Ambato se han identificado los siguientes tipos de amenazas:

Amenaza por inundaciones

En el cantón Ambato, en términos generales, tiene una baja amenaza en lo relacionado a las inundaciones. Han ocurrido menos de 20 entre 1988 y el 2010. A pesar de ubicarse en una zona seca, según estudios realizados, tiene sectores de posibles inundaciones.

Figura 3.2 Afectación por inundación Ambato-2015



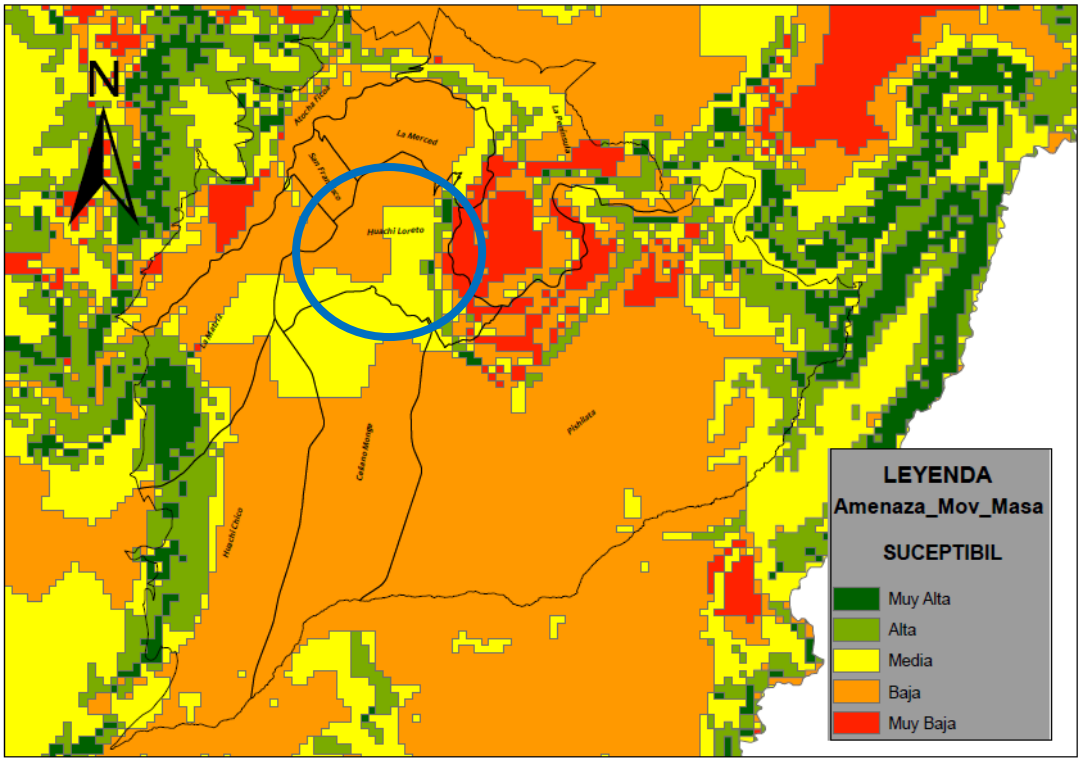
Fuente: Plan de Desarrollo y Ordenamiento Territorial.

En el círculo rojo de la figura 3.2 se puede observar la zona donde se encuentra ubicado el Gobierno Autónomo Descentralizado de la Municipalidad de Ambato GADMA, dando como resultado una afectación media de inundación.

Amenaza por fallas sísmicas

Si bien la ciudad de Ambato tiene un suelo bastante bueno desde el punto de vista sísmico, no es menos cierto que una gran cantidad de fallas geológicas atraviesan la ciudad o están muy próximas. Esto se debe al continuo movimiento de las placas tectónicas. Es necesario conocer esta realidad para construir estructuras seguras contra la acción de sismos y para hacer estudios de vulnerabilidad sísmica de las estructuras existentes pensando en el reforzamiento de estas [27].

Figura 3.3 Amenazas por movimiento de masa

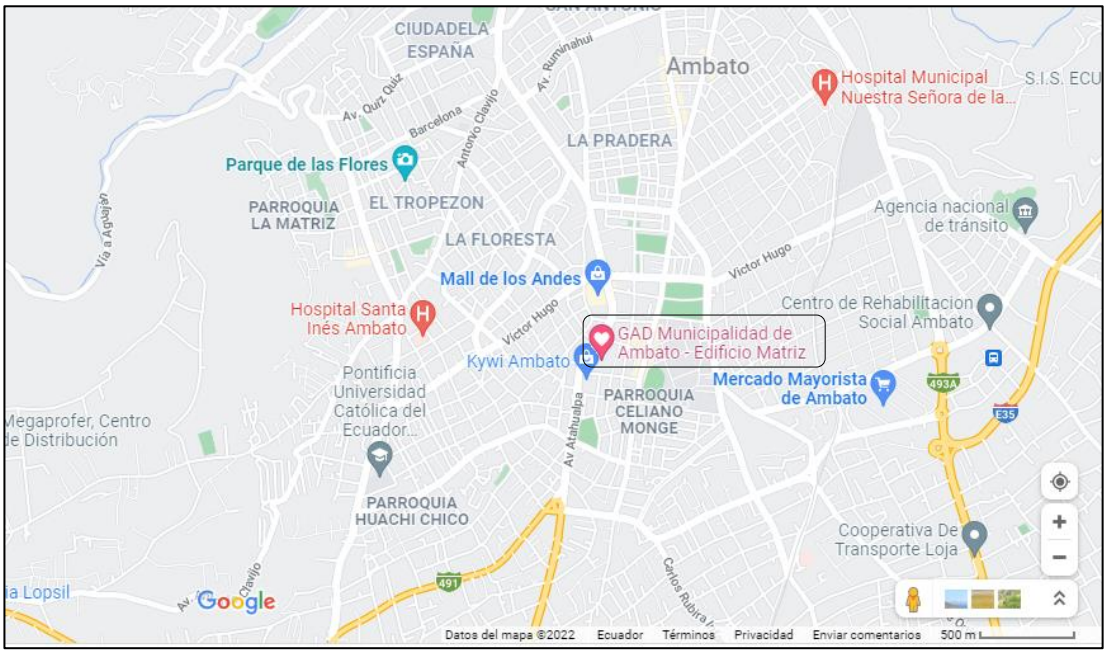


Fuente: Plan de Desarrollo y Ordenamiento Territorial

En el círculo azul de la figura 3.3 se puede observar que la afectación al Gobierno Autónomo Descentralizado de la Municipalidad de Ambato GADMA es media alta por los colores naranja y amarillo.

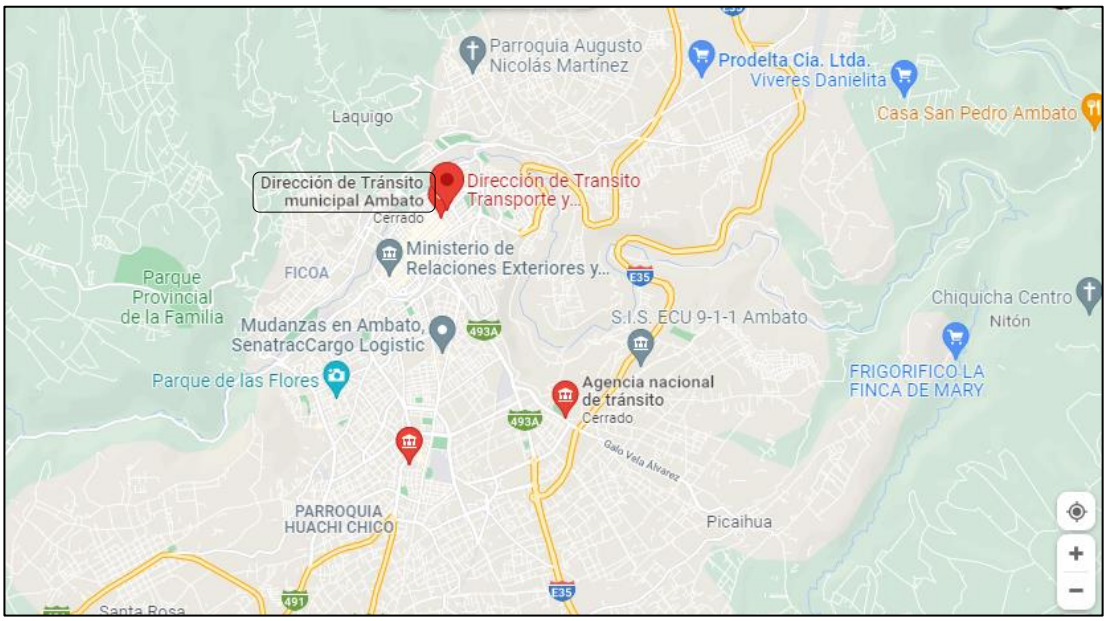
El Gobierno Autónomo Descentralizado de la Municipalidad de Ambato, se encuentra ubicado en la ciudad de Ambato, entre la Av. Atahualpa y Rio Cutuchi, Huachi Loreto.

Figura 3.4 Ubicación geográfica del GADMA



Fuente: Google Maps

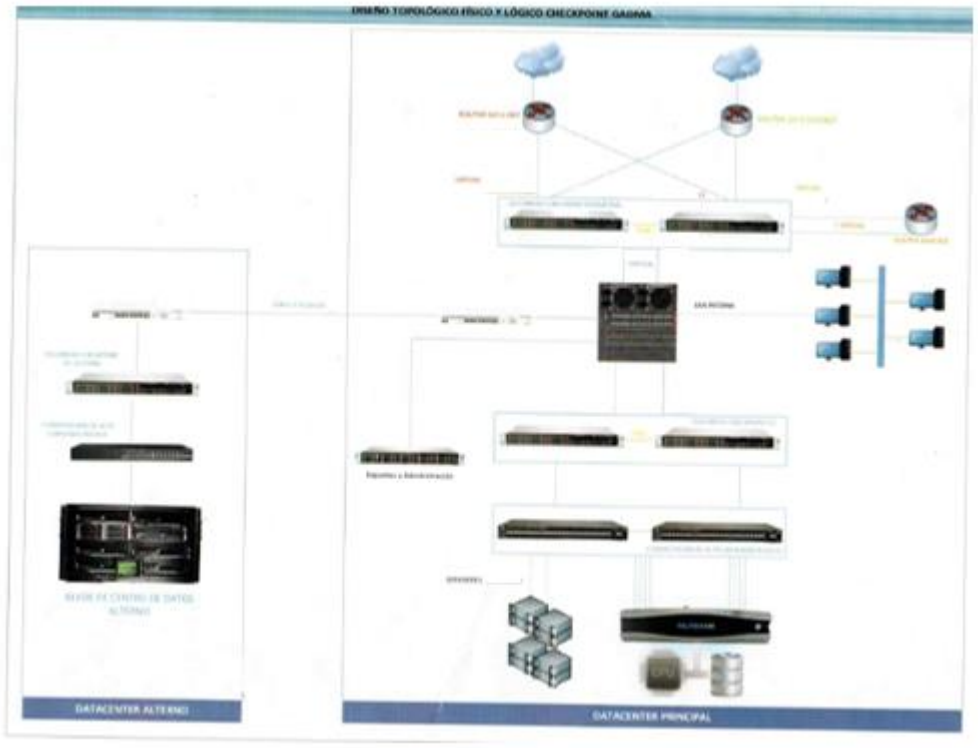
El GADMA posee un Data Center alterno que funciona como respaldo de información de la institución, se encuentra ubicado en el centro de la ciudad de Ambato, entre las calles Simón Bolívar y Vargas Torres.



3.1.8 Diseño topológico de la institución

La institución cuenta con un diseño topológico físico y lógico Check Point para seguridad del Data Center, cuenta con dos proveedores de internet: CNT (40 kbit/s) y TELCONET (70 kbit/s), posee seguridad perimetral, conmutación de alta capacidad, y además dispone de un Data Center alterno para respaldo. En la figura 3.5 se observa el diseño topológico de la institución.

Figura 3.5 Diseño Topológico del GADMA



Fuente: Departamento de TI.

3.1.9 Activos informáticos

El departamento de Tecnologías de la Información se encarga de dirigir y gestionar servicios relacionados con tecnologías de la información; proveer servicios de diseño y desarrollo de software; y, realizar el monitoreo y mantenimiento continuo de la infraestructura de telecomunicaciones [28].

Principales Servicios del GAD Municipalidad de Ambato

En la siguiente tabla se especifican los servicios que brinda la municipalidad por medio del departamento de TI.

Tabla 3.5 Principales servicios de GAD Municipalidad de Ambato

NOMBRE	DESCRIPCION	ELABORACION (INTERNO/EXTERNO)	CARACTERISTICAS ESPECIALES	EQUIPAMIENTO	ESTADO	PRIORIDAD
GADMATIC	Servicios tramites en línea, pagos de predios, historial de un contribuyente, sacar certificados, portal del ciudadano.	Interno	Sistema almacenado en Oracle	Servicio de internet	Funcionando	5
Archivo Digital	Archivos de procesos municipales, ordenanzas, Resoluciones, CURs	Interno	Sistema desarrollado internamente	Servicio de internet	Funcionando	2
SMS Enviar Mensajes	Mensajes de textos a los contribuyentes, notificaciones de trámites	Interno	Sistema desarrollado internamente	Servicio de internet	Funcionando	1
Campus Virtual GADMA	Campus Virtual de Capacitaciones y cursos gratuitos para personal interno y externos	Interno	Desarrollado en Moddle	Servicio de internet	Funcionando	1
Permisos y Vacaciones	Requerimientos de usuarios internos	Interno	Sistema desarrollado internamente	Servicio de internet	Funcionando	2
Consulta en Línea	Consultas básicas de trámites municipales	Interno	Sistema desarrollado internamente	Servicio de internet	Funcionando	3
DOCFLOW WEB	Sistema de administración y seguimiento del proceso de trámites	Interno	Sistema adquirido, Almacenado en Oracle	Servicio de internet	Funcionando	2
Archivo Digital Interno	Archivo digital interno Secretaría Ejecutiva	Interno	Sistema adquirido VERSION ACTUALIZADA, Oracle, Sistema desarrollado en Apex	Servicio de internet	Funcionando	2

N.º	NOMBRE	DESCRIPCION	ELABORACION (INTERNO/EXTERNO)	CARACTERISTICAS ESPECIALES	EQUIPAMIENTO	ESTADO	PRIORIDAD	N.º
9	Correo y Office 365	Correo Institucional Office 365	Interno	Office 365	Servicio de internet	Funcionando	3	1
10	Sistema E-SIP	Elaboración de PAC (Plan de contratación Anual) y POA (Plan Organizacional Anual)	Interno	Sistema adquirido	Servicio de internet	Funcionando	2	2
11	Solicitud Horas Extras	Sistema para el personal que labora los fines de semana y pasadas las 5pm	Interno	Sistema desarrollado internamente	Servicio de internet	Funcionando	1	3
12	Facturación Electrónica	Retenciones que emite el municipio	Interno	Sistema desarrollado con el sistema financiero	Servicio de internet	Funcionando	2	4
13	GIS- Sistema de Catastros	Sistema Georreferencial de todo el cantón, avalúos y Catastros	Interno	Sistema de Información Geográfica (GIS)	Servicio de internet	Funcionando	4	5
14	Consulta Horarios	Personal Interno, cambio de horario, Agente de Tránsito y Municipal	Interno	Sistema desarrollado en Apex	Servicio de internet	Funcionando	1	6
15	Sistema de Denuncias de Justicia	Trámites de departamento Jurídico	Interno	Sistema desarrollado internamente	Servicio de internet	Funcionando	2	7
16	Mis Activos	Consultar los activos fijos del municipio	Interno	Sistema desarrollado internamente, almacenada en Oracle	Servicio de internet	Funcionando	2	8

N.º	NOMBRE	DESCRIPCION	ELABORACION (INTERNO/EXTERNO)	CARACTERISTICAS ESPECIALES	EQUIPAMIENTO	ESTADO	PRIORIDAD
17	Consulta Dato Seguro	Consulta de información de un contribuyente, datos personales	Interno	Sistema desarrollado internamente, con intercomunicación con Dato Seguro	Servicio de internet	Funcionando	2
18	GLPI Help Desk	Sistema de Tickets para soporte de Tecnologías	Interno	Sistema Open Source de GLPI	Servicio de internet	Funcionando	1
19	Mis Datos Personales	Actualización de datos Personales del Municipio	Interno	Sistema desarrollado en Apex	Servicio de internet	Funcionando	1
20	Turnos para trámites municipales	Generación de turnos para trámites municipales	Externo	Sistema desarrollado en Apex y almacenado en Oracle	Servicio de internet	Funcionando	2
21	Traspasos de Dominios	Trámite de traspaso con la clave catastral con la finalidad de agilizar los tiempos de atención.	Externo	Sistema desarrollado en Apex y almacenado en Oracle	Servicio de internet	Funcionando	3
22	Consulta de impuestos prediales	Consulta de impuestos municipales mediante la cédula, RUC o CIU	Externo	Sistema desarrollado en Apex y almacenado en Oracle	Servicio de internet	Funcionando	4
23	Consulta de otros impuestos municipales	Consultar si tiene deudas pendientes de pago por concepto de Predio o Contribuciones Especiales	Externo	Sistema desarrollado en Apex y almacenado en Oracle	Servicio de internet	Funcionando	4
24	Consulta de Avalúo Vehicular	Consulta de Avalúo Vehicular mediante la placa o RAMW	Externo	Sistema desarrollado en Apex y almacenado en Oracle	Servicio de internet	Funcionando	3

N.º	NOMBRE	DESCRIPCION	ELABORACION (INTERNO/EXTERNO)	CARACTERISTICAS ESPECIALES	EQUIPAMIENTO	ESTADO	PRIORIDAD
25	Consulta de Regularización de Áreas	Predios sujetos a regularización de áreas, excedentes que superan el 100% de la superficie medida, con respecto a la superficie de la escritura	Externo	Sistema desarrollado en Apex y almacenado en Oracle	Servicio de internet	Funcionando	3
26	Consultas Públicas	Consultas Públicas de los servicios que presta el municipio a la ciudadanía	Externo	Sistema desarrollado en Apex y almacenado en Oracle	Servicio de internet	Funcionando	3
27	Sistema de Quejas y Sugerencias	Manifestación que se hace a causa de un desacuerdo o inconformidad respecto a una conducta incorrecta o servicio brindado por servidores públicos o particulares que llevan a cabo un servicio público para la Municipalidad	Externo	Sistema desarrollado en Apex y almacenado en Oracle	Servicio de internet	Funcionando	2
28	Solicitud de acceso al Sistema GADMAPPS	Ingreso autorizado para contribuyentes	Externo	Sistema desarrollado en Apex y almacenado en Oracle	Servicio de internet	Funcionando	5
29	Acceder al formulario de contestación y	Consulta de infracciones registradas con el número de cédula o pasaporte	Externo	Sistema desarrollado en Apex y almacenado en Oracle	Servicio de internet	Funcionando	1
30	Reserva de cancha de césped sintético	Reserva de recursos del GADMA: Salones y auditorios, teatros, canchas.	Interno	Sistema desarrollado en Apex y almacenado en Oracle	Servicio de internet	Funcionando	1
31	Sistema de Información	Información de los servicios que el GADMA brinda a la ciudadanía	Interno	Sistema desarrollado en Apex y almacenado en Oracle	Servicio de internet	Funcionando	3
32	Ingreso Teletrabajo	Sistema que proporciona facilidad y agilidad a los trámites para la autorización de permisos o de vacaciones dentro de la institución	Interno	Aplicación desarrollada en Java	Servicio de internet	Funcionando	1

N.º	NOMBRE	DESCRIPCION	ELABORACION (INTERNO/EXTERNO)	CARACTERISTICAS ESPECIALES	EQUIPAMIENTO	ESTADO	PRIORIDAD
33	Control Horas Extras	Sistema para solicitar horas extras del personal de la institución	Externo	Aplicación desarrollada en Java	Servicio de internet	Funcionando	1
34	Acceso Remoto	Conexión mediante un dominio, usuario y clave	Externo	Aplicación web para escritorio remoto para teletrabajo	Servicio de internet	Funcionando	3
35	Entrega de Placas	Consultar si la nueva placa está lista para su entrega en las oficinas de Matriculación del GADMA.	Externo	Sistema desarrollado en Apex y almacenado en Oracle	Servicio de internet	Funcionando	1
36	Solicitud de Acceso GADMATIC	Acceso al portal de servicios GADMATIC Trámites en Línea	Externo	Aplicación desarrollada en Java	Servicio de internet	Funcionando	4
37	Pago con Tarjeta de Crédito	Sistema de pagos en línea del GADMA	Externo	Aplicación desarrollada en Java	Servicio de internet	Funcionando	4
38	Turno para matriculación	Sistema de turnos para matriculación vehicular	Externo	Aplicación desarrollada en Java	Servicio de internet	Funcionando	3
39	Actualización Catastral	Sistema de turnos para actualización catastral	Externo	Aplicación desarrollada en Java	Servicio de internet	Funcionando	5
40	Emisión títulos de matriculación/ rodaje	Sistema de solicitudes para emisión de títulos	Externo	Aplicación desarrollada en Java	Servicio de internet	Funcionando	3
41	Turnos H. Nuestra Señora de la Merced	Sistema de turnos para el Hospital Nuestra Señora de la Merced mediante la cédula, historia clínica, apellidos y nombres o celular	Externo	Aplicación desarrollada en Java	Servicio de internet	Funcionando	1

Fuente: Elaborado por el investigador, a partir de la página oficial de la institución

https://ambato.gob.ec/

3.1.10 Identificación de activos de información más relevantes

El departamento de Tecnologías de la Información tiene bajo su responsabilidad un sinnúmero de servicios, datos/información, hardware, software, redes de comunicación, para ello se ha identificado los activos más importantes que posee el departamento para el normal funcionamiento de los servicios que presta la municipalidad a la ciudadanía.

3.1.10.1 Servicios

Debido a la gran cantidad de servicios que brinda la municipalidad a la ciudadanía se ha agrupado como se muestra en la tabla 3.5, dando como resultado 10 servicios, que a su vez se dividen en públicos (3) e internos (7).

Tabla 3.6 Servicios

N.º	CÓDIGO	DESCRIPCION
1	Spub01	Servicio público 1
2	Spub02	Servicio público 2
3	Spub03	Servicio público 3
4	Sint01	Servicio interno 1
5	Sint02	Servicio interno 2
6	Sint03	Servicio interno 3
7	Sint04	Servicio interno 4
8	Sint05	Servicio interno 5
9	Sint06	Servicio interno 6
10	Sint07	Servicio interno 7

Fuente: Elaborado por el Investigador

3.1.10.2 Activos de Hardware

En el Data Center se almacenan los activos más importantes de la institución, debido a que almacena gran cantidad de información valiosa, por ello es vital mantenerlos disponibles y accesibles para brindar continuidad a las actividades de la institución.

Tabla 3.7 Activos de Hardware

N.º	CÓDIGO	DESCRIPCION	TIPO
1	HW-host01	Servidor 1	Virtual
2	HW-host02	Servidor 2	Físico
3	HW-host03	Servidor 3	Físico
4	HW-host04	Servidor 4	Físico
5	HW-switch01	Switch 1	Físico
6	HW-switch02	Switch 2	Físico
7	HW-firewall01	Firewall 1	Físico
8	HW-firewall02	Firewall 2	Físico

Fuente: Elaborado por el Investigador

3.1.10.3 Activos de Software

En la siguiente tabla se detalla los sistemas operativos y software en los cuales se ejecutan los servicios que están disponible para la ciudadanía.

Tabla 3.8 Activos de Software

N.º	CÓDIGO	DESCRIPCION
1	SW-std-os01	Sistema Operativo 1
2	SW-std-os02	Sistema Operativo 2
3	SW-std-os03	Sistema Operativo 3
4	SW-std-os04	Sistema Operativo 4
5	SW-std-os05	Sistema Operativo 5
6	SW-std-os06	Sistema Operativo 6
7	SW-std-os07	Sistema Operativo 7
8	SW-std-os08	Sistema Operativo 8
9	SW-std-os09	Sistema Operativo 9
10	SW-std-os10	Sistema Operativo 10

11	SW-std-1	Software 1
12	SW-std-dbms01	Software Base de Datos 1
13	SW-std-dbms02	Software Base de Datos 2
14	SW-std-2	Software 2
15	SW-std-3	Software 3
16	SW-std-4	Software 4
17	SW-std-5	Software 5
18	SW-std-6	Software Switch 1
19	SW-std-7	Software Switch 2
20	SW-std-8	Software Firewall 1
21	SW-std-9	Software Firewall 2

Fuente: Elaborado por el investigador

3.1.10.4 Datos/ Información

En la siguiente tabla se detalla las configuraciones sobre los activos más relevante que posee el Data Center del departamento de TI.

Tabla 3.9 Activos de Información

N.º	CÓDIGO	DESCRIPCION
1	D-conf01	Configuración Firewall 1
2	D-conf02	Configuración Firewall 2
3	D-conf03	Configuración de Switch

Fuente: Elaborado por el investigador

Otra información relevante de la institución esta almacenada en carpetas compartidas que a su vez se alojan en los servidores que se menciona en la tabla 3.7 Activos de Hardware.

3.1.10.5 Activo de Redes de Comunicación

En la siguiente tabla se detalla los activos de red de comunicación, el mismo que permite la conexión entre los activos del Data Center.

Tabla 3.10 Activo de Redes de Comunicación

N.º	CÓDIGO	DESCRIPCION
1	COM-internet01	Router 1
2	COM-internet02	Router 2

3.1.11 Análisis de Riesgo con la metodología MAGERIT

3.1.11.1 Valoración de activos

La valoración de los activos se realizó utilizando la metodología MAGERIT y el método Delphi, para lo cual se realizó un grupo de dos profesionales (un Ingeniero en Electrónica y Computación y un Ingeniero en Seguridad Informática) junto con el investigador, para asignar valores analizando las dimensiones de Confidencialidad (C), Integridad (I) y Disponibilidad (D), mediante los criterios valoración que encontramos en las tablas de la 2.5 a la 2.17. No se muestra las fichas de valoración para cada uno de los activos por el acuerdo confidencial con la institución.

En la siguiente tabla se muestra el valor final obtenido de las fichas de valoración de cada activo.

Tabla 3.11 Valoración de activos

N.º	ACTIVO	VALOR DEL ACTIVO			VALOR HEREDADO			VALOR TOTAL			VALOR PONDERADO		
		C	I	D	C	I	D	C	I	D	C	I	D
1	Spub01	-	3	5	-	-	-	-	3	5	-	M	M
2	Spub02	-	5	5	-	-	-	-	5	5	-	M	M
3	Spub03	-	5	5	-	-	-	-	5	5	-	M	M
4	Sint01	-	5	5	-	-	-	-	5	5	-	M	M
5	Sint02	-	7	7	-	-	-	-	7	7	-	A	A
6	Sint03	3	5	5	-	-	-	3	5	5	M	M	M
7	Sint04	7	7	7	-	-	-	7	7	7	A	A	A

8	Sint05	5	7	7	-	-	-	5	7	7	M	A	A
9	Sint06	3	3	3	-	-	-	3	3	3	M	M	M
10	Sint07	3	3	3	-	-	-	3	3	3	M	M	M
11	SW-std-os01	-	5	5	-	-	-	-	5	5	-	M	M
12	SW-std-os02	-	5	5	-	-	-	-	5	5	-	M	M
13	SW-std-os03	-	7	7	-	-	-	-	7	7	-	A	A
14	SW-std-os04	-	7	7	-	-	-	-	7	7	-	A	A
15	SW-std-os05	-	5	5	-	-	-	-	5	5	-	M	M
16	SW-std-os06	-	5	5	-	-	-	-	5	5	-	M	M
17	SW-std-os07	-	5	5	-	-	-		5	5	-	M	M
18	SW-std-os08	-	5	5	-	-	-	-	5	5	-	M	M
19	SW-std-os09	-	5	5	-	-	-	-	5	5	-	M	M
20	SW-std-os10	-	5	5	-	-	-	-	5	5	-	M	M
21	SW-std-1	-	5	5	-	3	5	-	5	5	-	M	M
22	SW-std-dbms01	-	5	5	3	5	5	3	5	5	M	M	M
23	SW-std-dbms02	-	5	5	7	7	7	7	7	7	A	A	A
24	SW-std-2	-	5	5	-	5	5	-	5	5	-	M	M
25	SW-std-3	-	5	5	-	5	5	-	5	5	-	M	M
26	SW-std-4	-	5	5	-	5	5	-	5	5	-	M	M
27	SW-std-5	-	5	5	-	7	7	-	7	7	-	A	A
28	SW-std-6	-	3	3	5	7	7	5	7	7	M	A	A
29	SW-std-7	-	3	3	5	7	7	5	7	7	M	A	A

30	SW-std-8	-	3	3	5	7	7	5	7	7	M	A	A
31	SW-std-9	-	3	3	5	7	7	5	7	7	M	A	A
32	HW-host01	-	7	7	5	7	7	5	7	7	M	A	A
33	HW-host02	-	7	7	7	7	7	7	7	7	A	A	A
34	HW-host03	-	5	5	3	3	3	3	5	5	M	M	M
35	HW-host04	-	5	5	3	3	3	3	5	5	M	M	M
36	HW-switch01	-	5	5	5	7	7	5	7	7	M	A	A
37	HW-firewall01	-	5	5	5	7	7	5	7	7	M	A	A
38	HW-switch02	-	5	5	5	7	7	5	7	7	M	A	A
39	HW-firewall02	-	5	5	5	7	7	5	7	7	M	A	A
40	D-conf01	9	9	9	5	7	7	9	9	9	A	A	A
41	D-conf02	9	9	9	5	7	7	9	9	9	A	A	A
42	D-conf03	9	9	9	5	7	7	9	9	9	A	A	A
43	COM-internet01	-	9	9	5	7	7	5	9	9	A	A	A
44	COM-internet02	-	9	9	5	7	7	5	9	9	A	A	A

Fuente: Elaborado por el investigador

3.1.11.2 Impacto de las amenazas sobre los activos

Una vez identificada las amenazas para cada tipo de activo y conociendo su valor, se evalúa el valor de degradación que afectan dichas amenazas al valor del activo, por consiguiente, conoceremos el daño en caso de materializarse las amenazas. En las siguientes tablas se detalla el impacto en cada uno de los activos.

Tabla 3.12 Impacto en Servicios

ACTIVO	AMENAZA	VALOR DEL ACTIVO			DEGRADACION			IMPACTO		
		C	I	D	C	I	D	C	I	D
Spub01	E.1 Errores de los usuarios	-	M	M	-	M	A	-	MB	B
	E.2 Errores del administrador	-	M	M	-	M	MA	-	MB	M
	E.18 Destrucción de información	-	M	M	-	M	MA	-	MB	M
	E.19 Fugas de información	-	M	M	-	M	MA	-	MB	M
	E.24 Caída del sistema por agotamiento de recursos	-	M	M	-	M	MA	-	MB	M
	A.6 Abuso de privilegios de acceso	-	M	M	-	M	MA	-	MB	M
	A.7 Uso no previsto	-	M	M	-	M	A	-	MB	B
	A.18 Destrucción de información	-	M	M	-	A	MA	-	B	M
	A.24 Denegación de servicio	-	M	M	-	M	MA	-	MB	M
Spub02	E.1 Errores de los usuarios	-		M	-	M	A	-	MB	B
	E.2 Errores del administrador	-	M	M	-	M	MA	-	MB	M
	E.18 Destrucción de información	-	M	M	-	M	MA	-	MB	M
	E.19 Fugas de información	-	M	M	-	M	MA	-	MB	M
	E.24 Caída del sistema por agotamiento de recursos	-	M	M	-	M	MA	-	MB	M
	A.6 Abuso de privilegios de acceso	-	M	M	-	M	MA	-	MB	M
	A.7 Uso no previsto	-	M	M	-	M	A	-	MB	B
	A.18 Destrucción de información	-	M	M	-	A	MA	-	B	M
	A.24 Denegación de servicio	-	M	M	-	M	MA	-	MB	M

Spub03	E.1 Errores de los usuarios	-	M	M	-	M	A	-	MB	B
	E.2 Errores del administrador	-	M	M	-	M	MA	-	MB	M
	E.18 Destrucción de información	-	M	M	-	M	MA	-	MB	M
	E.19 Fugas de información	-	M	M	-	M	MA	-	MB	M
	E.24 Caída del sistema por agotamiento de recursos	-	M	M	-	M	MA	-	MB	M
	A.6 Abuso de privilegios de acceso	-	M	M	-	M	MA	-	MB	M
	A.7 Uso no previsto	-	M	M	-	M	M	-	MB	MB
	A.18 Destrucción de información	-	M	M	-	M	MA	-	MB	M
	A.24 Denegación de servicio	-	M	M	-	M	MA	-	MB	M
Sint01	E.1 Errores de los usuarios	-	M	M	-	M	A	-	MB	B
	E.2 Errores del administrador	-	M	M	-	M	MA	-	MB	M
	E.18 Destrucción de información	-	M	M	-	M	MA	-	MB	M
	E.19 Fugas de información	-	M	M	-	M	MA	-	MB	M
	E.24 Caída del sistema por agotamiento de recursos	-	M	M	-	M	MA	-	MB	M
	A.6 Abuso de privilegios de acceso	-	M	M	-	M	MA	-	MB	M
	A.7 Uso no previsto	-	M	M	-	M	MA	-	MB	M
	A.18 Destrucción de información	-	M	M	-	M	MA	-	MB	M
	A.24 Denegación de servicio	-	M	M	-	M	MA	-	MB	M
Sint02	E.1 Errores de los usuarios	-	A	A	-	M	MA	-	B	A
	E.2 Errores del administrador	-	A	A	-	M	MA	-	B	A

	E.18 Destrucción de información	-	A	A	-	A	MA	-	M	A
	E.19 Fugas de información	-	A	A	-	A	MA	-	M	A
	E.24 Caída del sistema por agotamiento de recursos	-	A	A	-	M	MA	-	B	A
	A.6 Abuso de privilegios de acceso	-	A	A	-	M	MA	-	B	A
	A.7 Uso no previsto	-	A	A	-	M	MA	-	B	A
	A.18 Destrucción de información	-	A	A	-	A	MA	-	M	A
	A.24 Denegación de servicio	-	A	A	-	M	MA	-	B	A
Sint03	E.1 Errores de los usuarios	M	M	M	M	M	A	MB	MB	B
	E.2 Errores del administrador	M	M	M	M	M	MA	MB	MB	M
	E.18 Destrucción de información	M	M	M	M	M	MA	MB	MB	M
	E.19 Fugas de información	M	M	M	M	M	MA	MB	MB	M
	E.24 Caída del sistema por agotamiento de recursos	M	M	M	M	M	MA	MB	MB	M
	A.6 Abuso de privilegios de acceso	M	M	M	M	M	MA	MB	MB	M
	A.7 Uso no previsto	M	M	M	M	M	MA	MB	MB	M
	A.18 Destrucción de información	M	M	M	M	M	MA	MB	MB	M
	A.24 Denegación de servicio	M	M	M	M	M	MA	MB	MB	M
Sint04	E.1 Errores de los usuarios	A	A	A	A	A	A	M	M	M
	E.2 Errores del administrador	A	A	A	A	A	MA	M	M	A
	E.18 Destrucción de información	A	A	A	A	A	MA	M	M	A

	E.19 Fugas de información	A	A	A	A	A	MA	M	M	A
	E.24 Caída del sistema por agotamiento de recursos	A	A	A	A	A	MA	M	M	A
	A.6 Abuso de privilegios de acceso	A	A	A	A	A	MA	M	M	A
	A.7 Uso no previsto	A	A	A	A	A	MA	M	M	A
	A.18 Destrucción de información	A	A	A	A	A	MA	M	M	A
	A.24 Denegación de servicio	A	A	A	A	A	MA	M	M	A
Sint05	E.1 Errores de los usuarios	M	A	A	M	A	A	MB	M	M
	E.2 Errores del administrador	M	A	A	M	A	MA	MB	M	A
	E.18 Destrucción de información	M	A	A	A	A	MA	B	M	A
	E.19 Fugas de información	M	A	A	A	A	MA	B	M	A
	E.24 Caída del sistema por agotamiento de recursos	M	A	A	A	A	MA	B	M	A
	A.6 Abuso de privilegios de acceso	M	A	A	A	A	MA	B	M	A
	A.7 Uso no previsto	M	A	A	A	A	MA	B	M	A
	A.18 Destrucción de información	M	A	A	A	A	MA	B	M	A
	A.24 Denegación de servicio	M	A	A	A	A	MA	B	M	A
Sint06	E.1 Errores de los usuarios	M	M	M	M	M	A	MB	MB	B
	E.2 Errores del administrador	M	M	M	M	M	MA	MB	MB	M
	E.18 Destrucción de información	M	M	M	M	A	MA	MB	B	M
	E.19 Fugas de información	M	M	M	A	A	MA	B	B	M
	E.24 Caída del sistema por agotamiento de recursos	M	M	M	M	A	MA	MB	B	M

	A.6 Abuso de privilegios de acceso	M	M	M	A	A	MA	B	B	M
	A.7 Uso no previsto	M	M	M	A	A	MA	B	B	M
	A.18 Destrucción de información	M	M	M	A	A	MA	B	B	M
	A.24 Denegación de servicio	M	M	M	A	A	MA	B	B	M
Sint07	E.1 Errores de los usuarios	M	M	M	M	M	A	MB	MB	B
	E.2 Errores del administrador	M	M	M	M	M	MA	MB	MB	M
	E.18 Destrucción de información	M	M	M	M	A	MA	MB	B	M
	E.19 Fugas de información	M	M	M	A	A	MA	B	B	M
	E.24 Caída del sistema por agotamiento de recursos	M	M	M	M	A	MA	MB	B	M
	A.6 Abuso de privilegios de acceso	M	M	M	A	A	MA	B	B	M
	A.7 Uso no previsto	M	M	M	A	A	MA	B	B	M
	A.18 Destrucción de información	M	M	M	A	A	MA	B	B	M
	A.24 Denegación de servicio	M	M	M	A	A	MA	B	B	M

Fuente: Elaborador por el investigador

Tabla 3.13 Impacto en activos Software

ACTIVO	AMENAZA	VALOR DEL ACTIVO			DEGRADACION			IMPACTO		
		C	I	D	C	I	D	C	I	D
SW-std-os01	I.5Avería de origen físico o lógico	-	M	M	-	M	MA	-	MB	M
	E.1 Errores de los usuarios	-	M	M	-	M	A	-	MB	B
	E.2 Errores del administrador	-	M	M	-	A	MA	-	B	M
	E.8 Difusión de software dañino	-	M	M	-	A	MA	-	B	M
	E.18 Destrucción de información	-	M	M	-	M	MA	-	MB	M
	A.6 Abuso de privilegios de acceso	-	M	M	-	M	MA	-	MB	M

	A.7 Uso no previsto	-	M	M	-	M	A	-	MB	MB
	A.8 Difusión de software dañino	-	M	M	-	A	MA	-	B	M
	A.18 Destrucción de información	-	M	M	-	A	MA	-	B	M
	A.22 Manipulación de programas	-	M	M	-	A	MA	-	B	M
SW-std-os02	I.5Avería de origen físico o lógico	-	M	M	-	M	MA	-	MB	M
	E.1 Errores de los usuarios	-	M	M	-	M	A	-	MB	B
	E.2 Errores del administrador	-	M	M	-	A	MA	-	B	M
	E.8 Difusión de software dañino	-	M	M	-	M	MA	-	MB	M
	E.18 Destrucción de información	-	M	M	-	A	MA	-	B	M
	A.6 Abuso de privilegios de acceso	-	M	M	-	A	MA	-	B	M
	A.7 Uso no previsto	-	M	M	-	M	A	-	MB	B
	A.8 Difusión de software dañino	-	M	M	-	A	MA	-	B	M
	A.18 Destrucción de información	-	M	M	-	A	MA	-	B	M
	A.22 Manipulación de programas	-	M	M	-	A	MA	-	B	M
SW-std-os03	I.5Avería de origen físico o lógico	-	A	A	-	M	MA	-	B	A
	E.1 Errores de los usuarios	-	A	A	-	M	A	-	B	M
	E.2 Errores del administrador	-	A	A	-	A	A	-	M	M
	E.8 Difusión de software dañino	-	A	A	-	M	MA	-	B	A
	E.18 Destrucción de información	-	A	A	-	M	MA	-	B	A
	A.6 Abuso de privilegios de acceso	-	A	A	-	A	MA	-	M	A
	A.7 Uso no previsto	-	A	A	-	A	A	-	M	M
	A.8 Difusión de software dañino	-	A	A	-	A	MA	-	M	A
	A.18 Destrucción de información	-	A	A	-	A	MA	-	M	A
	A.22 Manipulación de programas	-	A	A	-	A	MA	-	M	A
SW-std-os04	I.5Avería de origen físico o lógico	-	A	A	-	M	MA	-	B	A
	E.1 Errores de los usuarios	-	A	A	-	M	A	-	B	M
	E.2 Errores del administrador	-	A	A	-	A	A	-	M	M

	E.8 Difusión de software dañino	-	A	A	-	M	MA	-	B	A
	E.18 Destrucción de información	-	A	A	-	M	MA	-	B	A
	A.6 Abuso de privilegios de acceso	-	A	A	-	A	MA	-	B	A
	A.7 Uso no previsto	-	A	A	-	A	A	-	B	M
	A.8 Difusión de software dañino	-	A	A	-	A	MA	-	B	A
	A.18 Destrucción de información	-	A	A	-	A	MA	-	B	A
	A.22 Manipulación de programas	-	A	A	-	A	MA	-	B	A
SW-std-os05	I.5Avería de origen físico o lógico	-	M	M	-	M	MA	-	MB	M
	E.1 Errores de los usuarios	-	M	M	-	M	A	-	MB	B
	E.2 Errores del administrador	-	M	M	-	A	A	-	B	B
	E.8 Difusión de software dañino	-	M	M	-	M	MA	-	MB	M
	E.18 Destrucción de información	-	M	M	-	M	MA	-	MB	M
	A.6 Abuso de privilegios de acceso	-	M	M	-	M	MA	-	MB	M
	A.7 Uso no previsto	-	M	M	-	M	A	-	MB	B
	A.8 Difusión de software dañino	-	M	M	-	A	MA	-	B	M
	A.18 Destrucción de información	-	M	M	-	A	MA	-	B	M
	A.22 Manipulación de programas	-	M	M	-	A	MA	-	B	M
SW-std-os06	I.5Avería de origen físico o lógico	-	M	M	-	M	MA	-	MB	M
	E.1 Errores de los usuarios	-	M	M	-	M	A	-	MB	B
	E.2 Errores del administrador	-	M	M	-	A	MA	-	B	M
	E.8 Difusión de software dañino	-	M	M	-	M	MA	-	MB	M
	E.18 Destrucción de información	-	M	M	-	M	MA	-	MB	M
	A.6 Abuso de privilegios de acceso	-	M	M	-	M	MA	-	MB	M
	A.7 Uso no previsto	-	M	M	-	M	MA	-	MB	M
	A.8 Difusión de software dañino	-	M	M	-	A	MA	-	B	M
	A.18 Destrucción de información	-	M	M	-	A	MA	-	B	M

	A.22 Manipulación de programas	-	M	M	-	A	MA	-	B	M
SW-std-os07	I.5Avería de origen físico o lógico	-	M	M	-	M	MA	-	MB	M
	E.1 Errores de los usuarios	-	M	M	-	M	A	-	MB	B
	E.2 Errores del administrador	-	M	M	-	A	A	-	B	B
	E.8 Difusión de software dañino	-	M	M	-	M	MA	-	MB	M
	E.18 Destrucción de información	-	M	M	-	M	MA	-	MB	M
	A.6 Abuso de privilegios de acceso	-	M	M	-	A	MA	-	B	M
	A.7 Uso no previsto	-	M	M	-	A	A	-	B	B
	A.8 Difusión de software dañino	-	M	M	-	A	MA	-	B	M
	A.18 Destrucción de información	-	M	M	-	A	MA	-	B	M
	A.22 Manipulación de programas	-	M	M	-	A	MA	-	B	M
W-std-os08	I.5Avería de origen físico o lógico	-	M	M	-	M	MA	-	MB	M
	E.1 Errores de los usuarios	-	M	M	-	A	A	-	B	B
	E.2 Errores del administrador	-	M	M	-	A	A	-	B	B
	E.8 Difusión de software dañino	-	M	M	-	M	MA	-	MB	M
	E.18 Destrucción de información	-	M	M	-	M	MA	-	MB	M
	A.6 Abuso de privilegios de acceso	-	M	M	-	A	MA	-	B	M
	A.7 Uso no previsto	-	M	M	-	A	A	-	B	B
	A.8 Difusión de software dañino	-	M	M	-	A	MA	-	B	M
	A.18 Destrucción de información	-	M	M	-	A	MA	-	B	M
	A.22 Manipulación de programas	-	M	M	-	A	MA	-	B	M
SW-std-os09	I.5Avería de origen físico o lógico	-	M	M	-	M	MA	-	MB	M
	E.1 Errores de los usuarios	-	M	M	-	A	A	-	B	B
	E.2 Errores del administrador	-	M	M	-	A	A	-	B	B
	E.8 Difusión de software dañino	-	M	M	-	M	MA	-	MB	M
	E.18 Destrucción de información	-	M	M	-	A	MA	-	B	M
	A.6 Abuso de privilegios de acceso	-	M	M	-	A	MA	-	B	M

	A.7 Uso no previsto	-	M	M	-	A	A	-	B	B
	A.8 Difusión de software dañino	-	M	M	-	A	MA	-	B	M
	A.18 Destrucción de información	-	M	M	-	A	MA	-	B	M
	A.22 Manipulación de programas	-	M	M	-	A	MA	-	B	M
SW-std-os10	I.5Avería de origen físico o lógico	-	M	M	-	M	MA	-	MB	M
	E.1 Errores de los usuarios	-	M	M	-	M	A	-	MB	B
	E.2 Errores del administrador	-	M	M	-	A	A	-	B	B
	E.8 Difusión de software dañino	-	M	M	-	M	MA	-	MB	M
	E.18 Destrucción de información	-	M	M	-	A	MA	-	B	M
	A.6 Abuso de privilegios de acceso	-	M	M	-	A	MA	-	B	M
	A.7 Uso no previsto	-	M	M	-	A	A	-	B	B
	A.8 Difusión de software dañino	-	M	M	-	A	MA	-	B	M
	A.18 Destrucción de información	-	M	M	-	A	MA	-	B	M
	A.22 Manipulación de programas	-	M	M	-	A	MA	-	B	M
SW-std-1	I.5Avería de origen físico o lógico	-	M	M	-	M	MA	-	MB	M
	E.1 Errores de los usuarios	-	M	M	-	M	MA	-	MB	M
	E.2 Errores del administrador	-	M	M	-	A	MA	-	B	M
	E.8 Difusión de software dañino	-	M	M	-	A	MA	-	B	M
	E.18 Destrucción de información	-	M	M	-	A	MA	-	B	M
	E.20 Vulnerabilidades de los programas (software)	-	M	M	-	A	MA	-	B	M
	E.21 Errores de mantenimiento/actualización de programas(software)	-	M	M	-	A	MA	-	B	M
	A.6 Abuso de privilegios de acceso	-	M	M	-	A	MA	-	B	M
	A.7 Uso no previsto	-	M	M	-	A	A	-	B	B
	A.8 Difusión de software dañino	-	M	M	-	A	MA	-	B	M
	A.18 Destrucción de información	-	M	M	-	A	MA	-	B	M
	A.22 Manipulación de programas	-	M	M	-	A	MA	-	B	M

SW-std-dbm01	I.5Avería de origen físico o lógico	M	M	M	A	A	MA	B	B	M
	E.1 Errores de los usuarios	M	M	M	A	A	MA	B	B	M
	E.2 Errores del administrador	M	M	M	A	A	MA	B	B	M
	E.8 Difusión de software dañino	M	M	M	A	A	MA	B	B	M
	E.18 Destrucción de información	M	M	M	A	A	MA	B	B	M
	E.20 Vulnerabilidades de los programas (software)	M	M	M	A	A	MA	B	B	M
	E.21 Errores de mantenimiento/actualización de programas(software)	M	M	M	A	A	MA	B	B	M
	A.6 Abuso de privilegios de acceso	M	M	M	A	A	MA	B	B	M
	A.7 Uso no previsto	M	M	M	A	A	MA	B	B	M
	A.8 Difusión de software dañino	M	M	M	A	A	MA	B	B	M
	A.18 Destrucción de información	M	M	M	A	A	MA	B	B	M
	A.22 Manipulación de programas	M	M	M	A	A	MA	B	B	M
SW-std-dbms02	I.5Avería de origen físico o lógico	A	A	A	A	A	MA	M	M	A
	E.1 Errores de los usuarios	A	A	A	A	A	MA	M	M	A
	E.2 Errores del administrador	A	A	A	A	A	MA	M	M	A
	E.8 Difusión de software dañino	A	A	A	A	A	MA	M	M	A
	E.18 Destrucción de información	A	A	A	A	A	MA	M	M	A
	E.20 Vulnerabilidades de los programas (software)	A	A	A	A	A	MA	M	M	A
	E.21 Errores de mantenimiento/actualización de programas(software)	A	A	A	A	A	MA	M	M	A
	A.6 Abuso de privilegios de acceso	A	A	A	A	A	MA	M	M	A
	A.7 Uso no previsto	A	A	A	A	A	MA	M	M	A
	A.8 Difusión de software dañino	A	A	A	A	A	MA	M	M	A
	A.18 Destrucción de información	A	A	A	A	A	MA	M	M	A
	A.22 Manipulación de programas	A	A	A	A	A	MA	M	M	A
SW-std-2	I.5Avería de origen físico o lógico	-	M	M	-	A	MA	-	B	M
	E.1 Errores de los usuarios	-	M	M	-	M	A	-	MB	B

	E.2 Errores del administrador	-	M	M	-	M	MA	-	MB	M
	E.8 Difusión de software dañino	-	M	M	-	M	MA	-	MB	M
	E.18 Destrucción de información	-	M	M	-	M	A	-	MB	B
	E.20 Vulnerabilidades de los programas (software)	-	M	M	-	M	A	-	MB	B
	E.21 Errores de mantenimiento/actualización de programas(software)	-	M	M	-	M	A	-	MB	B
	A.6 Abuso de privilegios de acceso	-	M	M	-	A	MA	-	B	M
	A.7 Uso no previsto	-	M	M	-	A	MA	-	B	M
	A.8 Difusión de software dañino	-	M	M	-	A	MA	-	B	M
	A.18 Destrucción de información	-	M	M	-	A	MA	-	B	M
	A.22 Manipulación de programas	-	M	M	-	A	MA	-	B	M
SW-std-3	I.5Avería de origen físico o lógico	-	M	M	-	A	MA	-	B	M
	E.1 Errores de los usuarios	-	M	M	-	M	A	-	MB	B
	E.2 Errores del administrador	-	M	M	-	M	MA	-	MB	M
	E.8 Difusión de software dañino	-	M	M	-	M	MA	-	MB	M
	E.18 Destrucción de información	-	M	M	-	M	A	-	MB	B
	E.20 Vulnerabilidades de los programas (software)	-	M	M	-	M	A	-	MB	B
	E.21 Errores de mantenimiento/actualización de programas(software)	-	M	M	-	M	A	-	MB	B
	A.6 Abuso de privilegios de acceso	-	M	M	-	A	MA	-	B	M
	A.7 Uso no previsto	-	M	M	-	A	MA	-	B	M
	A.8 Difusión de software dañino	-	M	M	-	A	MA	-	B	M
	A.18 Destrucción de información	-	M	M	-	A	MA	-	B	M
	A.22 Manipulación de programas	-	M	M	-	A	MA	-	B	M
SW-std-4	I.5Avería de origen físico o lógico	-	M	M	-	A	MA	-	B	M
	E.1 Errores de los usuarios	-	M	M	-	M	A	-	MB	B
	E.2 Errores del administrador	-	M	M	-	M	MA	-	MB	M

	E.8 Difusión de software dañino	-	M	M	-	M	MA	-	MB	M
	E.18 Destrucción de información	-	M	M	-	M	A	-	MB	B
	E.20 Vulnerabilidades de los programas (software)	-	M	M	-	M	A	-	MB	B
	E.21 Errores de mantenimiento/actualización de programas(software)	-	M	M	-	M	A	-	MB	B
	A.6 Abuso de privilegios de acceso	-	M	M	-	A	MA	-	B	M
	A.7 Uso no previsto	-	M	M	-	A	MA	-	B	M
	A.8 Difusión de software dañino	-	M	M	-	A	MA	-	B	M
	A.18 Destrucción de información	-	M	M	-	A	MA	-	B	M
	A.22 Manipulación de programas	-	M	M	-	A	MA	-	B	M
SW-std-5	I.5Avería de origen físico o lógico	-	A	A	-	A	MA	-	M	A
	E.1 Errores de los usuarios	-	A	A	-	A	A	-	M	M
	E.2 Errores del administrador	-	A	A	-	A	MA	-	M	A
	E.8 Difusión de software dañino	-	A	A	-	A	MA	-	M	A
	E.18 Destrucción de información	-	A	A	-	A	MA	-	M	A
	E.20 Vulnerabilidades de los programas (software)	-	A	A	-	A	MA	-	M	A
	E.21 Errores de mantenimiento/actualización de programas(software)	-	A	A	-	A	MA	-	M	A
	A.6 Abuso de privilegios de acceso	-	A	A	-	A	MA	-	M	A
	A.7 Uso no previsto	-	A	A	-	A	MA	-	M	A
	A.8 Difusión de software dañino	-	A	A	-	A	MA	-	M	A
	A.18 Destrucción de información	-	A	A	-	A	MA	-	M	A
	A.22 Manipulación de programas	-	A	A	-	A	MA	-	M	A
SW-std-6	I.5Avería de origen físico o lógico	M	A	A	A	A	MA	B	M	A
	E.1 Errores de los usuarios	M	A	A	M	M	A	MB	B	M
	E.2 Errores del administrador	M	A	A	A	A	MA	B	M	A
	E.8 Difusión de software dañino	M	A	A	A	A	MA	B	M	A

	E.18 Destrucción de información	M	A	A	A	A	MA	B	M	A
	E.20 Vulnerabilidades de los programas (software)	M	A	A	A	A	MA	B	M	A
	E.21 Errores de mantenimiento/actualización de programas(software)	M	A	A	A	A	MA	B	M	A
	A.6 Abuso de privilegios de acceso	M	A	A	A	A	MA	B	M	A
	A.7 Uso no previsto	M	A	A	M	A	MA	MB	M	A
	A.8 Difusión de software dañino	M	A	A	A	A	MA	B	M	A
	A.18 Destrucción de información	M	A	A	A	A	MA	B	M	A
	A.22 Manipulación de programas	M	A	A	A	A	MA	B	M	A
SW-std-7	I.5Avería de origen físico o lógico	M	A	A	A	A	MA	B	M	A
	E.1 Errores de los usuarios	M	A	A	M	M	A	MB	B	M
	E.2 Errores del administrador	M	A	A	A	A	MA	B	M	A
	E.8 Difusión de software dañino	M	A	A	A	A	MA	B	M	A
	E.18 Destrucción de información	M	A	A	A	A	MA	B	M	A
	E.20 Vulnerabilidades de los programas (software)	M	A	A	A	A	MA	B	M	A
	E.21 Errores de mantenimiento/actualización de programas(software)	M	A	A	A	A	MA	B	M	A
	A.6 Abuso de privilegios de acceso	M	A	A	A	A	MA	B	M	A
	A.7 Uso no previsto	M	A	A	M	A	MA	MB	M	A
	A.8 Difusión de software dañino	M	A	A	A	A	MA	B	M	A
	A.18 Destrucción de información	M	A	A	A	A	MA	B	M	A
	A.22 Manipulación de programas	M	A	A	A	A	MA	B	M	A
SW-std-8	I.5Avería de origen físico o lógico	M	A	A	A	A	MA	B	M	A
	E.1 Errores de los usuarios	M	A	A	M	M	MA	MB	B	A
	E.2 Errores del administrador	M	A	A	A	A	MA	B	M	A
	E.8 Difusión de software dañino	M	A	A	M	A	MA	MB	M	A
	E.18 Destrucción de información	M	A	A	A	A	MA	B	M	A

	E.20 Vulnerabilidades de los programas (software)	M	A	A	M	A	MA	MB	M	A
	E.21 Errores de mantenimiento/actualización de programas(software)	M	A	A	M	A	MA	MB	M	A
	A.6 Abuso de privilegios de acceso	M	A	A	A	A	MA	B	M	A
	A.7 Uso no previsto	M	A	A	A	A	MA	B	M	A
	A.8 Difusión de software dañino	M	A	A	A	A	MA	B	M	A
	A.18 Destrucción de información	M	A	A	A	A	MA	B	M	A
	A.22 Manipulación de programas	M	A	A	A	A	MA	B	M	A
SW-std-9	I.5Avería de origen físico o lógico	M	A	A	A	A	MA	B	M	A
	E.1 Errores de los usuarios	M	A	A	M	M	MA	MB	B	A
	E.2 Errores del administrador	M	A	A	A	A	MA	B	M	A
	E.8 Difusión de software dañino	M	A	A	M	A	MA	MB	M	A
	E.18 Destrucción de información	M	A	A	A	A	MA	B	M	A
	E.20 Vulnerabilidades de los programas (software)	M	A	A	M	A	MA	MB	M	A
	E.21 Errores de mantenimiento/actualización de programas(software)	M	A	A	M	A	MA	MB	M	A
	A.6 Abuso de privilegios de acceso	M	A	A	A	A	MA	B	M	A
	A.7 Uso no previsto	M	A	A	A	A	MA	B	M	A
	A.8 Difusión de software dañino	M	A	A	A	A	MA	B	M	A
	A.18 Destrucción de información	M	A	A	A	A	MA	B	M	A
	A.22 Manipulación de programas	M	A	A	A	A	MA	B	M	A

Fuente: Elaborador por el investigador

Tabla 3.14 Impacto en activos Hardware

ACTIVO	AMENAZAS	VALOR DEL ACTIVO			DEGRADACIÓN			IMPACTO		
		C	I	D	C	I	D	C	I	D
HW-host01	N.1 Fuego	M	A	A	M	M	MA	MB	B	A
	N.2 Daños de Agua	M	A	A	M	M	MA	MB	B	A
	N.7 Fenómeno Sísmico	M	A	A	M	M	MA	MB	B	A
	N.8 Fenómenos de Origen Volcánico	M	A	A	M	M	M	MB	B	B
	I.1 Fuego	M	A	A	M	M	MA	MB	B	A
	I.2 Daños por agua	M	A	A	M	M	MA	MB	B	A
	I.3 Contaminación mecánica	M	A	A	M	M	M	MB	B	B
	I.5 Avería de origen físico o lógico	M	A	A	A	A	MA	B	M	M
	I.6 Corte de suministro eléctrico	M	A	A	M	M	MA	MB	B	A
	I.7 Condiciones inadecuadas de temperatura o humedad	M	A	A	M	M	M	MB	B	B
	E.2 Errores del administrador	M	A	A	M	A	MA	MB	B	M
	E.23 Errores de mantenimiento/actualización de equipos (hardware)	M	A	A	A	A	MA	B	M	A
	E.24Caída del sistema por agotamiento de recursos	M	A	A	A	A	MA	B	M	A
	A.6Abuso de privilegios de acceso	M	A	A	A	A	MA	B	M	A
	A.7 Uso no previsto	M	A	A	M	A	MA	MB	B	M
	A.24 Denegación de servicio	M	A	A	A	A	MA	B	M	A
	A.25 Robo	M	A	A	A	A	MA	B	M	A
	A.26 Ataque destructivo	M	A	A	A	A	MA	B	M	A
HW-host02	N.1 Fuego	A	A	A	A	A	MA	A	M	A
	N.2 Daños de Agua	A	A	A	A	A	MA	M	M	A
	N.7 Fenómeno Sísmico	A	A	A	A	A	MA	M	M	A
	N.8 Fenómenos de Origen Volcánico	A	A	A	M	M	M	B	B	B
	I.1 Fuego	A	A	A	M	M	MA	B	B	A
	I.2 Daños por agua	A	A	A	M	M	MA	B	B	A

	I.3 Contaminación mecánica	A	A	A	M	M	M	B	B	B
	I.5 Avería de origen físico o lógico	A	A	A	A	A	MA	M	M	A
	I.6 Corte de suministro eléctrico	A	A	A	M	M	MA	B	B	A
	I.7 Condiciones inadecuadas de temperatura o humedad	A	A	A	M	M	M	B	B	B
	E.2 Errores del administrador	A	A	A	M	A	MA	B	B	A
	E.23 Errores de mantenimiento/actualización de equipos (hardware)	A	A	A	A	A	MA	M	M	A
	E.24 Caída del sistema por agotamiento de recursos	A	A	A	A	A	MA	M	M	A
	A.6Abuso de privilegios de acceso	A	A	A	A	A	MA	M	M	A
	A.7 Uso no previsto	A	A	A	M	A	MA	B	M	A
	A.24 Denegación de servicio	A	A	A	A	A	MA	M	M	A
	A.25 Robo	A	A	A	A	A	MA	M	M	A
	A.26 Ataque destructivo	A	A	A	A	A	MA	M	M	A
HW-host03	N.1 Fuego	M	M	M	M	M	MA	MB	MB	MB
	N.2 Daños de Agua	M	M	M	M	M	MA	MB	MB	M
	N.7 Fenómeno Sísmico	M	M	M	M	M	MA	MB	MB	M
	N.8 Fenómenos de Origen Volcánico	M	M	M	M	M	M	MB	MB	MB
	I.1 Fuego	M	M	M	M	M	MA	MB	MB	M
	I.2 Daños por agua	M	M	M	M	M	MA	MB	MB	M
	I.3 Contaminación mecánica	M	M	M	M	M	M	MB	MB	MB
	I.5 Avería de origen físico o lógico	M	M	M	A	A	MA	B	B	M
	I.6 Corte de suministro eléctrico	M	M	M	M	M	MA	MB	MB	M
	I.7 Condiciones inadecuadas de temperatura o humedad	M	M	M	M	M	M	MB	MB	MB
	E.2 Errores del administrador	M	M	M	M	A	MA	MB	MB	M

	E.23 Errores de mantenimiento/actualización de equipos (hardware)	M	M	M	A	A	MA	MB	MB	B
	E.24 Caída del sistema por agotamiento de recursos	M	M	M	A	A	MA	B	B	M
	A.6Abuso de privilegios de acceso	M	M	M	A	A	MA	B	B	M
	A.7 Uso no previsto	M	M	M	M	A	MA	MB	MB	M
	A.24 Denegación de servicio	M	M	M	A	A	MA	B	B	M
	A.25 Robo	M	M	M	A	A	MA	B	B	M
	A.26 Ataque destructivo	M	M	M	A	A	MA	B	B	M
HW-host04	N.1 Fuego	M	M	M	M	M	MA	MB	MB	M
	N.2 Daños de Agua	M	M	M	M	M	MA	MB	MB	M
	N.7 Fenómeno Sísmico	M	M	M	M	M	MA	MB	MB	M
	N.8 Fenómenos de Origen Volcánico	M	M	M	M	M	M	MB	MB	MB
	I.1 Fuego	M	M	M	M	M	MA	MB	MB	M
	I.2 Daños por agua	M	M	M	M	M	MA	MB	MB	M
	I.3 Contaminación mecánica	M	M	M	M	M	M	MB	MB	MB
	I.5 Avería de origen físico o lógico	M	M	M	A	A	MA	MB	B	M
	I.6 Corte de suministro eléctrico	M	M	M	M	M	MA	MB	MB	M
	I.7 Condiciones inadecuadas de temperatura o humedad	M	M	M	M	M	M	MB	MB	MB
	E.2 Errores del administrador	M	M	M	M	A	MA	MB	B	M
	E.23 Errores de mantenimiento/actualización de equipos (hardware)	M	M	M	A	A	MA	B	B	M
	E.24 Caída del sistema por agotamiento de recursos	M	M	M	A	A	MA	B	B	M
	A.6Abuso de privilegios de acceso	M	M	M	A	A	MA	B	B	M
	A.7 Uso no previsto	M	M	M	M	A	MA	MB	B	M
	A.24 Denegación de servicio	M	M	M	A	A	MA	B	B	M
	A.25 Robo	M	M	M	A	A	MA	B	B	M
	A.26 Ataque destructivo	M	M	M	M	A	MA	MB	B	M

HW-switch01	N.1 Fuego	M	A	A	M	M	MA	MB	B	A
	N.2 Daños de Agua	M	A	A	M	M	MA	MB	B	A
	N.7 Fenómeno Sísmico	M	A	A	M	M	MA	MB	B	A
	N.8 Fenómenos de Origen Volcánico	M	A	A	M	M	M	MB	B	B
	I.1 Fuego	M	A	A	M	M	MA	MB	B	A
	I.2 Daños por agua	M	A	A	M	M	MA	MB	B	A
	I.3 Contaminación mecánica	M	A	A	M	M	M	MB	B	B
	I.5 Avería de origen físico o lógico	M	A	A	A	A	MA	B	M	A
	I.6 Corte de suministro eléctrico	M	A	A	M	M	MA	MB	B	A
	I.7 Condiciones inadecuadas de temperatura o humedad	M	A	A	M	M	M	MB	B	B
	E.2 Errores del administrador	M	M	M	M	A	MA	MB	B	A
	E.23 Errores de mantenimiento/actualización de equipos (hardware)	M	A	A	A	A	MA	B	M	A
	E.24 Caída del sistema por agotamiento de recursos	M	A	A	A	A	MA	B	M	A
	A.6Abuso de privilegios de acceso	M	A	A	A	A	MA	B	M	A
	A.7 Uso no previsto	M	A	A	M	A	MA	MB	M	A
	A.24 Denegación de servicio	M	A	A	A	A	MA	B	M	A
	A.25 Robo	M	A	A	A	A	MA	B	M	A
	A.26 Ataque destructivo	M	A	A	A	A	MA	B	M	A
HW-firewall01	N.1 Fuego	M	A	A	M	M	MA	MB	B	A
	N.2 Daños de Agua	M	A	A	M	M	MA	MB	B	A
	N.7 Fenómeno Sísmico	M	A	A	M	M	MA	MB	B	B
	N.8 Fenómenos de Origen Volcánico	M	A	A	M	M	MA	MB	B	A
	I.1 Fuego	M	A	A	M	M	MA	MB	B	A
	I.2 Daños por agua	M	A	A	M	M	MA	MB	B	A
	I.3 Contaminación mecánica	M	A	A	M	M	MA	MB	B	A
	I.5 Avería de origen físico o lógico	M	A	A	A	A	MA	B	M	A
	I.6 Corte de suministro eléctrico	M	A	A	M	M	MA	MB	B	A

	I.7 Condiciones inadecuadas de temperatura o humedad	M	A	A	M	M	M	MB	B	B
	E.2 Errores del administrador	M	A	A	M	A	MA	MB	M	A
	E.23 Errores de mantenimiento/actualización de equipos (hardware)	M	A	A	A	A	MA	B	M	A
	E.24 Caída del sistema por agotamiento de recursos	M	A	A	A	A	MA	B	M	A
	A.6Abuso de privilegios de acceso	M	A	A	M	M	M	MB	B	B
	A.7 Uso no previsto	M	A	A	A	A	MA	B	M	A
	A.24 Denegación de servicio	M	A	A	M	M	MA	MB	B	A
	A.25 Robo	M	A	A	A	A	A	M	M	M
	A.26 Ataque destructivo	M	A	A	M	M	MA	MB	B	A
HW-switch02	N.1 Fuego	M	A	A	M	M	MA	MB	B	A
	N.2 Daños de Agua	M	A	A	M	M	MA	MB	B	A
	N.7 Fenómeno Sísmico	M	A	A	M	M	MA	MB	B	M
	N.8 Fenómenos de Origen Volcánico	M	A	A	M	M	M	MB	B	B
	I.1 Fuego	M	A	A	M	M	MA	MB	B	A
	I.2 Daños por agua	M	A	A	M	M	MA	MB	B	A
	I.3 Contaminación mecánica	M	A	A	M	M	M	MB	B	B
	I.5 Avería de origen físico o lógico	M	A	A	A	A	MA	B	M	M
	I.6 Corte de suministro eléctrico	M	A	A	M	M	MA	MB	B	B
	I.7 Condiciones inadecuadas de temperatura o humedad	M	A	A	M	M	M	MB	B	B
	E.2 Errores del administrador	M	A	A	M	A	MA	MB	M	A
	E.23 Errores de mantenimiento/actualización de equipos (hardware)	M	A	A	A	A	MA	B	M	A
	E.24 Caída del sistema por agotamiento de recursos	M	A	A	A	A	MA	B	M	A
	A.6Abuso de privilegios de acceso	M	A	A	A	A	MA	B	M	A
	A.7 Uso no previsto	M	A	A	M	A	MA	MB	M	A

	A.24 Denegación de servicio	M	A	A	A	A	MA	B	M	A
	A.25 Robo	M	A	A	A	A	MA	B	M	A
	A.26 Ataque destructivo	M	A	A	A	A	MA	B	M	A
HW-firewall02	N.1 Fuego	M	A	A	M	M	MA	MB	B	A
	N.2 Daños de Agua	M	A	A	M	M	MA	MB	B	A
	N.7 Fenómeno Sísmico	M	A	A	M	M	MA	MB	B	A
	N.8 Fenómenos de Origen Volcánico	M	A	A	M	M	M	MB	B	B
	I.1 Fuego	M	A	A	M	M	MA	MB	B	A
	I.2 Daños por agua	M	A	A	M	M	MA	MB	MB	A
	I.3 Contaminación mecánica	M	A	A	M	M	M	MB	B	B
	I.5 Avería de origen físico o lógico	M	A	A	A	A	MA	B	M	A
	I.6 Corte de suministro eléctrico	M	A	A	M	M	MA	MB	B	A
	I.7 Condiciones inadecuadas de temperatura o humedad	M	A	A	M	M	M	MB	B	B
	E.2 Errores del administrador	M	A	A	M	A	MA	MB	M	A
	E.23 Errores de mantenimiento/actualización de equipos (hardware)	M	A	A	A	A	MA	B	M	A
	E.24 Caída del sistema por agotamiento de recursos	M	A	A	A	A	MA	B	M	A
	A.6Abuso de privilegios de acceso	M	A	A	M	M	M	MB	B	B
	A.7 Uso no previsto	M	A	A	A	A	MA	B	M	A
	A.24 Denegación de servicio	M	A	A	M	M	MA	MB	B	A
	A.25 Robo	M	A	A	M	M	M	MB	B	B
	A.26 Ataque destructivo	M	A	A	M	M	MA	MB	B	A

Fuente: Elaborado por el investigador

Tabla 3.15 Impacto en activos Datos

ACTIVO	AMENAZAS	VALOR DEL ACTIVO			DEGRADACIÓN			IMPACTO		
		C	I	D	C	I	D	C	I	D
D-conf01	E.1 Errores de los usuarios	MA	MA	MA	A	A	MA	A	A	MA
	E.2 Errores del administrador	MA	MA	MA	A	A	MA	A	A	MA
	E.18 Destrucción de información	MA	MA	MA	A	A	MA	A	A	MA
	A.4 Manipulación de la configuración	MA	MA	MA	A	A	MA	A	A	MA
	D.log registros de actividad									
	A.6 Abuso de privilegios de acceso	MA	MA	MA	A	A	MA	A	A	MA
	A.18 Destrucción de información	MA	MA	MA	A	A	MA	A	A	MA
D-conf02	E.1 Errores de los usuarios	MA	MA	MA	A	A	MA	A	A	MA
	E.2 Errores del administrador	MA	MA	MA	A	A	MA	A	A	MA
	E.18 Destrucción de información	MA	MA	MA	A	A	MA	A	A	MA
	A.4 Manipulación de la configuración	MA	MA	MA	A	A	MA	A	A	MA
	D.log registros de actividad									
	A.6 Abuso de privilegios de acceso	MA	MA	MA	A	A	MA	A	A	MA
	A.18 Destrucción de información	MA	MA	MA	A	A	MA	A	A	MA
D-Conf03	E.1 Errores de los usuarios	MA	MA	MA	A	A	MA	A	A	MA
	E.2 Errores del administrador	MA	MA	MA	A	A	MA	A	A	MA
	E.18 Destrucción de información	MA	MA	MA	A	A	MA	A	A	MA
	A.4 Manipulación de la configuración	MA	MA	MA	A	A	MA	A	A	MA
	D.log registros de actividad									
	A.6 Abuso de privilegios de acceso	MA	MA	MA	A	A	MA	A	A	MA
	A.18 Destrucción de información	MA	MA	MA	A	A	MA	A	A	MA

Fuente: Elaborador por el investigador

Tabla 46Tabla 3.16 Impacto en activo Redes de Comunicación

ACTIVO	AMENAZAS	VALOR DEL ACTIVO			DEGRADACIÓN			IMPACTO		
		C	I	D	C	I	D	C	I	D
COM-internet01	I.8 Fallo de servicios de comunicaciones	MA	MA	MA	A	A	MA	A	A	MA
	E.2 Errores del administrador	MA	MA	MA	M	A	MA	M	A	MA
	E.18 Destrucción de información	MA	MA	MA	A	A	MA	A	A	MA
	E.24 Caída del sistema por agotamiento de recursos	MA	MA	MA	A	A	MA	A	A	MA
	A.6 Abuso de privilegio de acceso	MA	MA	MA	A	A	MA	A	A	MA
	A.7 Uso no previsto	MA	MA	MA	A	A	MA	A	A	MA
	A.24 Denegación de servicio	MA	MA	MA	A	A	MA	A	A	MA
COM-internet01	I.8 Fallo de servicios de comunicaciones	MA	MA	MA	A	A	MA	A	A	MA
	E.2 Errores del administrador	MA	MA	MA	M	A	MA	M	A	MA
	E.18 Destrucción de información	MA	MA	MA	A	A	MA	A	A	MA
	E.24 Caída del sistema por agotamiento de recursos	MA	MA	MA	A	A	MA	A	A	MA
	A.6 Abuso de privilegio de acceso	MA	MA	MA	A	A	MA	A	A	MA
	A.7 Uso no previsto	MA	MA	MA	A	A	MA	A	A	MA
	A.24 Denegación de servicio	MA	MA	MA	A	A	MA	A	A	MA

Fuente: Elaborador por el investigador

3.1.11.3 Matriz de Análisis de Riesgos

Para el análisis de riesgos, se realiza mediante la tabla 2.30 (Riesgo en función del impacto y la probabilidad). El riesgo se identifica por medio de los niveles MA (Muy Alto), A (Alto), M (Medio), B (Bajo) y MB (Muy Bajo), considerando prioridad los riesgos con el nivel MA, lo cuales necesitan un mayor cuidado.

Tabla 3.17 Riesgo en Servicios

ACTIVO	AMENAZA	IMPACTO			PROBABILIDAD			RIESGO		
		C	I	D	C	I	D	C	I	D
Spub01	E.1 Errores de los usuarios	-	MB	B	-	B	M	-	MB	B
	E.2 Errores del administrador	-	MB	M	-	M	M	-	MB	M
	E.18 Destrucción de información	-	MB	M	-	B	M	-	MB	M
	E.19 Fugas de información	-	MB	M	-	B	M	-	MB	A
	E.24 Caída del sistema por agotamiento de recursos	-	MB	M	-	M	M	-	MB	A
	A.6 Abuso de privilegios de acceso	-	MB	M	-	M	M	-	MB	M
	A.7 Uso no previsto	-	MB	B	-	B	B	-	MB	B
	A.18 Destrucción de información	-	B	M	-	M	M	-	B	M
	A.24 Denegación de servicio	-	MB	M	-	A	A	-	B	A
Spub02	E.1 Errores de los usuarios	-	MB	B	-	B	M	-	MB	B
	E.2 Errores del administrador	-	MB	M	-	M	M	-	MB	M
	E.18 Destrucción de información	-	MB	M	-	B	M	-	MB	M
	E.19 Fugas de información	-	MB	M	-	B	M	-	MB	M
	E.24 Caída del sistema por agotamiento de recursos	-	MB	M	-	M	M	-	MB	A
	A.6 Abuso de privilegios de acceso	-	MB	M	-	M	M	-	MB	M
	A.7 Uso no previsto	-	MB	B	-	B	B	-	MB	B
	A.18 Destrucción de información	-	B	M	-	M	M	-	B	M
	A.24 Denegación de servicio	-	MB	M	-	A	A	-	B	A
Spub03	E.1 Errores de los usuarios	MB	MB	B	B	B	M	MB	MB	B

	E.2 Errores del administrador	MB	MB	M	B	M	M	MB	MB	M
	E.18 Destrucción de información	MB	MB	M	B	B	M	MB	MB	M
	E.19 Fugas de información	MB	MB	M	B	B	M	MB	MB	A
	E.24 Caída del sistema por agotamiento de recursos	MB	MB	M	B	M	M	MB	MB	A
	A.6 Abuso de privilegios de acceso	MB	MB	M	B	M	M	MB	MB	M
	A.7 Uso no previsto	MB	MB	MB	B	B	B	MB	MB	MB
	A.18 Destrucción de información	MB	MB	M	B	M	M	MB	MB	M
	A.24 Denegación de servicio	MB	MB	M	B	A	A	MB	B	A
Sint01	E.1 Errores de los usuarios	-	MB	B	-	M	M	-	MB	B
	E.2 Errores del administrador	-	MB	M	-	M	M	-	MB	M
	E.18 Destrucción de información	-	MB	M	-	M	M	-	MB	M
	E.19 Fugas de información	-	MB	M	-	B	B	-	MB	A
	E.24 Caída del sistema por agotamiento de recursos	-	MB	M	-	M	A	-	MB	A
	A.6 Abuso de privilegios de acceso	-	MB	M	-	M	M	-	MB	M
	A.7 Uso no previsto	-	MB	M	-	M	M	-	MB	M
	A.18 Destrucción de información	-	MB	M	-	M	A	-	MB	M
	A.24 Denegación de servicio	-	MB	M	-	A	A	-	B	A
Sint02	E.1 Errores de los usuarios	-	B	A	-	M	M	-	B	A
	E.2 Errores del administrador	-	B	A	-	M	M	-	B	A
	E.18 Destrucción de información	-	M	A	-	M	M	-	M	M
	E.19 Fugas de información	-	M	A	-	B	B	-	M	A

	E.24 Caída del sistema por agotamiento de recursos	-	B	A	-	M	A	-	B	MA
	A.6 Abuso de privilegios de acceso	-	B	A	-	M	M	-	B	A
	A.7 Uso no previsto	-	B	A	-	M	M	-	B	M
	A.18 Destrucción de información	-	M	A	-	M	A	-	M	M
	A.24 Denegación de servicio	-	B	A	-	A	A	-	M	MA
Sint03	E.1 Errores de los usuarios	-	MB	B	-	M	M	-	MB	B
	E.2 Errores del administrador	-	MB	M	-	M	M	-	MB	M
	E.18 Destrucción de información	-	MB	M	-	M	M	-	MB	M
	E.19 Fugas de información	-	MB	M	-	B	B	-	MB	A
	E.24 Caída del sistema por agotamiento de recursos	-	MB	M	-	M	A	-	MB	A
	A.6 Abuso de privilegios de acceso	-	MB	M	-	M	M	-	MB	M
	A.7 Uso no previsto	-	MB	M	-	M	M	-	MB	M
	A.18 Destrucción de información	-	MB	M	-	M	A	-	MB	M
	A.24 Denegación de servicio	-	MB	M	-	A	A	-	B	A
Sint04	E.1 Errores de los usuarios	M	M	M	M	M	M	M	M	M
	E.2 Errores del administrador	M	M	A	M	M	M	A	M	M
	E.18 Destrucción de información	M	M	A	M	M	M	M	M	M
	E.19 Fugas de información	M	M	A	B	B	B	M	M	A
	E.24 Caída del sistema por agotamiento de recursos	M	M	A	A	M	A	A	M	MA
	A.6 Abuso de privilegios de acceso	M	M	A	M	M	M	M	M	A
	A.7 Uso no previsto	M	M	A	M	M	M	M	M	A

	A.18 Destrucción de información	M	M	A	M	M	A	M	M	M
	A.24 Denegación de servicio	M	M	A	M	A	A	M	A	MA
Sint05	E.1 Errores de los usuarios	MB	M	M	M	M	M	MB	M	M
	E.2 Errores del administrador	MB	M	A	M	M	M	MB	M	M
	E.18 Destrucción de información	B	M	A	M	M	M	B	M	M
	E.19 Fugas de información	B	M	A	B	B	B	B	M	A
	E.24 Caída del sistema por agotamiento de recursos	B	M	A	M	M	A	B	M	MA
	A.6 Abuso de privilegios de acceso	B	M	A	M	M	M	B	M	A
	A.7 Uso no previsto	B	M	A	M	M	M	B	M	A
	A.18 Destrucción de información	B	M	A	A	M	A	M	M	M
	A.24 Denegación de servicio	B	M	A	M	A	A	B	A	MA
Sint06	E.1 Errores de los usuarios	MB	MB	B	M	M	M	MB	MB	B
	E.2 Errores del administrador	MB	MB	M	M	M	M	MB	MB	M
	E.18 Destrucción de información	MB	B	M	M	M	M	MB	B	M
	E.19 Fugas de información	B	B	M	B	B	B	B	B	A
	E.24 Caída del sistema por agotamiento de recursos	MB	B	M	M	M	A	MB	B	A
	A.6 Abuso de privilegios de acceso	B	B	M	M	M	M	B	B	M
	A.7 Uso no previsto	B	B	M	M	M	M	B	B	M
	A.18 Destrucción de información	B	B	M	A	M	A	M	B	M
	A.24 Denegación de servicio	B	B	M	M	A	A	B	M	A
Sint07	E.1 Errores de los usuarios	MB	MB	B	M	M	M	MB	MB	B

	E.2 Errores del administrador	MB	MB	M	M	M	M	MB	MB	M
	E.18 Destrucción de información	MB	B	M	M	M	M	MB	B	M
	E.19 Fugas de información	B	B	M	B	B	B	B	B	A
	E.24 Caída del sistema por agotamiento de recursos	MB	B	M	M	M	A	MB	B	A
	A.6 Abuso de privilegios de acceso	B	B	M	M	M	M	B	B	M
	A.7 Uso no previsto	B	B	M	M	M	M	B	B	M
	A.18 Destrucción de información	B	B	M	A	M	A	B	B	M
	A.24 Denegación de servicio	B	B	M	M	A	A	B	M	A

Fuente: Elaborado por el investigador.

Tabla 3.18 Riesgos en Software

ACTIVO	AMENAZA	IMPACTO			PROBABILIDAD			RIESGO		
		C	I	D	C	I	D	C	I	D
SW-std-os01	I.5Avería de origen físico o lógico	-	MB	M	-	M	M	-	MB	M
	E.1 Errores de los usuarios	-	MB	B	-	B	B	-	MB	B
	E.2 Errores del administrador	-	B	M	-	M	M	-	B	M
	E.8 Difusión de software dañino	-	B	M	-	M	M	-	B	M
	E.18 Destrucción de información	-	MB	M	-	M	M	-	MB	M
	A.6 Abuso de privilegios de acceso	-	MB	M	-	M	M	-	MB	M
	A.7 Uso no previsto	-	MB	MB	-	A	A	-	B	B
	A.8 Difusión de software dañino	-	B	M	-	A	A	-	M	A
	A.18 Destrucción de información	-	B	M	-	A	A	-	M	A
	A.22 Manipulación de programas	-	B	M	-	A	A	-	M	A
SW-std-os02	I.5Avería de origen físico o lógico	-	MB	M	-	M	M	-	MB	M
	E.1 Errores de los usuarios	-	MB	B	-	B	B	-	MB	B
	E.2 Errores del administrador	-	B	M	-	M	M	-	B	M
	E.8 Difusión de software dañino	-	MB	M	-	M	M	-	MB	M

	E.18 Destrucción de información	-	B	M	-	M	M	-	B	M
	A.6 Abuso de privilegios de acceso	-	B	M	-	M	M	-	B	M
	A.7 Uso no previsto	-	MB	B	-	A	A	-	B	M
	A.8 Difusión de software dañino	-	B	M	-	A	A	-	M	A
	A.18 Destrucción de información	-	B	M	-	A	A	-	M	A
	A.22 Manipulación de programas	-	B	M	-	A	A	-	M	A
SW-std-os03	I.5Avería de origen físico o lógico	-	B	A	-	M	M	-	B	A
	E.1 Errores de los usuarios	-	B	M	-	B	B	-	B	M
	E.2 Errores del administrador	-	M	M	-	M	M	-	M	M
	E.8 Difusión de software dañino	-	B	A	-	M	M	-	B	A
	E.18 Destrucción de información	-	B	A	-	M	M	-	B	A
	A.6 Abuso de privilegios de acceso	-	M	A	-	M	M	-	M	A
	A.7 Uso no previsto	-	M	M	-	A	A	-	A	A
	A.8 Difusión de software dañino	-	M	A	-	A	A	-	A	A
	A.18 Destrucción de información	-	M	A	-	A	A	-	A	A
	A.22 Manipulación de programas	-	M	A	-	A	A	-	A	A
SW-std-os04	I.5Avería de origen físico o lógico	-	B	A	-	M	M	-	B	A
	E.1 Errores de los usuarios	-	B	M	-	B	B	-	B	M
	E.2 Errores del administrador	-	M	M	-	M	M	-	M	M
	E.8 Difusión de software dañino	-	B	A	-	M	M	-	B	A
	E.18 Destrucción de información	-	B	A	-	M	M	-	B	A
	A.6 Abuso de privilegios de acceso	-	B	A	-	M	M	-	B	A
	A.7 Uso no previsto	-	B	M	-	A	A	-	M	A
	A.8 Difusión de software dañino	-	B	A	-	A	A	-	M	MA
	A.18 Destrucción de información	-	B	A	-	A	A	-	M	MA
	A.22 Manipulación de programas	-	B	A	-	A	A	-	M	MA
SW-std-os05	I.5Avería de origen físico o lógico	-	MB	M	-	M	M	-	MB	M
	E.1 Errores de los usuarios	-	MB	B	-	B	B	-	MB	B
	E.2 Errores del administrador	-	B	B	-	M	M	-	B	B

	E.8 Difusión de software dañino	-	MB	M	-	M	M	-	MB	M
	E.18 Destrucción de información	-	MB	M	-	M	M	-	MB	M
	A.6 Abuso de privilegios de acceso	-	MB	M	-	M	M	-	MB	M
	A.7 Uso no previsto	-	MB	B	-	A	A	-	B	M
	A.8 Difusión de software dañino	-	B	M	-	A	A	-	M	A
	A.18 Destrucción de información	-	B	M	-	A	A	-	M	A
	A.22 Manipulación de programas	-	B	M	-	A	A	-	M	A
SW-std-os06	I.5Avería de origen físico o lógico	-	MB	M	-	M	M	-	MB	M
	E.1 Errores de los usuarios	-	MB	B	-	B	B	-	MB	MB
	E.2 Errores del administrador	-	B	M	-	M	M	-	B	M
	E.8 Difusión de software dañino	-	MB	M	-	M	M	-	MB	M
	E.18 Destrucción de información	-	MB	M	-	M	M	-	MB	M
	A.6 Abuso de privilegios de acceso	-	MB	M	-	M	M	-	MB	M
	A.7 Uso no previsto	-	MB	M	-	A	A	-	B	A
	A.8 Difusión de software dañino	-	B	M	-	A	A	-	M	A
	A.18 Destrucción de información	-	B	M	-	A	A	-	M	A
	A.22 Manipulación de programas	-	B	M	-	A	A	-	M	A
SW-std-os07	I.5Avería de origen físico o lógico	-	MB	M	-	M	M	-	MB	M
	E.1 Errores de los usuarios	-	MB	B	-	B	B	-	MB	B
	E.2 Errores del administrador	-	B	B	-	M	M	-	B	B
	E.8 Difusión de software dañino	-	MB	M	-	M	M	-	MB	M
	E.18 Destrucción de información	-	MB	M	-	M	M	-	MB	M
	A.6 Abuso de privilegios de acceso	-	B	M	-	M	M	-	B	M
	A.7 Uso no previsto	-	B	B	-	A	A	-	M	M
	A.8 Difusión de software dañino	-	B	M	-	A	A	-	M	A
	A.18 Destrucción de información	-	B	M	-	A	A	-	M	A
	A.22 Manipulación de programas	-	B	M	-	A	A	-	M	A
W-std-os08	I.5Avería de origen físico o lógico	-	MB	M	-	M	M	-	MB	M
	E.1 Errores de los usuarios	-	B	B	-	B	B	-	B	B

	E.2 Errores del administrador	-	B	B	-	M	M	-	B	B
	E.8 Difusión de software dañino	-	MB	M	-	M	M	-	MB	M
	E.18 Destrucción de información	-	MB	M	-	M	M	-	MB	M
	A.6 Abuso de privilegios de acceso	-	B	M	-	M	M	-	B	B
	A.7 Uso no previsto	-	B	B	-	A	A	-	M	M
	A.8 Difusión de software dañino	-	B	M	-	A	A	-	M	A
	A.18 Destrucción de información	-	B	M	-	A	A	-	M	A
	A.22 Manipulación de programas	-	B	M	-	A	A	-	M	A
SW-std-os09	I.5Avería de origen físico o lógico	-	MB	M	-	M	M	-	MB	M
	E.1 Errores de los usuarios	-	B	B	-	B	B	-	B	B
	E.2 Errores del administrador	-	B	B	-	M	M	-	B	B
	E.8 Difusión de software dañino	-	MB	M	-	M	M	-	MB	M
	E.18 Destrucción de información	-	B	M	-	M	M	-	B	M
	A.6 Abuso de privilegios de acceso	-	B	M	-	M	M	-	B	M
	A.7 Uso no previsto	-	B	B	-	A	A	-	M	M
	A.8 Difusión de software dañino	-	B	M	-	A	A	-	M	A
	A.18 Destrucción de información	-	B	M	-	A	A	-	M	A
	A.22 Manipulación de programas	-	B	M	-	A	A	-	M	A
SW-std-os10	I.5Avería de origen físico o lógico	-	MB	M	-	M	M	-	MB	M
	E.1 Errores de los usuarios	-	MB	B	-	B	B	-	MB	B
	E.2 Errores del administrador	-	B	B	-	M	M	-	B	B
	E.8 Difusión de software dañino	-	MB	M	-	M	M	-	MB	M
	E.18 Destrucción de información	-	B	M	-	M	M	-	B	M
	A.6 Abuso de privilegios de acceso	-	B	M	-	M	M	-	B	M
	A.7 Uso no previsto	-	B	B	-	A	A	-	M	M
	A.8 Difusión de software dañino	-	B	M	-	A	A	-	M	A
	A.18 Destrucción de información	-	B	M	-	A	A	-	M	A
	A.22 Manipulación de programas	-	B	M	-	A	A	-	M	A
SW-std-1	I.5Avería de origen físico o lógico	-	MB	M	-	M	M	-	MB	M

	E.1 Errores de los usuarios	-	MB	M	-	M	M	-	MB	M
	E.2 Errores del administrador	-	B	M	-	M	M	-	B	M
	E.8 Difusión de software dañino	-	B	M	-	M	M	-	B	M
	E.18 Destrucción de información	-	B	M	-	M	M	-	B	M
	E.20 Vulnerabilidades de los programas (software)	-	B	M	-	A	A	-	M	A
	E.21 Errores de mantenimiento/actualización de programas(software)	-	B	M	-	A	A	-	M	A
	A.6 Abuso de privilegios de acceso	-	B	M	-	M	M	-	B	M
	A.7 Uso no previsto	-	B	B	-	M	M	-	B	B
	A.8 Difusión de software dañino	-	B	M	-	M	M	-	B	B
	A.18 Destrucción de información	-	B	M	-	A	A	-	M	A
	A.22 Manipulación de programas	-	B	M	-	A	A	-	M	A
SW-std-dbm01	I.5Avería de origen físico o lógico	B	B	M	M	M	A	B	B	A
	E.1 Errores de los usuarios	B	B	M	M	M	A	B	B	A
	E.2 Errores del administrador	B	B	M	M	M	A	B	B	A
	E.8 Difusión de software dañino	B	B	M	M	M	A	B	B	A
	E.18 Destrucción de información	B	B	M	M	M	A	B	B	A
	E.20 Vulnerabilidades de los programas (software)	B	B	M	M	A	A	B	M	A
	E.21 Errores de mantenimiento/actualización de programas(software)	B	B	M	M	A	A	B	M	A
	A.6 Abuso de privilegios de acceso	B	B	M	M	A	A	B	M	A
	A.7 Uso no previsto	B	B	M	M	A	A	B	M	A
	A.8 Difusión de software dañino	B	B	M	M	A	A	B	M	A
	A.18 Destrucción de información	B	B	M	M	A	A	B	M	A
	A.22 Manipulación de programas	B	B	M	M	A	A	B	M	A
SW-std-dbms02	I.5Avería de origen físico o lógico	M	M	A	M	M	A	M	M	MA
	E.1 Errores de los usuarios	M	M	A	M	M	A	M	M	MA
	E.2 Errores del administrador	M	M	A	M	M	A	M	M	MA
	E.8 Difusión de software dañino	M	M	A	M	M	A	M	M	MA
	E.18 Destrucción de información	M	M	A	M	M	A	M	M	MA

	E.20 Vulnerabilidades de los programas (software)	M	M	A	M	A	A	M	A	MA
	E.21 Errores de mantenimiento/actualización de programas(software)	M	M	A	M	A	A	M	A	MA
	A.6 Abuso de privilegios de acceso	M	M	A	M	A	A	M	A	MA
	A.7 Uso no previsto	M	M	A	M	A	A	M	A	MA
	A.8 Difusión de software dañino	M	M	A	M	A	A	M	A	MA
	A.18 Destrucción de información	M	M	A	M	A	A	M	A	MA
	A.22 Manipulación de programas	M	M	A	M	A	A	M	A	MA
SW-std-2	I.5Avería de origen físico o lógico	-	B	M	-	M	M	-	B	M
	E.1 Errores de los usuarios	-	MB	B	-	M	M	-	MB	B
	E.2 Errores del administrador	-	MB	M	-	M	M	-	MB	M
	E.8 Difusión de software dañino	-	MB	M	-	M	M	-	MB	M
	E.18 Destrucción de información	-	MB	B	-	M	M	-	MB	B
	E.20 Vulnerabilidades de los programas (software)	-	MB	B	-	A	A	-	B	M
	E.21 Errores de mantenimiento/actualización de programas(software)	-	MB	B	-	A	A	-	B	M
	A.6 Abuso de privilegios de acceso	-	B	M	-	M	M	-	B	B
	A.7 Uso no previsto	-	B	M	-	M	M	-	B	B
	A.8 Difusión de software dañino	-	B	M	-	M	M	-	B	B
	A.18 Destrucción de información	-	B	M	-	A	A	-	M	A
	A.22 Manipulación de programas	-	B	M	-	A	A	-	M	A
SW-std-3	I.5Avería de origen físico o lógico	-	B	M	-	M	M	-	M	A
	E.1 Errores de los usuarios	-	MB	B	-	M	M	-	MB	B
	E.2 Errores del administrador	-	MB	M	-	M	M	-	MB	M
	E.8 Difusión de software dañino	-	MB	M	-	M	M	-	MB	M
	E.18 Destrucción de información	-	MB	B	-	M	M	-	MB	B
	E.20 Vulnerabilidades de los programas (software)	-	MB	B	-	A	A	-	M	M
	E.21 Errores de mantenimiento/actualización de programas(software)	-	MB	B	-	A	A	-	B	M

	A.6 Abuso de privilegios de acceso	-	B	M	-	M	M	-	B	M
	A.7 Uso no previsto	-	B	M	-	M	M	-	B	M
	A.8 Difusión de software dañino	-	B	M	-	M	M	-	B	M
	A.18 Destrucción de información	-	B	M	-	A	A	-	M	A
	A.22 Manipulación de programas	-	B	M	-	A	A	-	M	A
SW-std-4	I.5Avería de origen físico o lógico	-	B	M	-	M	M	-	M	M
	E.1 Errores de los usuarios	-	MB	B	-	M	M	-	MB	B
	E.2 Errores del administrador	-	MB	M	-	M	M	-	MB	M
	E.8 Difusión de software dañino	-	MB	M	-	M	M	-	MB	M
	E.18 Destrucción de información	-	MB	B	-	M	M	-	MB	B
	E.20 Vulnerabilidades de los programas (software)	-	MB	B	-	A	A	-	B	M
	E.21 Errores de mantenimiento/actualización de programas(software)	-	MB	B	-	A	A	-	B	M
	A.6 Abuso de privilegios de acceso	-	B	M	-	M	M	-	B	M
	A.7 Uso no previsto	-	B	M	-	M	M	-	B	M
	A.8 Difusión de software dañino	-	B	M	-	M	M	-	B	M
	A.18 Destrucción de información	-	B	M	-	A	A	-	M	A
	A.22 Manipulación de programas	-	B	M	-	A	A	-	M	A
SW-std-5	I.5Avería de origen físico o lógico	-	M	A	-	M	M	-	M	A
	E.1 Errores de los usuarios	-	M	M	-	M	M	-	M	M
	E.2 Errores del administrador	-	M	A	-	M	M	-	M	A
	E.8 Difusión de software dañino	-	M	A	-	M	M	-	M	A
	E.18 Destrucción de información	-	M	A	-	M	M	-	M	A
	E.20 Vulnerabilidades de los programas (software)	-	M	A	-	A	A	-	A	MA
	E.21 Errores de mantenimiento/actualización de programas(software)	-	M	A	-	A	A	-	A	MA
	A.6 Abuso de privilegios de acceso	-	M	A	-	M	M	-	M	A
	A.7 Uso no previsto	-	M	A	-	M	M	-	M	A
	A.8 Difusión de software dañino	-	M	A	-	M	M	-	M	A
	A.18 Destrucción de información	-	M	A	-	A	A	-	A	MA

	A.22 Manipulación de programas	-	M	A	-	A	A	-	A	MA
SW-std-6	I.5Avería de origen físico o lógico	B	M	A	M	M	M	B	M	A
	E.1 Errores de los usuarios	MB	B	M	M	M	M	MB	B	B
	E.2 Errores del administrador	B	M	A	M	M	M	B	M	A
	E.8 Difusión de software dañino	B	M	A	M	M	M	B	M	A
	E.18 Destrucción de información	B	M	A	M	M	M	B	M	A
	E.20 Vulnerabilidades de los programas (software)	B	M	A	A	A	A	M	A	MA
	E.21 Errores de mantenimiento/actualización de programas(software)	B	M	A	A	A	A	M	A	MA
	A.6 Abuso de privilegios de acceso	B	M	A	M	M	M	B	M	A
	A.7 Uso no previsto	MB	M	A	M	M	M	MB	M	A
	A.8 Difusión de software dañino	B	M	A	M	M	M	B	M	A
	A.18 Destrucción de información	B	M	A	A	A	A	M	A	MA
	A.22 Manipulación de programas	B	M	A	A	A	A	M	A	MA
SW-std-7	I.5Avería de origen físico o lógico	B	M	A	M	M	M	B	M	A
	E.1 Errores de los usuarios	MB	B	M	M	M	M	MB	B	M
	E.2 Errores del administrador	B	M	A	M	M	M	B	M	A
	E.8 Difusión de software dañino	B	M	A	M	M	M	B	M	A
	E.18 Destrucción de información	B	M	A	M	M	M	B	M	A
	E.20 Vulnerabilidades de los programas (software)	B	M	A	A	A	A	M	A	MA
	E.21 Errores de mantenimiento/actualización de programas(software)	B	M	A	A	A	A	M	A	MA
	A.6 Abuso de privilegios de acceso	B	M	A	M	M	M	B	M	A
	A.7 Uso no previsto	MB	M	A	M	M	M	MB	M	A
	A.8 Difusión de software dañino	B	M	A	M	M	M	B	M	A
	A.18 Destrucción de información	B	M	A	A	A	A	M	A	MA
	A.22 Manipulación de programas	B	M	A	A	A	A	M	A	MA
SW-std-8	I.5Avería de origen físico o lógico	B	M	A	M	M	M	B	M	A
	E.1 Errores de los usuarios	MB	B	A	M	M	M	MB	B	A
	E.2 Errores del administrador	B	M	A	M	M	M	B	M	A

	E.8 Difusión de software dañino	MB	M	A	M	M	M	MB	M	A
	E.18 Destrucción de información	B	M	A	M	M	M	B	M	A
	E.20 Vulnerabilidades de los programas (software)	MB	M	A	A	A	A	B	A	MA
	E.21 Errores de mantenimiento/actualización de programas(software)	MB	M	A	A	A	A	B	A	MA
	A.6 Abuso de privilegios de acceso	B	M	A	M	M	M	B	M	A
	A.7 Uso no previsto	B	M	A	M	M	M	B	M	A
	A.8 Difusión de software dañino	B	M	A	M	M	M	B	M	A
	A.18 Destrucción de información	B	M	A	A	A	A	M	A	MA
	A.22 Manipulación de programas	B	M	A	A	A	A	M	A	MA
SW-std-9	I.5Avería de origen físico o lógico	B	M	A	M	M	M	B	M	A
	E.1 Errores de los usuarios	MB	B	A	M	M	M	MB	B	A
	E.2 Errores del administrador	B	M	A	M	M	M	B	M	A
	E.8 Difusión de software dañino	MB	M	A	M	M	M	MB	M	A
	E.18 Destrucción de información	B	M	A	M	M	M	B	M	A
	E.20 Vulnerabilidades de los programas (software)	MB	M	A	A	A	A	B	A	MA
	E.21 Errores de mantenimiento/actualización de programas(software)	MB	M	A	A	A	A	B	A	MA
	A.6 Abuso de privilegios de acceso	B	M	A	M	M	M	B	M	A
	A.7 Uso no previsto	B	M	A	M	M	M	B	M	A
	A.8 Difusión de software dañino	B	M	A	M	M	M	B	M	A
	A.18 Destrucción de información	B	M	A	A	A	A	M	A	MA
	A.22 Manipulación de programas	B	M	A	A	A	A	M	A	MA

Fuente: Elaborado por el investigador

Tabla 3.20 Riesgos en Hardware

ACTIVO	AMENAZAS	IMPACTO			PROBABILIDAD			RIESGO		
		C	I	D	C	I	D	C	I	D
HW-host01	N.1 Fuego	MB	B	A	B	B	B	MB	B	A
	N.2 Daños de Agua	MB	B	A	B	B	B	MB	B	A
	N.7 Fenómeno Sísmico	MB	B	A	B	B	B	MB	B	A
	N.8 Fenómenos de Origen Volcánico	MB	B	B	MB	MB	MB	MB	MB	MB
	I.1 Fuego	MB	B	A	B	B	B	MB	B	A
	I.2 Daños por agua	MB	B	A	B	B	B	MB	B	A
	I.3 Contaminación mecánica	MB	B	B	B	B	B	MB	B	B
	I.5 Avería de origen físico o lógico	B	M	M	M	M	M	B	M	M
	I.6 Corte de suministro eléctrico	MB	B	A	A	A	A	B	M	MA
	I.7 Condiciones inadecuadas de temperatura o humedad	MB	B	B	B	B	B	MB	B	B
	E.2 Errores del administrador	MB	B	M	M	M	M	MB	B	M
	E.23 Errores de mantenimiento/actualización de equipos (hardware)	B	M	A	M	M	M	B	M	A
	E.24Caída del sistema por agotamiento de recursos	B	M	A	M	M	M	B	M	A
	A.6Abuso de privilegios de acceso	B	M	A	B	B	B	B	M	A
	A.7 Uso no previsto	MB	B	M	B	B	B	MB	B	M
	A.24 Denegación de servicio	B	M	A	M	M	M	B	M	A
	A.25 Robo	B	M	A	MB	MB	MB	MB	B	M
	A.26 Ataque destructivo	B	M	A	B	B	B	B	M	M
HW-host02	N.1 Fuego	A	M	A	B	B	B	A	M	A
	N.2 Daños de Agua	M	M	A	B	B	B	M	M	A
	N.7 Fenómeno Sísmico	M	M	A	B	B	B	M	M	A
	N.8 Fenómenos de Origen Volcánico	B	B	B	MB	MB	MB	MB	MB	MB
	I.1 Fuego	B	B	A	B	B	B	B	B	A
	I.2 Daños por agua	B	B	A	B	B	B	B	B	A
	I.3 Contaminación mecánica	B	B	B	B	B	B	B	B	B
	I.5 Avería de origen físico o lógico	M	M	A	M	M	M	M	M	A

	I.6 Corte de suministro eléctrico	B	B	A	A	A	A	M	M	MA
	I.7 Condiciones inadecuadas de temperatura o humedad	B	B	B	B	B	B	B	B	B
	E.2 Errores del administrador	B	B	A	M	M	M	B	B	A
	E.23 Errores de mantenimiento/actualización de equipos (hardware)	M	M	A	M	M	M	M	M	A
	E.24 Caída del sistema por agotamiento de recursos	M	M	A	M	M	M	M	M	A
	A.6Abuso de privilegios de acceso	M	M	A	B	B	B	M	M	A
	A.7 Uso no previsto	B	M	A	B	B	B	B	M	A
	A.24 Denegación de servicio	M	M	A	M	M	M	M	M	A
	A.25 Robo	M	M	A	MB	MB	MB	B	B	M
	A.26 Ataque destructivo	M	M	A	B	B	B	M	M	M
HW-host03	N.1 Fuego	MB	MB	MB	B	B	B	MB	MB	MB
	N.2 Daños de Agua	MB	MB	M	B	B	B	MB	MB	M
	N.7 Fenómeno Sísmico	MB	MB	M	B	B	B	MB	MB	M
	N.8 Fenómenos de Origen Volcánico	MB	MB	MB	MB	MB	MB	MB	MB	MB
	I.1 Fuego	MB	MB	M	B	B	B	MB	MB	M
	I.2 Daños por agua	MB	MB	M	B	B	B	MB	MB	M
	I.3 Contaminación mecánica	MB	MB	MB	B	B	B	MB	MB	MB
	I.5 Avería de origen físico o lógico	B	B	M	M	M	M	B	B	M
	I.6 Corte de suministro eléctrico	MB	MB	M	A	A	A	B	B	A
	I.7 Condiciones inadecuadas de temperatura o humedad	MB	MB	MB	B	B	B	MB	MB	MB
	E.2 Errores del administrador	MB	MB	M	M	M	M	MB	MB	M
	E.23 Errores de mantenimiento/actualización de equipos (hardware)	MB	MB	B	M	M	M	MB	MB	B
	E.24 Caída del sistema por agotamiento de recursos	B	B	M	M	M	M	B	B	M

	A.6Abuso de privilegios de acceso	B	B	M	B	B	B	B	B	M
	A.7 Uso no previsto	MB	MB	M	B	B	B	MB	MB	M
	A.24 Denegación de servicio	B	B	M	M	M	M	B	B	M
	A.25 Robo	B	B	M	MB	MB	MB	MB	MB	B
	A.26 Ataque destructivo	B	B	M	B	B	B	B	B	M
HW-host04	N.1 Fuego	MB	MB	M	B	B	B	MB	MB	M
	N.2 Daños de Agua	MB	MB	M	B	B	B	MB	MB	M
	N.7 Fenómeno Sísmico	MB	MB	M	B	B	B	MB	MB	M
	N.8 Fenómenos de Origen Volcánico	MB	MB	MB	MB	MB	MB	MB	MB	MB
	I.1 Fuego	MB	MB	M	B	B	B	MB	MB	M
	I.2 Daños por agua	MB	MB	M	B	B	B	MB	MB	M
	I.3 Contaminación mecánica	MB	MB	MB	B	B	B	MB	MB	MB
	I.5 Avería de origen físico o lógico	MB	B	M	M	M	M	MB	B	M
	I.6 Corte de suministro eléctrico	MB	MB	M	A	A	A	B	B	A
	I.7 Condiciones inadecuadas de temperatura o humedad	MB	MB	MB	B	B	B	MB	MB	MB
	E.2 Errores del administrador	MB	B	M	M	M	M	MB	B	M
	E.23 Errores de mantenimiento/actualización de equipos (hardware)	B	B	M	M	M	M	B	B	M
	E.24 Caída del sistema por agotamiento de recursos	B	B	M	M	M	M	B	B	M
	A.6Abuso de privilegios de acceso	B	B	M	B	B	B	B	B	M
	A.7 Uso no previsto	MB	B	M	B	B	B	MB	B	M
	I.8 Sobrecarga eléctrica	B	B	M	M	M	M	B	B	M
	A.25 Robo	B	B	M	MB	MB	MB	MB	MB	B
	A.26 Ataque destructivo	MB	B	M	B	B	B	MB	B	M
HW-switch01	N.1 Fuego	MB	B	A	B	B	B	MB	B	A
	N.2 Daños de Agua	MB	B	A	B	B	B	MB	B	A
	N.7 Fenómeno Sísmico	MB	B	A	B	B	B	MB	B	A

	N.8 Fenómenos de Origen Volcánico	MB	B	B	MB	MB	MB	MB	MB	MB
	I.1 Fuego	MB	B	A	B	B	B	MB	B	A
	I.2 Daños por agua	MB	B	A	B	B	B	MB	B	A
	I.3 Contaminación mecánica	MB	B	B	B	B	B	MB	B	B
	I.5 Avería de origen físico o lógico	B	M	A	M	M	M	B	M	A
	I.6 Corte de suministro eléctrico	MB	B	A	A	A	A	B	M	MA
	I.7 Condiciones inadecuadas de temperatura o humedad	MB	B	B	B	B	B	MB	B	B
	E.2 Errores del administrador	MB	B	A	M	M	M	MB	B	A
	E.23 Errores de mantenimiento/actualización de equipos (hardware)	B	M	A	M	M	M	B	M	A
	E.24 Caída del sistema por agotamiento de recursos	B	M	A	M	M	M	B	M	A
	A.6Abuso de privilegios de acceso	B	M	A	B	B	B	B	M	A
	A.7 Uso no previsto	MB	M	A	B	B	B	MB	M	A
	A.24 Denegación de servicio	B	M	A	M	M	M	B	M	A
	A.25 Robo	B	M	A	MB	MB	MB	MB	B	M
	A.26 Ataque destructivo	B	M	A	M	M	M	B	M	M
HW-firewall01	N.1 Fuego	MB	B	A	B	B	B	MB	B	A
	N.2 Daños de Agua	MB	B	A	B	B	B	MB	B	A
	N.7 Fenómeno Sísmico	MB	B	B	B	B	B	MB	B	B
	N.8 Fenómenos de Origen Volcánico	MB	B	A	MB	MB	MB	MB	MB	M
	I.1 Fuego	MB	B	A	B	B	B	MB	B	A
	I.2 Daños por agua	MB	B	A	B	B	B	MB	B	A
	I.3 Contaminación mecánica	MB	B	A	B	B	B	MB	B	A
	I.5 Avería de origen físico o lógico	B	M	A	M	M	M	B	M	A
	I.6 Corte de suministro eléctrico	MB	B	A	A	A	A	B	M	MA
	I.7 Condiciones inadecuadas de temperatura o humedad	MB	B	B	B	B	B	MB	B	B
	E.2 Errores del administrador	MB	M	A	M	M	M	MB	M	A

	E.23 Errores de mantenimiento/actualización de equipos (hardware)	B	M	A	M	M	M	B	M	A
	E.24 Caída del sistema por agotamiento de recursos	B	M	A	M	M	M	B	M	A
	A.6Abuso de privilegios de acceso	MB	B	B	B	B	B	MB	B	B
	A.7 Uso no previsto	B	M	A	B	B	B	B	M	A
	A.24 Denegación de servicio	MB	B	A	M	M	M	MB	B	A
	A.25 Robo	M	M	M	MB	MB	MB	B	B	B
	A.26 Ataque destructivo	MB	B	A	M	M	M	MB	B	M
HW-switch02	N.1 Fuego	MB	B	A	B	B	B	MB	B	A
	N.2 Daños de Agua	MB	B	A	B	B	B	MB	B	A
	N.7 Fenómeno Sísmico	MB	B	M	B	B	B	MB	B	M
	N.8 Fenómenos de Origen Volcánico	MB	B	B	MB	MB	MB	MB	MB	MB
	I.1 Fuego	MB	B	A	B	B	B	MB	B	A
	I.2 Daños por agua	MB	B	A	B	B	B	MB	B	A
	I.3 Contaminación mecánica	MB	B	B	B	B	B	MB	B	B
	I.5 Avería de origen físico o lógico	B	M	M	M	M	M	B	M	M
	I.6 Corte de suministro eléctrico	MB	B	B	A	A	A	B	M	M
	I.7 Condiciones inadecuadas de temperatura o humedad	MB	B	B	M	M	M	MB	B	B
	E.2 Errores del administrador	MB	M	A	M	M	M	MB	M	A
	E.23 Errores de mantenimiento/actualización de equipos (hardware)	B	M	A	M	M	M	B	M	A
	E.24 Caída del sistema por agotamiento de recursos	B	M	A	M	M	M	B	M	A
	A.6Abuso de privilegios de acceso	B	M	A	B	B	B	B	M	A
	A.7 Uso no previsto	MB	M	A	B	B	B	MB	M	A
	A.24 Denegación de servicio	B	M	A	M	M	M	B	M	A
	A.25 Robo	B	M	A	MB	MB	MB	MB	B	M
	A.26 Ataque destructivo	B	M	A	M	M	M	B	M	M
HW-fire	N.1 Fuego	MB	B	A	B	B	B	MB	B	A

	N.2 Daños de Agua	MB	B	A	B	B	B	MB	B	A
	N.7 Fenómeno Sísmico	MB	B	A	B	B	B	MB	B	A
	N.8 Fenómenos de Origen Volcánico	MB	B	B	MB	MB	MB	MB	MB	MB
	I.1 Fuego	MB	B	A	B	B	B	MB	B	A
	I.2 Daños por agua	MB	MB	A	B	B	B	MB	MB	A
	I.3 Contaminación mecánica	MB	B	B	B	B	B	MB	B	B
	I.5 Avería de origen físico o lógico	B	M	A	M	M	M	B	M	A
	I.6 Corte de suministro eléctrico	MB	B	A	A	A	A	B	M	MA
	I.7 Condiciones inadecuadas de temperatura o humedad	MB	B	B	M	M	M	MB	B	B
	E.2 Errores del administrador	MB	M	A	M	M	M	MB	M	A
	E.23 Errores de mantenimiento/actualización de equipos (hardware)	B	M	A	M	M	M	B	M	A
	E.24 Caída del sistema por agotamiento de recursos	B	M	A	M	M	M	B	M	A
	A.6Abuso de privilegios de acceso	MB	B	B	B	B	B	MB	B	B
	A.7 Uso no previsto	B	M	A	B	B	B	B	M	A
	A.24 Denegación de servicio	MB	B	A	M	M	M	MB	B	A
	A.25 Robo	MB	B	B	MB	MB	MB	MB	MB	MB
	A.26 Ataque destructivo	MB	B	A	M	M	M	MB	B	M

Fuente: Elaborador por el investigador

Tabla 3.21 Riesgo en Datos

ACTIVO	AMENAZAS	IMPACTO			PROBABILIDAD			RIESGO		
		C	I	D	C	I	D	C	I	D
D-conf01	E.1 Errores de los usuarios	A	A	MA	M	M	M	A	A	MA
	E.2 Errores del administrador	A	A	MA	M	M	M	A	A	MA
	E.18 Destrucción de información	A	A	MA	B	B	B	A	A	MA
	A.4 Manipulación de la configuración	A	A	MA	MB	MB	MB	M	M	A
	D.log registros de actividad									
	A.6 Abuso de privilegios de acceso	A	A	MA	B	B	B	A	A	MA
	A.18 Destrucción de información	A	A	MA	B	B	B	A	A	MA
D-conf02	E.1 Errores de los usuarios	A	A	MA	M	M	M	A	A	MA
	E.2 Errores del administrador	A	A	MA	M	M	M	A	A	MA
	E.18 Destrucción de información	A	A	MA	B	B	B	A	A	MA
	A.4 Manipulación de la configuración	A	A	MA	MB	MB	MB	M	M	A
	D.log registros de actividad									
	A.6 Abuso de privilegios de acceso	A	A	MA	B	B	B	A	A	MA
	A.18 Destrucción de información	A	A	MA	B	B	B	A	A	MA
D-Conf03	E.1 Errores de los usuarios	A	A	MA	M	M	M	A	A	MA
	E.2 Errores del administrador	A	A	MA	M	M	M	A	A	MA
	E.18 Destrucción de información	A	A	MA	B	B	B	A	A	MA
	A.4 Manipulación de la configuración	A	A	MA	MB	MB	MB	M	M	A
	D.log registros de actividad									
	A.6 Abuso de privilegios de acceso	A	A	MA	B	B	B	A	A	MA
	A.18 Destrucción de información	A	A	MA	B	B	B	A	A	MA

Fuente: Elaborado por el investigador

Tabla 3.22 Riesgos en Redes de Comunicación

ACTIVO	AMENAZAS	IMPACTO			PROBABILIDAD			RIESGO		
		C	I	D	C	I	D	C	I	D
COM-internet01	I.8 Fallo de servicios de comunicaciones	A	A	MA	B	B	B	A	A	MA
	E.2 Errores del administrador	M	A	MA	M	M	M	M	A	MA
	E.18 Destrucción de información	A	A	MA	B	B	B	A	A	MA
	E.24 Caída del sistema por agotamiento de recursos	A	A	MA	B	B	B	A	A	MA
	A.6 Abuso de privilegio de acceso	A	A	MA	B	B	B	A	A	MA
	A.7 Uso no previsto	A	A	MA	B	B	B	A	A	MA
	A.24 Denegación de servicio	A	A	MA	B	B	B	A	A	MA
COM-internet01	I.8 Fallo de servicios de comunicaciones	A	A	MA	B	B	B	A	A	MA
	E.2 Errores del administrador	M	A	MA	M	M	M	M	A	MA
	E.18 Destrucción de información	A	A	MA	B	B	B	A	A	MA
	E.24 Caída del sistema por agotamiento de recursos	A	A	MA	B	B	B	A	A	MA
	A.6 Abuso de privilegio de acceso	A	A	MA	B	B	B	A	A	MA
	A.7 Uso no previsto	A	A	MA	B	B	B	A	A	MA
	A.24 Denegación de servicio	A	A	MA	B	B	B	A	A	MA

Fuente: Elaborado por el investigador

3.1.12 Cláusulas de la norma ISO 24762:2008

Tabla 3.23 Cláusulas de la norma ISO 24762:2008

5.- Recuperación de desastres de TIC	
5.2 Estabilidad Ambiental	La ocurrencia frecuente de huelgas, demostraciones, disturbios, delitos violentos, desastres naturales, pandemias, ataques deliberados indicarían una inestabilidad ambiental.
5.3 Gestión de Activos	protección de activos a través de un listado y almacenamiento de inventario, y la documentación relevante

5.4 Proximidad del sitio	Se emplean estrategias de selección del sitio para elegir una ubicación de sitios de recuperación de Desastres que esté bien aislada de varios peligros.
5.5. Gestión de proveedores	El personal, los servicios, los suministros y las soluciones proporcionados por los proveedores de una organización pueden verse afectados durante una emergencia. Esto, a su vez, afecta los plazos, los objetivos y los plazos de entrega de procesos.
5.6 Acuerdos de Subcontratación	El grado limitado de control que una organización puede ejercer mientras subcontrata tareas y procesos se contrarresta mediante controles estrictos, acuerdos contractuales, revisiones periódicas y medidas para aumentar la conciencia.
5.7 Seguridad de la Información	Los sistemas de TIC se agrupan en diferentes ubicaciones físicas en función de sus diferentes requisitos de protección durante situaciones de crisis. Además, los diversos componentes de todos los incidentes relacionados con la seguridad de TI (detección, notificación, respuesta y análisis de efectividad) se evalúan periódicamente.
5.8 Activación y desactivación del plan de recuperación ante desastres	Se establecen planes y procedimientos para identificar cuándo debe activarse un plan de recuperación ante desastres y cuándo pueden detenerse las medidas de recuperación.
5.9 Formación y Educación	La transferencia de conocimientos juega un papel importante en la sensibilización del personal, esto implica revisiones periódicas para evaluar la excelencia de los módulos de capacitación.
5.10 Pruebas en Sistemas de TIC	Las capacidades de continuidad comercial de los sistemas de TIC se prueban rigurosamente durante los cambios en los requisitos de la organización o la expansión de las operaciones comerciales.
5.11 Planificación de la continuidad del negocio para proveedores de servicios de Recuperación de Desastres de TIC	Las prioridades, los plazos, los requisitos mínimos y la logística se diseñan y prueban para determinar su eficacia para minimizar el impacto en los proveedores de servicios.

5.12 Documentación y revisión periódica	Todas las medidas de recuperación ante desastres se archivan y consultan constantemente. Esto permite actualizaciones y mejoras periódicas.
6.- Instalación de recuperación de Desastres de TIC	
6.2 Ubicación de los sitios de recuperación	Las ubicaciones de los sitios de recuperación se deciden en función de factores como la vulnerabilidad a los peligros naturales, los incidentes climáticos extremos, la disponibilidad de infraestructura, la proximidad de varios, como el transporte público, instituciones médicas, servicios como agua, gas, electricidad, etc.
6.3 Controles de acceso físico	La categorización de seguridad, las normas de entrada y salida, los protocolos de conducta y otras restricciones se establecen para varios departamentos mientras se encuentran en los sitios de recuperación.
6.4 Seguridad de Instalaciones físicas	Los sitios de recuperación están protegidos del acceso no autorizado y otras brechas de seguridad a través de inspecciones regulares, vigilancia constante, sistemas de detección y alarma, control de personal a través de identificación visible como credenciales / tarjetas de identificación y administración desde una ubicación central.
6.5 Áreas dedicadas	Se prevén áreas dedicadas para ejecutar medidas de recuperación como montaje, tenencia, puesta en escena y otras actividades.
6.6 Controles ambientales	Se abordan la temperatura, ventilación, humedad, vibración, ruido y otros factores ambientales en el sitio de recuperación. Controles, acuerdos contractuales, revisiones periódicas y medidas de sensibilización.
6.7 Telecomunicaciones	Las capacidades para compartir información se establecen al garantizar la conectividad, la seguridad de los datos, la diversidad de la red, la confiabilidad y los estándares de calidad.
6.8 Fuente de alimentación	Un suministro de electricidad continuo y estable es vital para que las operaciones continúen sin interrupciones. Esto se logra identificando proveedores de servicios confiables, estableciendo fuentes alternativas de suministro de energía, como generadores, instalaciones de suministro de energía ininterrumpida (UPS), etc.

6.9 Gestión de cables	Los cables relacionados con la electrónica y la fuente de alimentación cuentan con la protección y el blindaje adecuados para evitar interrupciones y pérdidas de información. Las bandejas y los conductos se revisan periódicamente para detectar daños, alteraciones y otras vulnerabilidades.
6.10 Protección contra incendios	Esto incluye adherirse a las normas de cumplimiento reglamentario, establecer planes de escape en caso de incendio e instalar equipos como extintores de incendios, rutas de escape, etc.
6.11 Centro de Operaciones de Emergencias (COE)	El mantenimiento de la comunicación entre la institución y las entidades externas se logra mediante un suministro adecuado de equipos, infraestructura relacionada con las telecomunicaciones, material de oficina, instalaciones físicas como áreas de reuniones, etc.
6.12 Instalaciones restringidas	El acceso a varias áreas en el sitio de recuperación está restringido según la designación y el propósito.
6.13 Servicios que no son de recuperación	Se toman medidas para atender el bienestar y la seguridad del personal presente en las instalaciones durante las emergencias.
6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo	Se administran mediante el cumplimiento de los requisitos y las mejores prácticas durante el período de vida útil del activo para garantizar el acceso ininterrumpido para las actividades de la institución.
6.15 Prueba	Las instalaciones físicas y los equipos se mantienen actualizados mediante un mantenimiento y pruebas regulares para garantizar una calidad óptima.
7.- Capacidad del proveedor de servicios subcontratados	
7.2 Revisar el estado de recuperación ante desastres de la organización	Las organizaciones se aseguran de tener una solución de recuperación ante desastres de calidad.
7.3 Requisitos de las instalaciones	Los proveedores de servicios se aseguran de que se cumplan adecuadamente todos los requisitos enumerados según la cláusula de recuperación de desastres de las TIC.
7.4 Experiencia	La capacidad del proveedor de servicios se destaca a través de la pericia y la experiencia del personal para brindar soluciones de calidad.

7.5 Controles de acceso lógico	Los proveedores de servicios subcontratados que brindan soporte operativo deben establecer sus credenciales para manejar los sistemas informáticos del sitio de recuperación.
7.6 Equipos de TIC y disponibilidad operativa	El equipo de computación y la infraestructura relacionada están instalados, operativos y bien mantenidos para un rendimiento óptimo.
7.7 Soporte de recuperación simultanea	Los proveedores de servicios deben asegurarse de que pueden cumplir con sus obligaciones contractuales a pesar de que muchos clientes activan sus servicios de recuperación ante desastres simultáneamente.
7.8 Niveles de servicio	La institución puede decidir el alcance de los servicios solicitados en función de la importancia de sus necesidades.
7.9 Tipos de servicio	La institución puede decidir sobre la gama de servicios solicitados en función de la complejidad de las medidas de recuperación.
7.10 Proximidad de servicios	Los proveedores de servicios se aseguran de tener las capacidades para abordar las necesidades de recuperación de varios clientes que enfrentan la misma interrupción, para minimizar riesgos.
7.11 Proporción de suscripción para servicios compartidos	Los proveedores de servicios deben mantener el número de organizaciones que se suscriben a sus servicios en un número óptimo para garantizar que siempre se preste un servicio de alta calidad
7.12 Activación de servicios suscritos	Los términos y condiciones para activar y desactivar el servicio suscrito están claramente definidos
7.13 Pruebas de Organización	Permite a las organizaciones probar periódicamente los servicios de recuperación ante desastres a los que se han suscrito.
7.14 Cambios en la capacidad	Los proveedores de servicios deben asegurarse de que las mejoras en sus capacidades debidas a inversiones, avances tecnológicos, etc., no afecten
7.15 Plan de respuesta a emergencias	Los proveedores de servicios deben protegerse contra emergencias no planificadas que pueden obstaculizar las soluciones que brindan a sus clientes.
7.16 Autoevaluación	Las áreas de evaluación identificadas están sujetas a extensas auditorías internas y pruebas integrales para garantizar que las soluciones se mantengan actualizadas.
8.- Selección de sitios de recuperación	

8.- Selección de sitios de recuperación	Se establecen normas para la selección de una buena infraestructura donde se dispone de mano de obra calificada. Esto incluye condiciones socioeconómicas favorables en la ubicación del sitio de recuperación. Esto está determinado por la disponibilidad de infraestructura, mano de obra calificada y soporte, masa crítica de vendedores y proveedores, historial de proveedores de servicios locales y apoyo proactivo de la comunidad local.
9.- Mejora continua	
9.- Mejora continua	Los procesos existentes se actualizan constantemente con la última tecnología y tendencias en función de las demandas y los factores impulsores de la industria. Tendencias de recuperación de Desastres de TIC Medición del desempeño Escalabilidad Mitigación de riesgos

Fuente: Elaborador por el investigador a partir de [29].

3.1.13 Categorización de riesgos y aplicabilidad de la norma ISO 24762:2008

Tabla 3.24 Categorización de riesgos y aplicabilidad de la norma ISO 24762:2008

ACTIVO	AMENAZA	RIESGO			NORMA ISO 24762:2008
		C	I	D	
SERVICIOS					
Spub01	E.19 Fugas de información	-	MB	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3 Controles de acceso físico. 7.16 Autoevaluación.
	E.24 Caída del sistema por agotamiento de recursos	-	MB	A	6.4 Seguridad de instalaciones físicas. 6.6 Controles ambientales. 6.8 Fuente de alimentación. 7.7 Soporte de recuperación simultánea. 7.14.7 Servicios existentes. 7.15 Plan de respuesta a emergencias.
	A.24 Denegación de servicio	-	B	A	5.5 Gestión de proveedores. 5.5.2 Soporte de equipos críticos.

					6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.15 Plan de respuesta a emergencias.
Spub02	E.24 Caída del sistema por agotamiento de recursos	-	MB	A	6.4 Seguridad de instalaciones físicas. 6.6 Controles ambientales. 6.8 Fuente de alimentación. 7.7 Soporte de recuperación simultánea. 7.14.7 Servicios existentes. 7.15 Plan de respuesta a emergencias.
	A.24 Denegación de servicio	-	B	A	5.5 Gestión de proveedores. 5.5.2 Soporte de equipos críticos. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.15 Plan de respuesta a emergencias.
Spub03	E.19 Fugas de información	MB	MB	A	5.7 Seguridad de la información 5.9 Formación y educación. 6.3 Controles de acceso físico. 7.16 Autoevaluación.
	E.24 Caída del sistema por agotamiento de recursos	MB	MB	A	6.4 Seguridad de instalaciones físicas. 6.6 Controles ambientales. 6.8 Fuente de alimentación. 7.7 Soporte de recuperación simultánea. 7.14.7 Servicios existentes. 7.15 Plan de respuesta a emergencias.
	A.24 Denegación de servicio	MB	B	A	5.5 Gestión de proveedores. 5.5.2 Soporte de equipos críticos. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.15 Plan de respuesta a emergencias.
Sint01	E.19 Fugas de información	-	MB	A	5.7 Seguridad de la información 5.9 Formación y educación. 6.3 Controles de acceso físico. 7.16 Autoevaluación.
	E.24 Caída del sistema por agotamiento de recursos	-	MB	A	6.4 Seguridad de instalaciones físicas. 6.6 Controles ambientales. 6.8 Fuente de alimentación. 7.7 Soporte de recuperación simultánea. 7.14.7 Servicios existentes.

					7.15 Plan de respuesta a emergencias.
	A.24 Denegación de servicio	-	B	A	5.5 Gestión de proveedores. 5.5.2 Soporte de equipos críticos. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.15 Plan de respuesta a emergencias.
Sint02	E.1 Errores de los usuarios	-	B	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.14.4 Reentrenamiento del personal.
	E.2 Errores del administrador	-	B	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.14.4 Reentrenamiento del personal.
	E.19 Fugas de información	-	M	A	5.7 Seguridad de la información 5.9 Formación y educación. 6.3 Controles de acceso físico. 7.16 Autoevaluación.
	E.24 Caída del sistema por agotamiento de recursos	-	B	MA	6.4 Seguridad de instalaciones físicas. 6.6 Controles ambientales. 6.8 Fuente de alimentación. 7.7 Soporte de recuperación simultánea. 7.14.7 Servicios existentes. 7.15 Plan de respuesta a emergencias.
	A.6 Abuso de privilegios de acceso	-	B	A	5.3.3 Protección de activos. 5.6.5 Controles de seguridad. 5.7 Seguridad de la información. 6.3 Controles de acceso físico. 6.4 Seguridad de instalaciones físicas. 5.8 Activación y desactivación del plan de recuperación ante desastres.
	A.24 Denegación de servicio	-	M	MA	5.5 Gestión de proveedores. 5.5.2 Soporte de equipos críticos. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo.

					7.15 Plan de respuesta a emergencias.
Sint03	E.19 Fugas de información	-	MB	A	5.7 Seguridad de la información 5.9 Formación y educación. 6.3 Controles de acceso físico. 7.16 Autoevaluación.
	E.24 Caída del sistema por agotamiento de recursos	-	MB	A	6.4 Seguridad de instalaciones físicas. 6.6 Controles ambientales. 6.8 Fuente de alimentación. 7.14.7 Servicios existentes. 7.7 Soporte de recuperación simultánea.
	A.24 Denegación de servicio	-	B	A	5.5 Gestión de proveedores. 5.5.2 Soporte de equipos críticos. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.15 Plan de respuesta a emergencias.
Sint04	E.19 Fugas de información	M	M	A	5.7 Seguridad de la información 5.9 Formación y educación. 6.3 Controles de acceso físico. 7.16 Autoevaluación.
	E.24 Caída del sistema por agotamiento de recursos	A	M	MA	6.4 Seguridad de instalaciones físicas. 6.6 Controles ambientales. 6.8 Fuente de alimentación. 7.7 Soporte de recuperación simultánea. 7.14.7 Servicios existentes. 7.15 Plan de respuesta a emergencias.
	A.6 Abuso de privilegios de acceso	M	M	A	5.5 Gestión de proveedores. 5.5.2 Soporte de equipos críticos. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.15 Plan de respuesta a emergencias.
	A.24 Denegación de servicio	M	A	MA	5.5 Gestión de proveedores. 5.5.2 Soporte de equipos críticos. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.15 Plan de respuesta a emergencias.
Sint05	E.19 Fugas de información	B	M	A	5.7 Seguridad de la información 5.9 Formación y educación. 6.3 Controles de acceso físico. 7.16 Autoevaluación.

	E.24 Caída del sistema por agotamiento de recursos	B	M	MA	6.4 Seguridad de instalaciones físicas. 6.6 Controles ambientales. 6.8 Fuente de alimentación. 7.7 Soporte de recuperación simultánea. 7.14.7 Servicios existentes. 7.15 Plan de respuesta a emergencias.
	A.6 Abuso de privilegios de acceso	B	M	A	5.5 Gestión de proveedores. 5.5.2 Soporte de equipos críticos. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.15 Plan de respuesta a emergencias.
	A.24 Denegación de servicio	B	A	MA	5.5 Gestión de proveedores. 5.5.2 Soporte de equipos críticos. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.15 Plan de respuesta a emergencias.
Sint06	E.19 Fugas de información	B	B	A	5.7 Seguridad de la información 5.9 Formación y educación. 6.3 Controles de acceso físico. 7.16 Autoevaluación.
	E.24 Caída del sistema por agotamiento de recursos	MB	B	A	6.4 Seguridad de instalaciones físicas. 6.6 Controles ambientales. 6.8 Fuente de alimentación. 7.7 Soporte de recuperación simultánea. 7.14.7 Servicios existentes. 7.15 Plan de respuesta a emergencias.
	A.24 Denegación de servicio	B	M	A	5.5 Gestión de proveedores. 5.5.2 Soporte de equipos críticos. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.15 Plan de respuesta a emergencias.
Sint07	E.19 Fugas de información	B	B	A	5.7 Seguridad de la información 5.9 Formación y educación. 6.3 Controles de acceso físico. 7.16 Autoevaluación.
	E.24 Caída del sistema por agotamiento de recursos	MB	B	A	6.4 Seguridad de instalaciones físicas. 6.6 Controles ambientales. 6.8 Fuente de alimentación. 7.7 Soporte de recuperación simultánea.

					7.14.7 Servicios existentes. 7.15 Plan de respuesta a emergencias.
	A.24 Denegación de servicio	B	M	A	5.5 Gestión de proveedores. 5.5.2 Soporte de equipos críticos. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.15 Plan de respuesta a emergencias.
	ACTIVOS SOFTWARE				
SW-std-os01	A.8 Difusión de software dañino	-	M	A	5.6.5 Controles de seguridad. 5.12 Documentación y revisión periódica. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.4 Experiencia 7.14.6 Actualización de inventario.
	A.18 Destrucción de información	-	M	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.15 Plan de recuperación a emergencias.
SW-std-os02	A.8 Difusión de software dañino	-	M	A	5.6.5 Controles de seguridad. 5.12 Documentación y revisión periódica. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.4 Experiencia 7.14.6 Actualización de inventario.
	A.18 Destrucción de información	-	M	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.15 Plan de recuperación a emergencias.
SW-std-os03	I.5Avería de origen físico o lógico	-	B	A	5.6.5 Controles de seguridad. 6.2.3 Cambio climáticos. 6.6 Controles ambientales. 7.5 Control de acceso lógico. 7.5.3 Autorización.

					7.5.8 Funciones y roles de seguridad. 7.6 Equipos de TIC y disponibilidad operativa.
	E.8 Difusión de software dañino	-	B	A	5.6.5 Controles de seguridad. 5.12 Documentación y revisión periódica. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.4 Experiencia 7.14.6 Actualización de inventario.
	E.18 Destrucción de información	-	B	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.15 Plan de recuperación a emergencias.
	A.6 Abuso de privilegios de acceso	-	M	A	7.4.3 Retención de conocimientos. 7.5 Control de acceso lógico. 7.5.8 Funciones y roles de seguridad. 7.6 Equipos de TIC y disponibilidad operativa. 7.8.3 Plataformas de hardware y software.
	A.8 Difusión de software dañino	-	A	A	5.6.5 Controles de seguridad. 5.12 Documentación y revisión periódica. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.4 Experiencia 7.14.6 Actualización de inventario.
	A.18 Destrucción de información	-	A	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.15 Plan de recuperación a emergencias.
SW-std-os04	I.5Avería de origen físico o lógico	-	B	A	5.6.5 Controles de seguridad. 6.2.3 Cambio climáticos. 6.6 Controles ambientales. 7.5 Control de acceso lógico. 7.5.3 Autorización. 7.5.8 Funcione y roles de seguridad. 7.6 Equipos de TIC y disponibilidad operativa.

SW-std-os05	E.8 Difusión de software dañino	-	B	A	5.6.5 Controles de seguridad. 5.12 Documentación y revisión periódica. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.4 Experiencia 7.14.6 Actualización de inventario.
	E.18 Destrucción de información	-	B	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.15 Plan de recuperación a emergencias.
	A.6 Abuso de privilegios de acceso	-	B	A	7.4.3 Retención de conocimientos. 7.5 Control de acceso lógico. 7.5.8 Funciones y roles de seguridad. 7.6 Equipos de TIC y disponibilidad operativa. 7.8.3 Plataformas de hardware y software.
	A.8 Difusión de software dañino	-	M	MA	5.6.5 Controles de seguridad. 5.12 Documentación y revisión periódica. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.4 Experiencia 7.14.6 Actualización de inventario.
	A.18 Destrucción de información	-	M	MA	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.15 Plan de recuperación a emergencias.
	A.8 Difusión de software dañino	-	M	A	5.6.5 Controles de seguridad. 5.12 Documentación y revisión periódica. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.4 Experiencia 7.14.6 Actualización de inventario.
	A.18 Destrucción de información	-	M	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad.

					7.15 Plan de recuperación a emergencias.
SW-std-os06	A.8 Difusión de software dañino	-	M	A	5.6.5 Controles de seguridad. 5.12 Documentación y revisión periódica. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.4 Experiencia 7.14.6 Actualización de inventario.
	A.18 Destrucción de información	-	M	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.15 Plan de recuperación a emergencias.
SW-std-os07	A.8 Difusión de software dañino	-	M	A	5.6.5 Controles de seguridad. 5.12 Documentación y revisión periódica. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.4 Experiencia 7.14.6 Actualización de inventario.
	A.18 Destrucción de información	-	M	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.15 Plan de recuperación a emergencias.
W-std-os08	A.8 Difusión de software dañino	-	M	A	5.6.5 Controles de seguridad. 5.12 Documentación y revisión periódica. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.4 Experiencia 7.14.6 Actualización de inventario.
	A.18 Destrucción de información	-	M	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.15 Plan de recuperación a emergencias.
SW-std-os09	A.8 Difusión de software dañino	-	M	A	5.6.5 Controles de seguridad. 5.12 Documentación y revisión periódica.

					6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.4 Experiencia 7.14.6 Actualización de inventario.
SW-std-os10	A.18 Destrucción de información	-	M	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.15 Plan de recuperación a emergencias.
	A.8 Difusión de software dañino	-	M	A	5.6.5 Controles de seguridad. 5.12 Documentación y revisión periódica. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.4 Experiencia 7.14.6 Actualización de inventario.
	A.18 Destrucción de información	-	M	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.15 Plan de recuperación a emergencias.
SW-std-1	E.20 Vulnerabilidades de los programas (software)	-	M	A	7.5.10 Incidentes de seguridad lógica 7.6.2 Políticas y procedimientos.
	E.21 Errores de mantenimiento/actualización de programas(software)	-	M	A	7.5 Control de acceso lógico. 7.8.3 Plataformas de hardware y software 7.14.4 Reentrenamiento del personal.
SW-std-dbm01	I.5Avería de origen físico o lógico	B	B	A	5.6.5 Controles de seguridad. 6.2.3 Cambio climáticos. 6.6 Controles ambientales. 7.5 Control de acceso lógico. 7.5.3 Autorización. 7.5.8 Funcione y roles de seguridad. 7.6 Equipos de TIC y disponibilidad operativa.
	E.1 Errores de los usuarios	B	B	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.14.4 Reentrenamiento del personal.

E.2 Errores del administrador	B	B	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.14.4 Reentrenamiento del personal.
E.8 Difusión de software dañino	B	B	A	5.6.5 Controles de seguridad. 5.12 Documentación y revisión periódica. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.4 Experiencia 7.14.6 Actualización de inventario.
E.18 Destrucción de información	B	B	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.15 Plan de recuperación a emergencias.
E.20 Vulnerabilidades de los programas (software)	B	M	A	7.5.10 Incidentes de seguridad lógica 7.6.2 Políticas y procedimientos.
E.21 Errores de mantenimiento/actualización de programas(software)	B	M	A	7.5 Control de acceso lógico. 7.8.3 Plataformas de hardware y software 7.14.4 Reentrenamiento del personal.
A.6 Abuso de privilegios de acceso	B	M	A	7.4.3 Retención de conocimientos. 7.5 Control de acceso lógico. 7.5.8 Funciones y roles de seguridad. 7.6 Equipos de TIC y disponibilidad operativa. 7.8.3 Plataformas de hardware y software.
A.8 Difusión de software dañino	B	M	A	5.6.5 Controles de seguridad. 5.12 Documentación y revisión periódica. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.4 Experiencia 7.14.6 Actualización de inventario.
A.18 Destrucción de información	B	M	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad.

SW-std-dbms02					7.15 Plan de recuperación a emergencias.
	I.5Avería de origen físico o lógico	M	M	MA	5.6.5 Controles de seguridad. 6.2.3 Cambio climáticos. 6.6 Controles ambientales. 7.5 Control de acceso lógico. 7.5.3 Autorización. 7.5.8 Funcione y roles de seguridad. 7.6 Equipos de TIC y disponibilidad operativa.
	E.1 Errores de los usuarios	M	M	MA	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.14.4 Reentrenamiento del personal.
	E.2 Errores del administrador	M	M	MA	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.14.4 Reentrenamiento del personal.
	E.8 Difusión de software dañino	M	M	MA	5.6.5 Controles de seguridad. 5.12 Documentación y revisión periódica. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.4 Experiencia 7.14.6 Actualización de inventario.
	E.18 Destrucción de información	M	M	MA	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.15 Plan de recuperación a emergencias.
	E.20 Vulnerabilidades de los programas (software)	M	A	MA	7.5.10 Incidentes de seguridad lógica 7.6.2 Políticas y procedimientos.
	E.21 Errores de mantenimiento/actualización de programas(software)	M	A	MA	7.5 Control de acceso lógico. 7.8.3 Plataformas de hardware y software 7.14.4 Reentrenamiento del personal.
	A.6 Abuso de privilegios de acceso	M	A	MA	7.4.3 Retención de conocimientos. 7.5 Control de acceso lógico.

					7.5.8 Funciones y roles de seguridad. 7.6 Equipos de TIC y disponibilidad operativa. 7.8.3 Plataformas de hardware y software.
	A.8 Difusión de software dañino	M	A	MA	5.6.5 Controles de seguridad. 5.12 Documentación y revisión periódica. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.4 Experiencia 7.14.6 Actualización de inventario.
	A.18 Destrucción de información	M	A	MA	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.15 Plan de recuperación a emergencias.
SW-std-2	E.20 Vulnerabilidades de los programas (software)	-	B	A	7.5.10 Incidentes de seguridad lógica 7.6.2 Políticas y procedimientos.
SW-std-3	E.21 Errores de mantenimiento/actualización de programas(software)	-	B	A	7.5 Control de acceso lógico. 7.8.3 Plataformas de hardware y software 7.14.4 Reentrenamiento del personal.
	E.20 Vulnerabilidades de los programas (software)	-	M	A	7.5.10 Incidentes de seguridad lógica 7.6.2 Políticas y procedimientos.
SW-std-4	E.21 Errores de mantenimiento/actualización de programas(software)	-	B	A	7.5 Control de acceso lógico. 7.8.3 Plataformas de hardware y software 7.14.4 Reentrenamiento del personal.
	E.20 Vulnerabilidades de los programas (software)	-	B	A	7.5.10 Incidentes de seguridad lógica 7.6.2 Políticas y procedimientos.
SW-std-5	E.21 Errores de mantenimiento/actualización de programas(software)	-	B	A	7.5 Control de acceso lógico. 7.8.3 Plataformas de hardware y software 7.14.4 Reentrenamiento del personal.
	I.5Avería de origen físico o lógico	-	M	A	5.6.5 Controles de seguridad. 6.2.3 Cambio climáticos. 6.6 Controles ambientales. 7.5 Control de acceso lógico. 7.5.3 Autorización.

					7.5.8 Funcione y roles de seguridad. 7.6 Equipos de TIC y disponibilidad operativa.
	E.2 Errores del administrador	-	M	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.14.4 Reentrenamiento del personal.
	E.8 Difusión de software dañino	-	M	A	5.6.5 Controles de seguridad. 5.12 Documentación y revisión periódica. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.4 Experiencia 7.14.6 Actualización de inventario.
	E.18 Destrucción de información	-	M	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.15 Plan de recuperación a emergencias.
	E.20 Vulnerabilidades de los programas (software)	-	A	MA	7.5.10 Incidentes de seguridad lógica 7.6.2 Políticas y procedimientos.
	E.21 Errores de mantenimiento/actualización de programas(software)	-	A	MA	7.5 Control de acceso lógico. 7.8.3 Plataformas de hardware y software 7.14.4 Reentrenamiento del personal.
	A.6 Abuso de privilegios de acceso	-	M	A	7.4.3 Retención de conocimientos. 7.5 Control de acceso lógico. 7.5.8 Funciones y roles de seguridad. 7.6 Equipos de TIC y disponibilidad operativa. 7.8.3 Plataformas de hardware y software.
	A.8 Difusión de software dañino	-	M	A	5.6.5 Controles de seguridad. 5.12 Documentación y revisión periódica. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.4 Experiencia 7.14.6 Actualización de inventario.

SW-std-6	I.5Avería de origen físico o lógico	B	M	A	5.6.5 Controles de seguridad. 6.2.3 Cambio climáticos. 6.6 Controles ambientales. 7.5 Control de acceso lógico. 7.5.3 Autorización. 7.5.8 Funcione y roles de seguridad. 7.6 Equipos de TIC y disponibilidad operativa.
	E.2 Errores del administrador	B	M	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.14.4 Reentrenamiento del personal.
	E.8 Difusión de software dañino	B	M	A	5.6.5 Controles de seguridad. 5.12 Documentación y revisión periódica. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.4 Experiencia 7.14.6 Actualización de inventario.
	E.18 Destrucción de información	B	M	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.15 Plan de recuperación a emergencias.
	E.20 Vulnerabilidades de los programas (software)	M	A	MA	7.5.10 Incidentes de seguridad lógica 7.6.2 Políticas y procedimientos.
	E.21 Errores de mantenimiento/actualización de programas(software)	M	A	MA	7.5 Control de acceso lógico. 7.8.3 Plataformas de hardware y software 7.14.4 Reentrenamiento del personal.
	A.6 Abuso de privilegios de acceso	B	M	A	7.4.3 Retención de conocimientos. 7.5 Control de acceso lógico. 7.5.8 Funciones y roles de seguridad. 7.6 Equipos de TIC y disponibilidad operativa. 7.8.3 Plataformas de hardware y software.
	A.8 Difusión de software dañino	B	M	A	5.6.5 Controles de seguridad. 5.12 Documentación y revisión periódica.

SW-std-7					6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.4 Experiencia 7.14.6 Actualización de inventario.
	I.5Avería de origen físico o lógico	B	M	A	5.6.5 Controles de seguridad. 6.2.3 Cambio climáticos. 6.6 Controles ambientales. 7.5 Control de acceso lógico. 7.5.3 Autorización. 7.5.8 Funcione y roles de seguridad. 7.6 Equipos de TIC y disponibilidad operativa.
	E.2 Errores del administrador	B	M	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.14.4 Reentrenamiento del personal.
	E.8 Difusión de software dañino	B	M	A	5.6.5 Controles de seguridad. 5.12 Documentación y revisión periódica. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.4 Experiencia 7.14.6 Actualización de inventario.
	E.18 Destrucción de información	B	M	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.15 Plan de recuperación a emergencias.
	E.20 Vulnerabilidades de los programas (software)	M	A	MA	7.5.10 Incidentes de seguridad lógica 7.6.2 Políticas y procedimientos.
	E.21 Errores de mantenimiento/actualización de programas(software)	M	A	MA	7.5 Control de acceso lógico. 7.8.3 Plataformas de hardware y software 7.14.4 Reentrenamiento del personal.
	A.6 Abuso de privilegios de acceso	B	M	A	7.4.3 Retención de conocimientos. 7.5 Control de acceso lógico. 7.5.8 Funciones y roles de seguridad. 7.6 Equipos de TIC y disponibilidad operativa.

SW-std-8					7.8.3 Plataformas de hardware y software.
	A.8 Difusión de software dañino	B	M	A	5.6.5 Controles de seguridad. 5.12 Documentación y revisión periódica. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.4 Experiencia 7.14.6 Actualización de inventario.
	I.5Avería de origen físico o lógico	B	M	A	5.6.5 Controles de seguridad. 6.2.3 Cambio climáticos. 6.6 Controles ambientales. 7.5 Control de acceso lógico. 7.5.3 Autorización. 7.5.8 Funcione y roles de seguridad. 7.6 Equipos de TIC y disponibilidad operativa.
	E.1 Errores de los usuarios	MB	B	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.14.4 Reentrenamiento del personal.
	E.2 Errores del administrador	B	M	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.14.4 Reentrenamiento del personal.
	E.8 Difusión de software dañino	MB	M	A	5.6.5 Controles de seguridad. 5.12 Documentación y revisión periódica. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.4 Experiencia 7.14.6 Actualización de inventario.
	E.18 Destrucción de información	B	M	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.15 Plan de recuperación a emergencias.
	E.20 Vulnerabilidades de los programas (software)	B	A	MA	7.5.10 Incidentes de seguridad lógica 7.6.2 Políticas y procedimientos.

SW-std-9	E.21 Errores de mantenimiento/actualización de programas(software)	B	A	MA	7.5 Control de acceso lógico. 7.8.3 Plataformas de hardware y software 7.14.4 Reentrenamiento del personal.
	A.6 Abuso de privilegios de acceso	B	M	A	7.4.3 Retención de conocimientos. 7.5 Control de acceso lógico. 7.5.8 Funciones y roles de seguridad. 7.6 Equipos de TIC y disponibilidad operativa. 7.8.3 Plataformas de hardware y software.
	A.8 Difusión de software dañino	B	M	A	5.6.5 Controles de seguridad. 5.12 Documentación y revisión periódica. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.4 Experiencia 7.14.6 Actualización de inventario.
	I.5Avería de origen físico o lógico	B	M	A	5.6.5 Controles de seguridad. 6.2.3 Cambio climáticos. 6.6 Controles ambientales. 7.5 Control de acceso lógico. 7.5.3 Autorización. 7.5.8 Funcione y roles de seguridad. 7.6 Equipos de TIC y disponibilidad operativa.
	E.1 Errores de los usuarios	MB	B	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.14.4 Reentrenamiento del personal.
	E.2 Errores del administrador	B	M	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.14.4 Reentrenamiento del personal.
	E.8 Difusión de software dañino	MB	M	A	5.6.5 Controles de seguridad. 5.12 Documentación y revisión periódica. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.4 Experiencia 7.14.6 Actualización de inventario.

	E.18 Destrucción de información	B	M	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.15 Plan de recuperación a emergencias.
	E.20 Vulnerabilidades de los programas (software)	B	A	MA	7.5.10 Incidentes de seguridad lógica 7.6.2 Políticas y procedimientos.
	E.21 Errores de mantenimiento/actualización de programas(software)	B	A	MA	7.5 Control de acceso lógico. 7.8.3 Plataformas de hardware y software 7.14.4 Reentrenamiento del personal.
	A.6 Abuso de privilegios de acceso	B	M	A	7.4.3 Retención de conocimientos. 7.5 Control de acceso lógico. 7.5.8 Funciones y roles de seguridad. 7.6 Equipos de TIC y disponibilidad operativa. 7.8.3 Plataformas de hardware y software.
	A.8 Difusión de software dañino	B	M	A	5.6.5 Controles de seguridad. 5.12 Documentación y revisión periódica. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.4 Experiencia 7.14.6 Actualización de inventario.
	ACTIVOS HARDWARE				
HW-host01	N.1 Fuego	MB	B	A	6.3.11 Incidentes (y debilidades) de seguridad física. 6.4.5 Sistemas de detección y alarma 6.4.5.3 Tipos de advertencia 6.4.16 Salud y seguridad del personal 6.8 Fuentes de alimentación 6.10 Protección contra incendios 6.12.4 Fuego y humo. 6.12.5.3 Iluminación 7.15 Plan de respuesta a emergencias. 7.15.6 Simulacros de emergencia

N.2 Daños de Agua	MB	B	A	6.3.11 Incidentes (y debilidades) de seguridad física. 6.2.3 Cambios climáticos 6.4.5 Sistemas de detección y alarma 6.12.2.3 Peligros potenciales 6.12.7 Consideraciones generales de instalación 6.12.8 Áreas de exclusión.
N.7 Fenómeno Sísmico	MB	B	A	6.2.2 Riesgos naturales 6.3.11 Incidentes (y debilidades) de seguridad física. 7.15.6 Simulacros de emergencia
I.1 Fuego	MB	B	A	6.3.11 Incidentes (y debilidades) de seguridad física. 6.4.5 Sistemas de detección y alarma 6.4.5.3 Tipos de advertencia 6.4.16 Salud y seguridad del personal 6.8 Fuentes de alimentación 6.10 Protección contra incendios 6.12.4 Fuego y humo. 6.12.5.3 Iluminación 7.15 Plan de respuesta a emergencias. 7.15.6 Simulacros de emergencia
I.2 Daños por agua	MB	B	A	6.3.11 Incidentes (y debilidades) de seguridad física. 6.4.5 Sistemas de detección y alarma 6.12.2.3 Peligros potenciales 6.12.7 Consideraciones generales de instalación 6.12.8 Áreas de exclusión.
I.6 Corte de suministro eléctrico	B	M	MA	5.2 Estabilidad ambiental. 6.2.9 Infraestructura de cableado 6.8 Fuente de alimentación 6.9 Gestión de cables 6.12.2.4 Fuente de alimentación 6.12.2.5 Conectividad eléctrica 6.12.2.3 Aire acondicionado 6.12.5.3 Iluminación
E.23 Errores de mantenimiento/actualización de equipos (hardware)	B	M	A	6.3 Controles de acceso físico 6.6.4 Redundancia 6.9 Gestión de cables 6.14.2 Políticas y procedimientos 6.14.8 Repuestos y accesorios

	E.24 Caída del sistema por agotamiento de recursos	B	M	A	6.4 Seguridad de instalaciones físicas. 6.6 Controles ambientales. 6.8 Fuente de alimentación. 7.7 Soporte de recuperación simultánea. 7.14.7 Servicios existentes. 7.15 Plan de respuesta a emergencias.
	A.6 Abuso de privilegios de acceso	B	M	A	5.7.3 Restricción y segregación de personal 6.3 Controles de acceso físico 6.4 Seguridad de instalaciones físicas 6.12.2.2 Acceso físico.
	A.24 Denegación de servicio	B	M	A	5.5 Gestión de proveedores. 5.5.2 Soporte de equipos críticos. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.15 Plan de respuesta a emergencias.
HW-host02	N.1 Fuego	A	M	A	6.3.11 Incidentes (y debilidades) de seguridad física. 6.4.5 Sistemas de detección y alarma 6.4.5.3 Tipos de advertencia 6.4.16 Salud y seguridad del personal 6.8.5 Fuentes de alimentación alternativas 6.8.6 Disyuntores de emergencia 6.10 Protección contra incendios 6.12.4 Fuego y humo. 6.12.5.3 Iluminación 7.15 Plan de respuesta a emergencias. 7.15.6 Simulacros de emergencia
	N.2 Daños de Agua	M	M	A	6.3.11 Incidentes (y debilidades) de seguridad física. 6.2.3 Cambios climáticos 6.4.5 Sistemas de detección y alarma 6.12.2.3 Peligros potenciales 6.12.7 Consideraciones generales de instalación 6.12.8 Áreas de exclusión.
	N.7 Fenómeno Sísmico	M	M	A	6.2.2 Riesgos naturales 6.3.11 Incidentes (y debilidades) de seguridad física. 7.15.6 Simulacros de emergencia

	I.1 Fuego	B	B	A	6.3.11 Incidentes (y debilidades) de seguridad física. 6.4.5 Sistemas de detección y alarma 6.4.5.3 Tipos de advertencia 6.4.16 Salud y seguridad del personal 6.8.5 Fuentes de alimentación alternativas 6.8.6 Disyuntores de emergencia 6.10 Protección contra incendios 6.12.4 Fuego y humo. 6.12.5.3 Iluminación 7.15 Plan de respuesta a emergencias. 7.15.6 Simulacros de emergencia
	I.2 Daños por agua	B	B	A	6.3.11 Incidentes (y debilidades) de seguridad física. 6.4.5 Sistemas de detección y alarma 6.12.2.3 Peligros potenciales 6.12.7 Consideraciones generales de instalación 6.12.8 Áreas de exclusión.
	I.5 Avería de origen físico o lógico	M	M	A	5.6.5 Controles de seguridad. 6.2.3 Cambio climáticos. 6.6 Controles ambientales. 7.5 Control de acceso lógico. 7.5.3 Autorización. 7.5.8 Funcione y roles de seguridad. 7.6 Equipos de TIC y disponibilidad operativa.
	I.6 Corte de suministro eléctrico	M	M	MA	5.2 Estabilidad ambiental. 6.2.9 Infraestructura de cableado 6.8 Fuente de alimentación 6.9 Gestión de cables 6.12.2.4 Fuente de alimentación 6.12.2.5 Conectividad eléctrica 6.12.2.3 Aire acondicionado 6.12.5.3 Iluminación
	E.2 Errores del administrador	B	B	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.14.4 Reentrenamiento del personal.

	E.23 Errores de mantenimiento/actualización de equipos (hardware)	M	M	A	6.3 Controles de acceso físico 6.6.4 Redundancia 6.9 Gestión de cables 6.14.2 Políticas y procedimientos 6.14.8 Repuestos y accesorios
	A.6 Abuso de privilegios de acceso	M	M	A	5.7.3 Restricción y segregación de personal 6.3 Controles de acceso físico 6.4 Seguridad de instalaciones físicas 6.12.2.2 Acceso físico.
	A.24 Denegación de servicio	M	M	A	5.5 Gestión de proveedores. 5.5.2 Soporte de equipos críticos. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.15 Plan de respuesta a emergencias.
HW-host03	I.6 Corte de suministro eléctrico	B	B	A	5.2 Estabilidad ambiental. 6.2.9 Infraestructura de cableado 6.8 Fuente de alimentación 6.9 Gestión de cables 6.12.2.4 Fuente de alimentación 6.12.2.5 Conectividad eléctrica 6.12.2.3 Aire acondicionado 6.12.5.3 Iluminación
HW-host04	I.6 Corte de suministro eléctrico	B	B	A	5.2 Estabilidad ambiental. 6.2.9 Infraestructura de cableado 6.8 Fuente de alimentación 6.9 Gestión de cables 6.12.2.4 Fuente de alimentación 6.12.2.5 Conectividad eléctrica 6.12.2.3 Aire acondicionado 6.12.5.3 Iluminación
HW-switch01	N.1 Fuego	MB	B	A	6.3.11 Incidentes (y debilidades) de seguridad física. 6.4.5 Sistemas de detección y alarma 6.4.5.3 Tipos de advertencia 6.4.16 Salud y seguridad del personal 6.8.5 Fuentes de alimentación alternativas 6.8.6 Disyuntores de emergencia 6.10 Protección contra incendios 6.12.4 Fuego y humo. 6.12.5.3 Iluminación 7.15 Plan de respuesta a emergencias. 7.15.6 Simulacros de emergencia

N.2 Daños de Agua	MB	B	A	6.3.11 Incidentes (y debilidades) de seguridad física. 6.2.3 Cambios climáticos 6.4.5 Sistemas de detección y alarma 6.12.2.3 Peligros potenciales 6.12.7 Consideraciones generales de instalación 6.12.8 Áreas de exclusión.
N.7 Fenómeno Sísmico	MB	B	A	6.2.2 Riesgos naturales 6.3.11 Incidentes (y debilidades) de seguridad física. 7.15.6 Simulacros de emergencia
I.5 Avería de origen físico o lógico	B	M	A	5.6.5 Controles de seguridad. 6.2.3 Cambio climáticos. 6.6 Controles ambientales. 7.5 Control de acceso lógico. 7.5.3 Autorización. 7.5.8 Funcione y roles de seguridad. 7.6 Equipos de TIC y disponibilidad operativa.
I.6 Corte de suministro eléctrico	B	M	MA	5.2 Estabilidad ambiental. 6.2.9 Infraestructura de cableado 6.8 Fuente de alimentación 6.9 Gestión de cables 6.12.2.4 Fuente de alimentación 6.12.2.5 Conectividad eléctrica 6.12.2.3 Aire acondicionado 6.12.5.3 Iluminación
E.2 Errores del administrador	MB	B	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.14.4 Reentrenamiento del personal.
E.23 Errores de mantenimiento/actualización de equipos (hardware)	B	M	A	6.3 Controles de acceso físico 6.6.4 Redundancia 6.9 Gestión de cables 6.14.2 Políticas y procedimientos 6.14.8 Repuestos y accesorios
E.24 Caída del sistema por agotamiento de recursos	B	M	A	6.4 Seguridad de instalaciones físicas. 6.6 Controles ambientales. 6.8 Fuente de alimentación. 7.7 Soporte de recuperación simultánea. 7.14.7 Servicios existentes. 7.15 Plan de respuesta a emergencias.

	A.6 Abuso de privilegios de acceso	B	M	A	5.7.3 Restricción y segregación de personal 6.3 Controles de acceso físico 6.4 Seguridad de instalaciones físicas 6.12.2.2 Acceso físico.
	A.24 Denegación de servicio	B	M	A	5.5 Gestión de proveedores. 5.5.2 Soporte de equipos críticos. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.15 Plan de respuesta a emergencias.
HW-firewall01	N.1 Fuego	MB	B	A	6.3.11 Incidentes (y debilidades) de seguridad física. 6.4.5 Sistemas de detección y alarma 6.4.5.3 Tipos de advertencia 6.4.16 Salud y seguridad del personal 6.8.5 Fuentes de alimentación alternativas 6.8.6 Disyuntores de emergencia 6.10 Protección contra incendios 6.12.4 Fuego y humo. 6.12.5.3 Iluminación 7.15 Plan de respuesta a emergencias. 7.15.6 Simulacros de emergencia
	N.2 Daños de Agua	MB	B	A	6.2.3 Cambios climáticos 6.3.11 Incidentes (y debilidades) de seguridad física. 6.4.5 Sistemas de detección y alarma 6.12.2.3 Peligros potenciales 6.12.7 Consideraciones generales de instalación 6.12.8 Áreas de exclusión.

	I.1 Fuego	MB	B	A	6.3.11 Incidentes (y debilidades) de seguridad física. 6.4.5 Sistemas de detección y alarma 6.4.5.3 Tipos de advertencia 6.4.16 Salud y seguridad del personal 6.8.5 Fuentes de alimentación alternativas 6.8.6 Disyuntores de emergencia 6.10 Protección contra incendios 6.12.4 Fuego y humo. 6.12.5.3 Iluminación 7.15 Plan de respuesta a emergencias. 7.15.6 Simulacros de emergencia
	I.2 Daños por agua	MB	B	A	6.3.11 Incidentes (y debilidades) de seguridad física. 6.4.5 Sistemas de detección y alarma 6.12.2.3 Peligros potenciales 6.12.7 Consideraciones generales de instalación 6.12.8 Áreas de exclusión.
	I.3 Contaminación mecánica	MB	B	A	6.6 Controles ambientales
	I.5 Avería de origen físico o lógico	B	M	A	5.6.5 Controles de seguridad. 6.2.3 Cambio climáticos. 6.6 Controles ambientales. 7.5 Control de acceso lógico. 7.5.3 Autorización. 7.5.8 Funcione y roles de seguridad. 7.6 Equipos de TIC y disponibilidad operativa.
	I.6 Corte de suministro eléctrico	B	M	MA	5.2 Estabilidad ambiental. 6.2.9 Infraestructura de cableado 6.8 Fuente de alimentación 6.9 Gestión de cables 6.12.2.4 Fuente de alimentación 6.12.2.5 Conectividad eléctrica 6.12.2.3 Aire acondicionado 6.12.5.3 Iluminación
	E.2 Errores del administrador	MB	M	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.14.4 Reentrenamiento del personal.

	E.23 Errores de mantenimiento/actualización de equipos (hardware)	B	M	A	6.3 Controles de acceso físico 6.6.4 Redundancia 6.9 Gestión de cables 6.14.2 Políticas y procedimientos 6.14.8 Repuestos y accesorios
	E.24 Caída del sistema por agotamiento de recursos	B	M	A	6.4 Seguridad de instalaciones físicas. 6.6 Controles ambientales. 6.8 Fuente de alimentación. 7.7 Soporte de recuperación simultánea. 7.14.7 Servicios existentes. 7.15 Plan de respuesta a emergencias.
	A.24 Denegación de servicio	MB	B	A	5.5 Gestión de proveedores. 5.5.2 Soporte de equipos críticos. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.15 Plan de respuesta a emergencias.
HW-switch02	N.1 Fuego	MB	B	A	6.4.5 Sistemas de detección y alarma 6.4.5.3 Tipos de advertencia 6.4.16 Salud y seguridad del personal 6.8.5 Fuentes de alimentación alternativas 6.8.6 Disyuntores de emergencia 6.10 Protección contra incendios 6.12.4 Fuego y humo. 6.12.5.3 Iluminación 7.15 Plan de respuesta a emergencias. 7.15.6 Simulacros de emergencia
	N.2 Daños de Agua	MB	B	A	6.2.3 Cambios climáticos 6.3.11 Incidentes (y debilidades) de seguridad física. 6.4.5 Sistemas de detección y alarma 6.12.2.3 Peligros potenciales 6.12.7 Consideraciones generales de instalación 6.12.8 Áreas de exclusión.
	I.1 Fuego	MB	B	A	6.3.11 Incidentes (y debilidades) de seguridad física. 6.4.5 Sistemas de detección y alarma 6.4.5.3 Tipos de advertencia 6.4.16 Salud y seguridad del personal

					6.8.5 Fuentes de alimentación alternativas 6.8.6 Disyuntores de emergencia 6.10 Protección contra incendios 6.12.4 Fuego y humo. 6.12.5.3 Iluminación 7.15 Plan de respuesta a emergencias. 7.15.6 Simulacros de emergencia
	I.2 Daños por agua	MB	B	A	6.3.11 Incidentes (y debilidades) de seguridad física. 6.4.5 Sistemas de detección y alarma 6.12.2.3 Peligros potenciales 6.12.7 Consideraciones generales de instalación 6.12.8 Áreas de exclusión.
	E.2 Errores del administrador	MB	M	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.14.4 Reentrenamiento del personal.
	E.23 Errores de mantenimiento/actualización de equipos (hardware)	B	M	A	6.3 Controles de acceso físico 6.6.4 Redundancia 6.9 Gestión de cables 6.14.2 Políticas y procedimientos 6.14.8 Repuestos y accesorios
	E.24 Caída del sistema por agotamiento de recursos	B	M	A	6.4 Seguridad de instalaciones físicas. 6.6 Controles ambientales. 6.8 Fuente de alimentación. 7.7 Soporte de recuperación simultánea. 7.14.7 Servicios existentes. 7.15 Plan de respuesta a emergencias.
	A.6 Abuso de privilegios de acceso	B	M	A	5.7.3 Restricción y segregación de personal 6.3 Controles de acceso físico 6.4 Seguridad de instalaciones físicas 6.12.2.2 Acceso físico.
	A.24 Denegación de servicio	B	M	A	5.5 Gestión de proveedores. 5.5.2 Soporte de equipos críticos. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.15 Plan de respuesta a emergencias.

HW-firewall02	N.1 Fuego	MB	B	A	6.3.11 Incidentes (y debilidades) de seguridad física. 6.4.5 Sistemas de detección y alarma 6.4.5.3 Tipos de advertencia 6.4.16 Salud y seguridad del personal 6.8.5 Fuentes de alimentación alternativas 6.8.6 Disyuntores de emergencia 6.10 Protección contra incendios 6.12.4 Fuego y humo. 6.12.5.3 Iluminación 7.15 Plan de respuesta a emergencias. 7.15.6 Simulacros de emergencia
	N.2 Daños de Agua	MB	B	A	6.3.11 Incidentes (y debilidades) de seguridad física. 6.4.5 Sistemas de detección y alarma 6.12.2.3 Peligros potenciales 6.12.7 Consideraciones generales de instalación 6.12.8 Áreas de exclusión.
	N.7 Fenómeno Sísmico	MB	B	A	6.2.2 Riesgos naturales 6.3.11 Incidentes (y debilidades) de seguridad física. 7.15.6 Simulacros de emergencia
	I.1 Fuego	MB	B	A	6.3.11 Incidentes (y debilidades) de seguridad física. 6.4.5 Sistemas de detección y alarma 6.4.5.3 Tipos de advertencia 6.4.16 Salud y seguridad del personal 6.8.5 Fuentes de alimentación alternativas 6.8.6 Disyuntores de emergencia 6.10 Protección contra incendios 6.12.4 Fuego y humo. 6.12.5.3 Iluminación 7.15 Plan de respuesta a emergencias. 7.15.6 Simulacros de emergencia

	I.2 Daños por agua	MB	MB	A	6.3.11 Incidentes (y debilidades) de seguridad física. 6.4.5 Sistemas de detección y alarma 6.12.2.3 Peligros potenciales 6.12.7 Consideraciones generales de instalación 6.12.8 Áreas de exclusión.
	I.5 Avería de origen físico o lógico	B	M	A	5.6.5 Controles de seguridad. 6.2.3 Cambio climáticos. 6.6 Controles ambientales. 7.5 Control de acceso lógico. 7.5.3 Autorización. 7.5.8 Funcione y roles de seguridad. 7.6 Equipos de TIC y disponibilidad operativa.
	I.6 Corte de suministro eléctrico	B	M	MA	5.2 Estabilidad ambiental. 6.2.9 Infraestructura de cableado 6.8 Fuente de alimentación 6.9 Gestión de cables 6.12.2.4 Fuente de alimentación 6.12.2.5 Conectividad eléctrica 6.12.2.3 Aire acondicionado 6.12.5.3 Iluminación
	E.2 Errores del administrador	MB	M	A	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.14.4 Reentrenamiento del personal.
	E.23 Errores de mantenimiento/actualización de equipos (hardware)	B	M	A	6.3 Controles de acceso físico 6.6.4 Redundancia 6.9 Gestión de cables 6.14.2 Políticas y procedimientos 6.14.8 Repuestos y accesorios
	E.24 Caída del sistema por agotamiento de recursos	B	M	A	6.4 Seguridad de instalaciones físicas. 6.6 Controles ambientales. 6.8 Fuente de alimentación. 7.7 Soporte de recuperación simultánea. 7.14.7 Servicios existentes. 7.15 Plan de respuesta a emergencias.
	A.24 Denegación de servicio	MB	B	A	5.5 Gestión de proveedores. 5.5.2 Soporte de equipos críticos. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.15 Plan de respuesta a emergencias.

ACTIVOS DATOS					
D-conf01	E.1 Errores de los usuarios	A	A	MA	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.14.4 Reentrenamiento del personal.
	E.2 Errores del administrador	A	A	MA	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.14.4 Reentrenamiento del personal.
	E.18 Destrucción de información	A	A	MA	6.8 Fuente de alimentación 7.5 Control de acceso lógico 7.5.10 Incidentes de seguridad lógica 7.6.2 Políticas y procedimientos 7.11.3 Privacidad y confidencialidad
	A.6 Abuso de privilegios de acceso	A	A	MA	7.4.3 Retención de conocimientos. 7.5 Control de acceso lógico. 7.5.8 Funciones y roles de seguridad. 7.6 Equipos de TIC y disponibilidad operativa
	A.18 Destrucción de información	A	A	MA	6.8 Fuente de alimentación 7.5 Control de acceso lógico 7.5.10 Incidentes de seguridad lógica 7.6.2 Políticas y procedimientos 7.11.3 Privacidad y confidencialidad
D-conf02	E.1 Errores de los usuarios	A	A	MA	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.14.4 Reentrenamiento del personal.
	E.2 Errores del administrador	A	A	MA	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.14.4 Reentrenamiento del personal.

	E.18 Destrucción de información	A	A	MA	6.8 Fuente de alimentación 7.5 Control de acceso lógico 7.5.10 Incidentes de seguridad lógica 7.6.2 Políticas y procedimientos 7.11.3 Privacidad y confidencialidad
	A.6 Abuso de privilegios de acceso	A	A	MA	7.4.3 Retención de conocimientos. 7.5 Control de acceso lógico. 7.5.8 Funciones y roles de seguridad. 7.6 Equipos de TIC y disponibilidad operativa
	A.18 Destrucción de información	A	A	MA	6.8 Fuente de alimentación 7.5 Control de acceso lógico 7.5.10 Incidentes de seguridad lógica 7.6.2 Políticas y procedimientos 7.11.3 Privacidad y confidencialidad
D-Conf03	E.1 Errores de los usuarios	A	A	MA	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.14.4 Reentrenamiento del personal.
	E.2 Errores del administrador	A	A	MA	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.14.4 Reentrenamiento del personal.
	E.18 Destrucción de información	A	A	MA	6.8 Fuente de alimentación 7.5 Control de acceso lógico 7.5.10 Incidentes de seguridad lógica 7.6.2 Políticas y procedimientos 7.11.3 Privacidad y confidencialidad
	A.6 Abuso de privilegios de acceso	A	A	MA	7.4.3 Retención de conocimientos. 7.5 Control de acceso lógico. 7.5.8 Funciones y roles de seguridad. 7.6 Equipos de TIC y disponibilidad operativa

	A.18 Destrucción de información	A	A	MA	6.8 Fuente de alimentación 7.5 Control de acceso lógico 7.5.10 Incidentes de seguridad lógica 7.6.2 Políticas y procedimientos 7.11.3 Privacidad y confidencialidad
ACTIVO REDES DE COMUNICACION					
COM-internet01	I.8 Fallo de servicios de comunicaciones	A	A	MA	6.7 Telecomunicaciones. 6.7.4 Protección. 6.9 Gestión de cables.
	E.2 Errores del administrador	M	A	MA	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.14.4 Reentrenamiento del personal.
	E.18 Destrucción de información	A	A	MA	6.8 Fuente de alimentación 7.5 Control de acceso lógico 7.5.10 Incidentes de seguridad lógica 7.6.2 Políticas y procedimientos 7.11.3 Privacidad y confidencialidad
	E.24 Caída del sistema por agotamiento de recursos	A	A	MA	6.4 Seguridad de instalaciones físicas. 6.6 Controles ambientales. 6.8 Fuente de alimentación. 7.7 Soporte de recuperación simultánea. 7.14.7 Servicios existentes. 7.15 Plan de respuesta a emergencias.
	A.6 Abuso de privilegio de acceso	A	A	MA	7.4.3 Retención de conocimientos. 7.5 Control de acceso lógico. 7.5.8 Funciones y roles de seguridad. 7.6 Equipos de TIC y disponibilidad operativa
	A.24 Denegación de servicio	A	A	MA	5.5 Gestión de proveedores. 5.5.2 Soporte de equipos críticos. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.15 Plan de respuesta a emergencias.

COM-internet02	I.8 Fallo de servicios de comunicaciones	A	A	MA	6.7 Telecomunicaciones. 6.7.4 Protección. 6.9 Gestión de cables.
	E.2 Errores del administrador	M	A	MA	5.7 Seguridad de la información. 5.9 Formación y educación. 6.3.9 Funciones y roles de seguridad. 7.14.4 Reentrenamiento del personal.
	E.18 Destrucción de información	A	A	MA	6.8 Fuente de alimentación 7.5 Control de acceso lógico 7.5.10 Incidentes de seguridad lógica 7.6.2 Políticas y procedimientos 7.11.3 Privacidad y confidencialidad
	E.24 Caída del sistema por agotamiento de recursos	A	A	MA	6.4 Seguridad de instalaciones físicas. 6.6 Controles ambientales. 6.8 Fuente de alimentación. 7.7 Soporte de recuperación simultánea. 7.14.7 Servicios existentes. 7.15 Plan de respuesta a emergencias.
	A.6 Abuso de privilegio de acceso	A	A	MA	7.4.3 Retención de conocimientos. 7.5 Control de acceso lógico. 7.5.8 Funciones y roles de seguridad. 7.6 Equipos de TIC y disponibilidad operativa
	A.24 Denegación de servicio	A	A	MA	5.5 Gestión de proveedores. 5.5.2 Soporte de equipos críticos. 6.14 Ciclo de vida de las instalaciones físicas y del equipo de apoyo. 7.15 Plan de respuesta a emergencias.

Fuente: Elaborado por el investigador

3.2 Diseño del Plan de Contingencia Informático

El diseño de un plan de contingencia permite aplicar medidas de seguridad ante la presencia de un desastre que afecte a los activos del Data Center del departamento de TI de la institución, minimizando o evitando que los riesgos de mayor impacto lleguen a materializarse, y de esta manera salvaguardar la información de la institución.

Es de vital importancia incluir actividades antes, durante y después de un desastre en el plan de contingencia, para una pronta y eficaz recuperación del funcionamiento de los servicios que presta la institución a toda la ciudadanía ambateña.

Además de roles y funciones bien definidas para el personal del departamento de TI, con la finalidad de contrarrestar eventos catastróficos que afectan a los diferentes tipos de activos y de esta manera dar continuidad a los servicios que brinda la institución.

GAD MUNICIPALIDAD DE AMBATO	**GOBIERNO AUTÓNOMO DESCENTRALIZADO DE LA MUNICIPALIDAD DE AMBATO**	AMBATO · LA GRAN CIUDAD ·
PLAN DE CONTINGENCIA INFORMÁTICO PARA EL DEPARTAMENTO DE TI		
CONTENIDO OBJETIVO ALCANCE DEFINICIONES ROLES Y FUNCIONES DESCRIPCION DE AMENAZAS ACTIVIDADES ANTES, DURANTE Y DESPUES DE UN DESASTRE		

OBJETIVO

Diseñar un plan de contingencia informático que permita dar continuidad a los servicios que brinda el departamento de TI de manera rápida, oportuna y eficiente.

ALCANCE

El diseño del plan de contingencia permite analizar la situación actual del departamento de TI, identificando las amenazas potenciales que pueden causar un gran impacto, incluyendo que acciones tomar antes, durante y después de un evento o desastre. El proyecto se limita a la fase de pruebas, por consiguiente, no será implementado, y queda a cargo del personal del departamento de TI.

DEFINICIONES

Plan de Contingencia: Un plan de contingencia permite identificar los riesgos (de origen natural o humano) a sistemas o recursos informáticos, para mantener la continuidad del negocio de la organización recuperando la totalidad de su

funcionalidad en el menor tiempo posible, proteger la información es primordial, para garantizar su integridad, confidencialidad y disponibilidad [10]**.**

Confidencialidad: La confidencialidad garantiza que la información solo es accesible e interpretada por personas o sistemas autorizados [30].

Integridad: Garantiza la autenticidad y precisión de la información, sin importar el momento en que esta se solicita [12]**.**

Disponibilidad: La disponibilidad intenta que los usuarios puedan acceder a los servicios con normalidad en el horario establecido. [31].

Activo: En relación con la seguridad de la información, se refiere a cualquier información o elemento relacionado con el tratamiento de esta (sistemas, soportes, edificios, personas...) que tenga valor para la organización [15].

Amenaza: Se entiende por amenaza una condición del entorno de los sistemas, áreas o dispositivos que contienen información importante (persona, equipo, suceso o idea) que ante determinada circunstancia podría dar lugar a que se produjese una violación de seguridad, afectando parte de la información y de la TI de la organización [32].

Vulnerabilidad: Constituye un hecho o una actividad que permite concretar una amenaza. Se es vulnerable en la medida en que no hay suficiente protección como para evitar que llegue a suceder una amenaza [33]**.**

Riesgo: El riesgo de seguridad de la información está asociado con el potencial de que las amenazas exploten las vulnerabilidades de un activo de información o grupo de activos de información y, por lo tanto, causen daños a una organización [15].

Impacto: Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza [23].

ROLES Y FUNCIONES

ROL	FUNCIONES
Director TI	• Verificar y aprobar el plan de contingencia. • Declarar la emergencia. • Involucrar a todo el personal en el plan de contingencia. • Revisar los informes después de una eventualidad, desastre o falla. • Realizar informes después de simulacros. • Coloca a disposición de ayuda externa de instituciones.
Jefatura de Desarrollo de Software	• Diagnosticar los sistemas nuevos y existentes. • Corregir errores en el software. • Supervisar líneas de código del programador. • Realizar el mantenimiento oportuno a los sistemas.
Jefatura de Infraestructura y Soporte Técnico	• Brinda mantenimiento preventivo y correctivo a los equipos informáticos. • Analizar la adquisición de nuevos equipos informáticos o componentes relacionados.
Analista de Seguridad Informática	• Responsable de gestionar y almacenar contraseñas. • Supervisar y restaurar las copias de seguridad de la información (backup) de las bases de datos y programas.
Analista de Redes	• Supervisar la infraestructura de la red y solucionar problemas. • Asegurar el funcionamiento de la red. • Verificación de direccionamiento IP.

DESCRIPCION DE AMENAZAS

1.- Denegación de servicio

Si un activo informático no se encuentra disponible para uso de los usuarios, provocaría que los servicios que brinda el departamento de TI, no se encuentren marchando con normalidad. La institución pública maneja una gran cantidad de información por lo que resulta accesible para personas que tenga intención de hacer daño o terminar con la continuidad de las actividades. El departamento de TI es el encargado de administrar los servicios y equipo informático relacionado, para ello cuenta con un sistema de Firewall.

Consecuencias:

- Inactividad en sitios web.
- Perdida de acceso a los principales servicios.
- Desestabilización institucional.
- Pérdidas económicas.

2.- Caída del sistema por agotamiento de recursos

Se debe contar con equipos informáticos el cual contenga las características necesarias para brindar un excelente trabajo, pues si no se cuenta con estas, existe la posibilidad de la caída de los sistemas, además los equipos deben estar en mantenimiento continuo para permitir su disponibilidad e integridad.

Consecuencias:

- Interrupción en los principales servicios.
- Interrupción laboral.
- Pérdidas económicas.

3.- Fugas de información

La fuga de información está relacionada con la perdida de confidencialidad, debido al acceso por parte del personal no autorizado. El GADMA cuenta con una asignación de perfil de usuario para todo el personal, el cual debe tener acceso estrictamente para realizar sus actividades diarias dependiendo su rol o función. Es importante tener a todo el personal bien capacitado para que haga uso responsable de los equipos, además de conocer el valor de la información para diseñar medidas de prevención.

Consecuencias:

- Pérdida de información.
- Interrupción laboral.
- Interrupción en los principales servicios.

4.- Avería de origen físico o lógico

El deterioro de hardware en los equipos informáticos suele suceder por diversos factores, entre ellos, por el tiempo de uso, falta de mantenimiento, acumulación de polvo, desperfectos eléctricos, apagado incorrecto, sobrecalentamiento, entre otros.

El fallo en la configuración de los equipos suele estar relacionado con errores de los usuarios, virus o sabotaje, los cuales afectan al rendimiento de la institución.

Consecuencias:

- Pérdidas económicas.
- Lentitud en los equipos.
- Interrupción en los principales servicios.
- Pérdida de información.
- Apagones repentinos en los equipos.

5.-Errores de usuarios

Los usuarios (empleados municipales y contribuyentes) que utilizan los servicios y equipos informáticos pueden tener equivocaciones al momento de manejar los mismos, puede suceder por falta de conocimiento o negligencia laboral, lo que perjudicaría el rendimiento y la disponibilidad de estos, poniendo en riesgo la confidencialidad de la información y como resultado la suspensión de las actividades de la institución.

Consecuencias:

- Interrupción de los principales servicios.
- Fallo en equipos.
- Pérdidas económicas.
- Pérdida de información.

6.- Errores del administrador

El usuario con el rol de administrador debe entender sus responsabilidades y obligaciones dentro de la institución ya que son profesionales cuyo conocimiento radica a su profesión, por ello es importante capacitar a todo el personal de TI acerca de la seguridad de la información, para reducir riesgos de error humano, pues cuando se da el caso de reemplazo del personal también existe alto riesgo de pérdida de información.

Consecuencias:

- Interrupción de los principales servicios.
- Fallo en equipos.
- Pérdidas económicas.
- Pérdida de información.

7.- Difusión de software dañino

El GADMA utiliza software con licencias perpetuas, además tiene implementado un sistema de antivirus el cual se actualiza automáticamente en todos los computadores, de forma que los dispositivos externos como CD, DVD, USB, etc., son inspeccionados inmediatamente, detectando y eliminando las amenazas.

Consecuencias:

- Pérdida de información.
- Lentitud en equipos.
- Interrupción de los principales servicios.

8.- Vulnerabilidades de los programas (software)

Para el manejo de códigos, el departamento de TI cuenta con profesionales dedicados a esa área, sin embargo, si se diera el caso de reemplazo del personal, puede tener consecuencias en la integridad de los datos o la capacidad de operación de las actividades que brinda la institución a la ciudadanía.

Consecuencias:

- Interrupción de los principales servicios.
- Pérdida de información.
- Interrupción laboral.

9.- Errores de mantenimiento/ actualización de programas (software)

Existe personal específico del departamento de TI, que puede dar mantenimiento o actualización a los programas, sin embargo, puede presentarse factores como: desinstalación incorrecta de aplicaciones, uso inadecuado de dispositivos de almacenamiento externo, entre otros, provocando fallas en los sistemas y paralizando las actividades de la institución.

Consecuencias:

- Daño en equipos.
- Interrupción laboral.
- Interrupción en los principales servicios.
- Pérdidas económicas.

10.- Abuso de privilegio de acceso

El acceso al Data Center está absolutamente restringido, mediante un control biométrico y monitoreo constante por medio de cámaras, el personal autorizado es únicamente del área de Infraestructura y Soporte quienes además tienen acceso remoto a la red mediante VPN y TeamViewer. El acceso a diferentes sitios está inspeccionado por carnés de identificación del personal del GADMA, mientras que a los contribuyentes se les controla con tarjetas de visitantes.

Consecuencias:

- Pérdida de informacion.
- Pérdidas materiales.
- Interrupción laboral.
- Interrupción en los principales servicios.

11.- Fuego

El fuego es un factor crítico para la infraestructura del Data Center, donde se encuentran lo activos más importantes del departamento de TI, y por consiguiente de la institución, ya que conlleva a la indisponibilidad de estos, paralizando las actividades de la institución. El GADMA cuenta con dispositivos (extintores y detectores de humo), un sistema antiincendios para combatir el fuego, que se

encuentran en diferentes oficinas, además en cada piso del edificio matriz se encuentra tomas y mangueras de agua.

El Data Center cuenta con un sistema de aspersión automática con gas para proteger a los equipos.

Consecuencias:

- Daño en equipos.
- Pérdidas de información.
- Pérdidas económicas.
- Interrupción laboral.
- Interrupción a los principales servicios.

12.- Daños de agua

El cantón Ambato, tiene una baja amenaza relacionada a las inundaciones, han ocurrido menos de 20 entre 1988 y el 2010, las cuales se registran por lo general entre los meses de marzo a mayo y de octubre a diciembre. En la parroquia de Huachi Chico donde en encuentra el edificio matriz del GADMA, se producen avenidas de flujos de lodo, a pesar de ubicarse en una zona seca, tiene sectores de posibles inundaciones, como se muestra en la figura (de inundaciones). Además, existen otros factores que provocan daños a los activos informáticos tales como: fugas de la tubería de agua, conexiones de agua en mal estado, servicios higiénicos cerca del Data Center, entre otros.

Consecuencias:

- Interrupción laboral.
- Pérdidas materiales.
- Pérdidas económicas.
- Interrupción en los principales servicios.

13.- Fenómeno sísmico

Como se muestra en la figura (Movimiento de Masas), el cantón de Ambato presenta movimientos continuos de las placas tectónicas, por lo que existe una gran cantidad de fallas geológicas, por ello es necesario construir estructuras seguras (antisísmicas), o reforzar las existentes. La infraestructura donde se encuentra el Data Center podría

superar un evento catastrófico manteniendo a salvo los servidores y toda la información, pues si llegase a suceder afectaría la operatividad del GADMA.

Consecuencias:

- Pérdidas materiales.
- Interrupción laboral.
- Pérdidas económicas.
- Interrupción en los principales servicios.

14.- Contaminación mecánica

Para resguardar los equipos informáticos del polvo o suciedad, se debe realizar una limpieza, especialmente de los componentes eléctricos, discos magnéticos, entre otros, para evitar daño se puede utilizar, franelas, aire comprimido, brochas de cerdas suaves. Al existir acumulación de partículas de polvo pueden provocar sobrecalentamiento en los equipos del Data Center, incluyendo el aire acondicionado.

Consecuencias:

- Daños en equipos.
- Interrupción en los principales servicios.
- Interrupción laboral.
- Pérdidas materiales.

15.- Corte de suministro eléctrico

Según históricos de la institución, los cortes de suministro eléctrico en el GADMA son frecuentes, para ello cuentan con un UPS en el Data Center, el mismo que se encuentra con fallas, al ocurrir este corte tiene un impacto negativo para todos los equipos informáticos, pues interrumpen el trabajo dejando graves consecuencias. Los cambios regulares de voltaje pueden dañar los equipos, normalmente, cuando se baja el voltaje todo equipo eléctrico se apaga, pero cuando vuelve es cuando se producen daños en los equipos. En cuanto a los tomacorrientes si llegasen a calentarse, a la larga el material aislante de los cables y enchufes se derrite y puede producir cortocircuitos o quema de los mismos interrumpiendo el paso de energía eléctrica.

Consecuencias:

- Daño en el cableado.
- Daño en equipos.
- Pérdida de información.
- Interrupción en los principales servicios

16.- Errores de mantenimiento/actualización de equipos (hardware)

El departamento de TI cuenta con un equipo técnico que realizan las labores de mantenimiento preventivo de los equipos informáticos, sin embargo, existen factores como: el tiempo de vida útil de los equipos, sobrecalentamiento por partículas de polvo en equipos de Data Center, fallos en componente internos, entre otros, los cuales provocan fallos en los equipos.

Consecuencias:

- Daños en equipos.
- Interrupción en los principales servicios.
- Pérdidas económicas.
- Interrupción laboral.

17.- Fallo de los servicios de comunicación

Cuando un activo informático no tiene la capacidad de transmitir datos de un sitio a otro se debe a un daño físico, por ello se debe revisar que las instalaciones de red funcionen correctamente para que no exista fallos de comunicación entre los equipos.

Consecuencias

- Interrupción en los principales servicios.
- Interrupción laboral.
- Daños económicos.
- Daños en equipos.

ACTIVIDADES ANTES, DURANTE Y DESPUES DE UN DESASTRE

1.- Denegación de servicios

ACTIVIDADES ANTES

Medidas Técnicas

- Disponer de un excelente Proveedor de Servicio de Internet.
- Verificar que la conexión y configuración entre los routers de la red interna con los Proveedores de Servicio de Internet (ISP) se encuentre correcta.
- Utilizar un equipo o software específico para firewall.
- Poseer equipos para redundancia y balanceo la carga, ya que, si un equipo se cae, el otro asumirá el trabajo.
- Mantener el software actualizado de todos los equipos, para evitar cualquier tipo de ataque que vulnere las actividades de la institución.
- Mantener el antivirus actualizado en todos los equipos.
- Contar con un plan de pruebas de las aplicaciones expuestas a la red.
- Capacitar a todo el personal de TI sobre ataques informáticos, mediante charlas o reuniones para que se encuentren preparados ante cualquier tipo de ataque.
- En analista de seguridad informática deberá realizar copias de seguridad de información relevantes como: bases de datos, aplicaciones, entre otros.

ACTIVIDADES DURANTE

Medidas Técnicas

- El personal de soporte técnico debe monitorear el software de antivirus y firewall permitiendo detectar ataques que puedan afectar las actividades de la institución.
- El personal de soporte técnico se encargará de identificar cuales son los equipos que han sido afectados por este tipo de ataque, aislándolos para un breve análisis.

- En caso de reemplazo o adquisición de equipos informáticos el jefe de infraestructura y soporte técnico deberá seguir los siguientes pasos:
    - Adquirir el equipo con características similares.
    - Instalar el sistema operativo.
    - Instalar controladores.
    - Reiniciar el equipo.

  Además:
    - Estimar los tiempos de entrega de equipos y repuestos.
    - Garantía en caso de desperfectos.
    - Soporte en instalación y capacitación.
    - Para cada componente, detallar la siguiente información:
        - Descripción (nombre, serie, fecha de adquisición)
        - Fabricantes.
        - Proveedores.
        - Disponibilidad.
        - Tiempo de entrega e instalación.
- El analista de seguridad informática verificará que el firewall se encuentre activo, para evitar que intrusos puedan acceder a la red y así vulnerar a los servidores.
- El analista de redes deberá examinar los equipos infectados y eliminar dichas infecciones mediante un software de seguridad que:
    - Realice un seguimiento a las direcciones IP de toda la red
    - Gestione los picos de tráfico en toda la red.
    - Analice las IP de destino y puertos que se encuentren abiertos.
- El analista de redes deberá reforzar el tráfico de la red mediante subredes y reglas de firewall que permita proteger de las conexiones de tráfico no deseado.

ACTIVIDADES DESPUES

Medidas Técnicas

- Una vez detectado el ataque, contactar al analista de redes encargado para que realice:
    - Un bloqueo de las IP que muestren un comportamiento anormal.

- Restringir el acceso a los sitios web.
- Mantener habilitadas las aplicaciones más importantes.

- El analista de seguridad informática deberá:
  - Importar las copias de seguridad que se efectúo anteriormente.
  - Restaurar los archivos necesarios para el normal funcionamiento de los servicios
- El personal de soporte técnico deberá realizar un informe detallado de los incidentes (y debilidades) e informar al director de TI, en el cual debe abarcar:
  - Detección de incidentes de seguridad de la información.
  - Registrar e informar a todas las partes involucradas acerca de los incidentes de seguridad de la información.
  - Registrar las acciones preventivas y correctivas.
  - Evaluar periódicamente todos los incidentes de seguridad de la información.
  - Realizar mejoras en la seguridad de la información.
- Establecer políticas y procedimientos para la reparación, mantenimiento o reemplazo, para mantener a los equipos en buenas condiciones.
- El director de TI debe asegurarse que el personal cumpla con todas las responsabilidades asignadas ante un evento inesperado.
- El equipo de infraestructura y soporte técnico deberá anotar en la bitácora los acontecimientos sucedidos.

2.- Caída del sistema por agotamiento de recursos

ACTIVIDADES ANTES

Medidas Técnicas

- El Data Center debe contar con aire acondicionado, para evitar el sobrecalentamiento de los equipos informáticos que almacenan información relevante.
- El jefe de infraestructura y soporte técnico debe verificar que el sitio en donde se encuentra el Data Center alterno sea seguro para almacenar registros vitales, medios magnéticos y suministros, mediante controles de temperatura y

humedad, además que se encuentre en un lugar geográfico alejado de los riesgos que afectan al Data Center principal.

- El personal de soporte técnico debe realizar mantenimiento preventivo de hardware y software en los equipos.
- Contar con equipos de hardware de alta disponibilidad.
- El analista de seguridad informática debe realizar copias de seguridad (backup), para resguardar toda la información que maneja la institución, mediante:
    - Creación de imágenes de los sistemas operativos.
    - Creación de puntos de restauración.
    - Copia de seguridad de archivos, base de datos, aplicaciones y demás información relevante de la institución en equipos de respaldo.
- El personal de soporte técnico debe mantener el antivirus actualizado en todos los equipos.
- En caso de reemplazo de equipos, el jefe de infraestructura y soporte técnico debe asegurarse que estos no afecten a la institución.

ACTIVIDADES DURANTE

Medidas Técnicas

El analista de seguridad informática del departamento de TI deberá:

- Monitorear constante del rendimiento de los servidores del Data Center principal, mediante pantallas donde se debe visualizar:
    - El porcentaje del tiempo de inactividad.
    - El porcentaje de errores.
    - El tráfico saliente, entrante y total.
    - Consumo de ancho de banda en tiempo real.
- Verificar el normal funcionamiento del firewall:
    - Definiendo reglas.
    - Construyendo VPNs.
    - Funcionalidad del acceso remoto.
    - Mitigación de amenazas.

- Brindar seguimiento a los sistemas que se han caído, mediante los siguientes pasos:
    - Verificar si es un servidor virtual.
    - Reiniciar el o los servidores que han sido afectados, mediante el emulador de terminal Putty.
    - Revisar el contenido de los archivos logs para identificar el fallo de la caída de los servicios.
- Mantener la redundancia en los equipos para que los servicios se encuentren disponibles y la ciudadanía tenga acceso:
    - Sistemas RAID para discos duros.
    - La información de respaldo debe ser enviar al sitio alterno seguro (Data Center alterno).
- El equipo de soporte técnico debe identificar los equipos afectados, mediante el sistema de antivirus, el mismo que detecta y elimina amenazas.
- El proveedor de fuentes de alimentación deberá contar con una continua y estable para el normal funcionamiento de los equipos, que:
    - Cumpla con los estándares mínimos de redundancia, seguridad y calidad.
    - Minimice puntos de fallo, mediante fuentes alternativas como UPS y generadores.
    - Proteja a los equipos de daños ante aumento de potencia o sobretensiones.

ACTIVIDADES DESPUÉS

Medidas Técnicas

- El equipo de infraestructura y soporte técnico debe hacer uso de los datos históricos para realizar un análisis y una comparativa del incidente.
- El analista de seguridad informática deberá restaurar las copias de seguridad que se realizó previamente.
- El equipo de infraestructura y soporte técnico deberá verificar el rendimiento de los equipos informáticos mediante:
    - Carga de trabajo.

- Aumento en la actividad de los usuarios.
- Uso de aplicaciones de gran tamaño.

- Todo el personal de Ti deberá cumplir con las responsabilidades asignadas ante la presencia de eventos imprevistos para restaurar de manera rápida las actividades que brinda la institución.
- Establecer políticas y procedimientos para disponer de un suministro de energía eléctrica, para evitar pérdida de información vital para la institución.
- El equipo de infraestructura y soporte técnico deberá anotar en la bitácora los acontecimientos sucedidos.

3.- Fugas de información

ACTIVIDADES ANTES

Medidas Técnicas

- El jede de infraestructura y soporte técnico restringirá el acceso físico a las instalaciones donde se almacenan los sistemas y equipos de gran valor para la institución (Data Center).
- Cada jefe de cada grupo de trabajo del departamento de Ti debe brindar capacitaciones al personal nuevo que ingrese a la institución.
- El departamento de TI debe contar con un control de acceso, asignando para cada empleado municipal un usuario y contraseña dependiendo el cargo que desempeña en la institución. Se recomienda que la contraseña sea fuerte y difícil de descifrar, además no se debe almacenar en lugares visibles o de fácil acceso.
- El uso del equipo informático es para el ámbito laboral, mas no personal.
  El analista de seguridad informática debe:
- Revisar la configuración del firewall.
- Tener un control de copias de seguridad.
- Para mantener la integridad y confidencialidad de los datos que maneja la institución, se realiza copias de seguridad diarias, almacenándolas en los servidores ubicados en el Data Center alterno.

- Brindar formación a todo el personal de TI una vez al año con el fin de garantizar resultados satisfactorios ante un desastre, mediante:
    - Formación de introducción, que facilite conocimientos básicos para todo el personal que se integre al departamento de TI.
    - Formación de nivel avanzado, que bride funciones concretas para el personal específico.
    - Formación continua, para garantizar el desempeño en las funciones.
    - Formación para evaluar y mantener la capacidad del personal ante la presencia de eventos imprevistos.

  Categorización de la seguridad de personal:
    - Proveedores de servicios.
    - Empleados de la institución.
    - Contratistas.
    - Visitantes.
- Contar con procedimientos para hacer frente a la incorporación o salida del personal, que cubra:
    - Nivel de acceso autorizado para el personal que se integre, mediante la emisión de credenciales o tarjetas de control de acceso físico.
    - Aviso inmediato de la renuncia del personal, anulación de autorizaciones de acceso y entrega de credenciales o tarjetas de control de acceso físico.
- Control sobre el ingreso de personas ajenas a la institución, se debe tener un registro de:
    - Datos personales (incluyendo el nombre de la institución a la cual pertenece).
    - Propósito de entrada y salida.
    - Tiempo de entrada y salida.
    - Comentarios.
    - Firma.
- Todo el personal junto con el director de TI debe definir políticas donde el personal de la institución tenga claro cuáles son actividades que desempeña.

ACTIVIDADES DURANTE

Medidas Técnicas

- El GADMA maneja una gran cantidad de información, por lo que se debe realizar reuniones con el personal encargado de la seguridad de la información, para comprobar la cantidad de información que haya sido sustraída, además identificar cuáles fueron las causas, ya sea de origen humano o técnico, si es humano identificar a los responsables de la fuga, si es técnico identificar los sistemas o servicios afectados.
- Durante un desastre o falla, todo el personal del departamento de TI tiene acceso las 24 horas del día.
- La información que maneja la institución no debe ser accesible para otra institución, a menos que esta lo autorice, la información debe encontrarse resguardada en sitios seguros como:
    - Data Center alterno para respaldos.
- Identificar y segregar al personal del departamento de TI para el control del acceso físico al Data Center principal y alterno, los cuales deben ubicarse en sitios independientes.

ACTIVIDADES DESPUÉS

Medidas Técnicas

- El personal de soporte técnico debe seguir un procedimiento para hacer frente a estos incidentes (y debilidades), en el cual debe abarcar:
    - Detección de todos los incidentes de seguridad de la información.
    - Registrar e informar a todas las partes involucradas acerca de los incidentes de seguridad de la información.
    - Registrar las acciones preventivas y correctivas.
    - Evaluar periódicamente todos los incidentes de seguridad de la información.
    - Realizar mejoras en la seguridad de la información.

- Todo el personal junto con el director de TI debe definir políticas donde el personal de la institución tenga claro cuáles son actividades que desempeña.

4.- Avería de origen físico o lógico

ACTIVIDADES ANTES

Medidas Humanas

En el caso de origen físico:

- Disponer con proveedores para cambios, mantenimiento o alquiler de equipos informáticos.
- Ubicar extintores en sitios en donde requieran protección, como el Data Center, que el personal reciba información del uso, que se pueda alcanzar y activar fácilmente, además deben estar en lugar visible y recibir un mantenimiento adecuado.
- El director de TI debe asignar funciones y roles de seguridad al personal, que abarque:
    - Designación del personal para la seguridad física.
    - Designación de diputados para funciones y roles críticos.
    - Capacitación para todo el personal antes de designar funciones y roles de seguridad.
    - Asistencia a cursos periódicos para verificar la capacidad en el desempeño de sus funciones.
    - Evaluar al personal para asegurar su conocimiento.
- Contar con la categorización de la seguridad de personal:
    - Proveedores de servicios.
    - Empleados de la institución.
    - Contratistas.
    - Visitantes.

En el caso de origen lógico:

- Todo el personal pertinente debe estar capacitado cuando exista actualizaciones de instalaciones de software, o cuando exista cambios de software.

- Establecer políticas y procedimientos para la instalación de software.

Medidas Técnicas

En el caso de origen físico:

- Asegurarse de que solo el personal autorizado tenga en control de acceso de la seguridad física de los equipos que se encuentran en el Data Center principal.
- Los cambios climáticos extremos y repentinos pueden afectar las instalaciones del Data Center principal y alternos, por tal motivo, estos sitios deben estar ubicados en zonas alejadas a este tipo de amenaza.
- Los Data Center tanto principal como alterno deben ubicarse en áreas con buena accesibilidad mediante:
    - Sistema vial integral.
    - Transporte hasta llegar al sitio de recuperación.
- Las instalaciones de los Data Center no deben ubicarse cerca de las instalaciones se servicio público como:
    - Plantas de energía.
    - Torres de transmisión de telecomunicaciones.
    - Líneas ferroviarias subterráneas y de superficie.
- El personal profesional calificado debe comprobar periódicamente que la conectividad eléctrica se encuentra en buen estado, ya que se puede generar calor a partir de conexiones sueltas, las mismas que pueden representar un peligro potencial.
- Tener alternativas de fuentes de alimentación como UPS y generadores para que equipos informáticos operen de manera ordenada, estas fuentes deben recibir un mantenimiento adecuado y probarse periódicamente para respaldar los sistemas de la institución durante un desastre. Además, deben estar debidamente separados de los equipos que requieren alta disponibilidad.
- Deben asegurarse de mantener inventarios actualizados de sus instalaciones físicas y artículos de equipamiento, en donde conste:
    - Lista de todos los activos.
    - Etiquetas para identificación de manera única.

En caso de subcontratación:

- No se puede poner el nombre de la institución como etiqueta.
- Se informa a la institución cuando los activos están siendo reubicados.
- Los activos se devuelven dentro del plazo determinado y acordado.

- Procedimientos para la protección de todo el cableado:
  - Los cables de telecomunicaciones y de alimentación deben estar separados para evitar interferencias.
  - Los cables que se encuentran expuestos al público deben estar protegidos con cableado oculto con material adecuado para proteger de daños físicos.
  - Los cables se escogen en cuanto a la función de los requisitos de transmisión y del entorno externo.
  - Todo el cableado, bandejas y conductos se comprueban periódicamente para identificar daños o riesgos potenciales.

En el caso de origen lógico:

- Procedimientos para el control de acceso lógico:
  - La información que maneja la institución no puede ser revelada a otra institución.
  - Responsabilidad del mantenimiento de control de acceso lógico es del personal encargado del departamento de TI.
  - El personal del departamento de TI es el encargado de las instalaciones de control de acceso lógico para las operaciones durante la recuperación.
- El directo de TI deberá asignar funciones y roles de seguridad al personal para el acceso lógico.
- Los desarrolladores de software deberán realizar respaldos de los códigos fuentes de los sistemas desarrollados internamente.
- Mantener inventario actualizados de software utilizado en el GADMA.
- Contar con profesionales en conocimientos basados en software.
- Respaldar toda la información en los principales activos del Data Center alterno que posee la institución, mediante:
  - Creación de imágenes de los sistemas operativos.

- Creación de puntos de restauración.
- Copia de seguridad de archivos, base de datos, aplicaciones y demás información relevante de la institución en equipos de respaldo.

ACTIVIDADES DURANTE

Medidas Humanas

- Cualquier evento que se presente en la institución, se debe informar al departamento de TI.

Medidas Técnicas

En el caso de origen físico:

- Verificar que las instalaciones tanto para el Data Center principal como el alterno cuente con buenas medidas de seguridad física, así como:
  - Construcción sólida de paredes externas.
  - Todas las puertas deben estar protegidas con cerraduras y alarmas.
  - Paredes de losa a losa para evitar la contaminación de fuego o humo.
- Cumplir con el comportamiento del personal en las instalaciones del Data Center mediante:
  - Prohibición de fumar.
  - Prohibición de alimentos y bebidas.
  - Condiciones para el uso de dispositivos que generen radiofrecuencia.
  - Condiciones para el uso de dispositivos de almacenamiento.
- Si se presenta daños en el disco duro:
  - No se debe realizar movimientos bruscos a los equipos informáticos, porque los cabezales de lectura y escritura pueden dañar el disco duro.
  - Verificar las fuentes de alimentación, ya que si se ocurre una subida de tensión puede afectar a las partes vitales de un disco duro.
  - Revisar las medidas de temperatura y humedad del Data Center, donde se encuentra alojados los equipos donde se almacena información valiosa de la institución.
  - Formatear o particionar la unidad errónea.

- Si el equipo fue remplazado el personal responsable deberá realizar el siguiente proceso para dar continuidad a los servicios que brinda la institución a la ciudadanía:
    - Adquirir el equipo con características similares.
    - Instalar el sistema operativo.
    - Instalar controladores.
    - Reiniciar el equipo.

En el caso de origen lógico:

- El analista de seguridad informática debe contar con listas de control de acceso lógico:
    - Para cada uno del personal (usuario y contraseña).
    - Registro de los usuarios que realizaron cambios de lectura, escritura, modificación o eliminación de información.
    - Suspensión de los usuarios en un determinado número de intentos en inicio de sesión.
- El analista de seguridad informática debe realizar procedimientos para el control de acceso lógico de manera temporal:
    - Autorización y creación de perfil "invitado"
    - Tiempo y duración de uso.
    - Verificación del registro de actividad.
    - Realizar mejoras en la seguridad de la información

ACTIVIDADES DESPUÉS

Medidas Técnicas

En el caso de origen físico:

- El personal de TI encargado debe asegurarse que todos los equipos informáticos y relacionados se encuentren protegidos contra la sobreprotección eléctrica incluyendo:
    - Dispositivos de protección contra sobretensión los mismos serán revisados periódicamente después de incidentes, y reemplazados si están dañados.

- Mantener la redundancia en los equipos para que los servicios se encuentren disponibles y la ciudadanía tenga acceso, mediante:
    - Sistemas RAID para discos duros.
    - La información de respaldo debe ser enviar al sitio alterno seguro (Data Center alterno).

En el caso de origen lógico:

- El personal de soporte técnico puede utilizar equipos y software adicionales que no afecten la seguridad y el funcionamiento del equipo posteriormente:
    - El software se puede instalar o activar de forma remota para solucionar problemas, el mismo se debe desactivar y borrar por completo antes de instalar en el equipo reparado.
    - Los equipos que son puesto nuevamente en servicios deben ser revisados y probados para verificar su configuración y normal funcionamiento, además debe ser apagado y reiniciado antes de ser puesto en servicio.
- El personal de soporte técnico debe identificar los daños que causó la avería y seguir el procedimiento para hacer frente a estos incidentes (y debilidades) e informar al director de TI, en el cual debe abarcar:
    - Detección de todos los incidentes de seguridad de la información.
    - Registrar e informar a todas las partes involucradas acerca de los incidentes de seguridad de la información.
    - Registrar las acciones preventivas y correctivas.
    - Evaluación periódica de todos los incidentes de seguridad de la información.
- El equipo de infraestructura y soporte técnico deberá anotar en la bitácora los acontecimientos sucedidos.

5.-Errores de usuarios

ACTIVIDADES ANTES

Medidas Técnicas

- Definir políticas donde los usuarios tengan claro cuáles son sus obligaciones y responsabilidades en la institución.

- Control de acceso basado en roles.
- Establecer vigilancia de seguridad física para monitorear el movimiento del personal dentro y alrededor de las instalaciones.
- Uso de herramienta o servicio para la administración de contraseñas.
- Monitoreo constante de archivos de configuración.
- Asegurarse que todo el personal esté capacitado cuando haya actualizaciones de equipos y software.
- La formación de todo el personal de TI debe realizarse una vez al año con el fin de garantizar resultados satisfactorios ante un desastre, mediante:
    - Formación de introducción, que facilite conocimientos básicos para todo el personal que se integre al departamento de TI.
    - Formación de nivel avanzado, que bride funciones concretas para el personal específico.
    - Formación continua, para garantizar el desempeño en las funciones.
    - Formación para evaluar y mantener la capacidad del personal ante la presencia de eventos imprevistos.

  Categorización de la seguridad de personal:
    - Proveedores de servicios.
    - Empleados de la institución.
    - Contratistas.
    - Visitantes.
- El director de TI debe asignar funciones y roles de seguridad que abarque:
    - Nombramiento del personal para la seguridad física.
    - Nombramiento de diputados para funciones y roles críticos.
    - Capacitación para todo el personal antes de designar funciones y roles de seguridad.
    - Asistencia a cursos periódicos de actualización, para verificar la capacidad en el desempeño de sus funciones.
    - Evaluar al personal para asegurar su conocimiento.
- El analista de seguridad de la información debe respaldar toda la información en los principales activos del Data Center alterno que posee la institución, mediante:

- Creación de imágenes de los sistemas operativos.
- Creación de puntos de restauración.
- Copia de seguridad de archivos, base de datos, aplicaciones y demás información relevante de la institución en equipos de respaldo.

ACTIVIDADES DURANTE

Medidas Técnicas

Error al no cambiar la contraseña

- El analista de seguridad informática debe administración de contraseñas mediante:
  - Generación de contraseñas fuertes, difíciles de descifrar, las cuales tengan como mínimo 8 caracteres, entre estos números, letras (mayúsculas y minúsculas) y caracteres especiales.
  - Deben estar almacenada en un sitio seguro.
  - Control de acceso basado en roles.

Error de confianza a terceras personas

- El analista de seguridad informática debe realizar procedimientos para el control de acceso lógico de manera temporal:
  - Autorización y creación de perfil "invitado"
  - Tiempo y duración de uso.
  - Verificación del registro de actividad.
- Identificación y control del personal mediante:
  - Insignias que identifique de manera única a una persona determinada.
  - No debe duplicarse fácilmente.
  - Cada persona recibe una insignia una sola vez.
  - Cada persona es responsable de su seguridad y uso.
  - La pérdida de credencial debe notificarse inmediatamente.
  - Colocar la credencial en un lugar visible.
  - Las credenciales entregadas a los visitantes deben devolverse al salir de la institución.
- Revisar el programa de FusionInventory de GLPI, (Gestión libre del parque informático) el cual permite:

- Obtener un inventario actualizado en tiempo real de todos lo equipos tanto de hardware y software que maneja la institución.

ACTIVIDADES DESPUÉS

Medidas Técnicas

- El personal de soporte técnico debe identificar los errores y seguir el procedimiento para hacer frente a estos incidentes (y debilidades), e informar al director de TI, en el cual debe abarcar:
  - Detección de todos los incidentes de seguridad de la información.
  - Registrar e informar a todas las partes involucradas acerca de los incidentes de seguridad de la información.
  - Registrar las acciones preventivas y correctivas.
  - Evaluación periódica de todos los incidentes de seguridad de la información.
  - Realizar mejoras en la seguridad de la información
- Administrar al personal involucrado en la recuperación de la institución mediante:
  - Designación de roles, responsabilidades de todo el personal durante un desastre.
  - Todo el personal debe estar informado de sus tareas de recuperación.
  - Planes de respaldo para el personal durante un desastre.
  - Todo el personal debe estar capacitado.
  - Designación de coordinadores para supervisar a la institución durante un desastre.
  - Lista del personal de operación de la institución.
- El equipo de infraestructura y soporte técnico deberá anotar en la bitácora los acontecimientos sucedidos.

6.- Errores del administrador

ACTIVIDADES ANTES

Medidas Técnicas

- Asignar responsables para las áreas de Soporte e Infraestructura y Desarrollo de Software, para manejar de manera eficiente la información.
- La formación de todo el personal de TI debe realizarse una vez al año con el fin de garantizar resultados satisfactorios ante un desastre, mediante:
    - Formación de introducción, que facilite conocimientos básicos para todo el personal que se integre al departamento de TI.
    - Formación de nivel avanzado, que bride funciones concretas para el personal específico.
    - Formación continua, para garantizar el desempeño en las funciones.
    - Formación para evaluar y mantener la capacidad del personal ante la presencia de eventos imprevistos.

  Categorización de la seguridad de personal:
    - Proveedores de servicios.
    - Empleados de la institución.
    - Contratistas.
    - Visitantes.
- Funciones y roles de seguridad que abarque:
    - Designación del personal para la seguridad física.
    - Designación de diputados para funciones y roles críticos.
    - Capacitación para todo el personal antes de designar funciones y roles de seguridad.
    - Asistencia a cursos periódicos de actualización, para verificar la capacidad en el desempeño de sus funciones.
    - Evaluar al personal para asegurar su conocimiento.
- Asignar políticas de seguridad para el departamento de TI.

ACTIVIDADES DURANTE

Medidas Técnicas

En caso de modificaciones a la base de datos

- Revisar los archivos logs.
- Revisar el programa de FusionInventory de GLPI, (Gestión libre del parque informático) el cual permite:
- Revisar la bitácora.

En caso de falta de conocimiento

- Identificar el equipo tuvo daños.
- Informar al personal de soporte técnico y brindar apoyo por parte del personal del departamento de TI.

ACTIVIDADES DESPUÉS

Medidas Técnicas

En caso de modificaciones a la base de datos

- Restaurar la última copia de seguridad de la base de datos.

En caso de falta de conocimiento

- Políticas y procedimientos con relación de la contratación del personal que debe incluir:
    - Calificaciones y experiencia del personal.
    - Políticas sobre ética, comportamiento, acoso sexual o racial.
    - Seguimiento del rendimiento.
    - Remplazo de personal.
- Administrar al personal involucrado en la recuperación de la institución mediante:
    - Designación de roles, responsabilidades de todo el personal durante un desastre.
    - Todo el personal debe estar informado de sus tareas de recuperación.
    - Planes de respaldo para el personal durante un desastre.
    - Todo el personal debe estar capacitado.
    - Designación de coordinadores para supervisar a la institución durante un desastre.

- Lista del personal de operación de la institución.

- El equipo de infraestructura y soporte técnico deberá anotar en la bitácora los acontecimientos sucedidos.

7.- Difusión de software dañino

ACTIVIDADES ANTES

Medidas Técnicas

- Cada equipo del departamento de TI debe tener software actualizados, para evitar ataques de software dañinos.
- Utilizar un software antivirus y mantenerlo actualizado para proteger a los equipos frente a software dañinos y evitar su distribución.
- Acceder solo a sitios seguros para realizar descargar de software o programas.
- Realizar copias de seguridad diarias, de base de datos y sistemas desarrollados internamente con el objetivo de salvaguardar la información manejada por la institución.
- Analizar dispositivos de almacenamiento como USB mediante el software antivirus antes de su uso.
- El analista de seguridad informática debe verificar que el firewall se encuentre activo para proteger los equipos de accesos no deseados.
- Restricciones de acceso físico a las instalaciones donde se albergan sistemas de TIC, para resguardar la información que se almacena en esta.
- El grupo de infraestructura y soporte debe asegurarse de mantener inventarios documentados y actualizados de los equipos informáticos y relacionados, en donde conste:
    - Lista de todos los activos.
    - Etiquetas para identificación de manera única.

      En caso de subcontratación:
    - No se puede poner el nombre de la institución como etiqueta.
    - Se informa a la institución cuando los activos están siendo reubicados.
    - Los activos se devuelven dentro del plazo determinado y acordado.

- Establecer horarios para realizar copias de seguridad regulares en medios de almacenamiento externos, los mismo que se encuentra en el Data Center alterno.
- El analista de seguridad informática debe respaldar toda la información en los principales activos del Data Center alterno que posee la institución, mediante:
    - Creación de imágenes de los sistemas operativos.
    - Creación de puntos de restauración.
    - Copia de seguridad de archivos, base de datos, aplicaciones y demás información relevante de la institución en equipos de respaldo

ACTIVIDADES DURANTE

Medidas Técnicas

- Una vez identificados los equipos que han sido infectados por un software dañino, se recomienda desconectar de la red los equipos que no ha sido infectados, ya que si se encuentran conectados la posibilidad de infectarse es mayor.
- El personal de soporte técnico de TI debe mantener el software de antivirus actualizado para realizar un análisis a los equipos para:
    - Escanear en tiempo real todos los archivos, aplicaciones y servicios.
    - Escanear los dispositivos de almacenamiento como USB o discos duros externos, pues estos pueden ser portadores de virus.
    - Analizar los tipos de virus.
- El personal no debe ingresar a enlaces o sitios no seguros, es recomendable pasar el ratón por encima del enlace y verificar si es confiable y seguro.
- Realizar reuniones con el personal encargado de TI, para comprobar si la amenaza tuvo origen interno o externo, si resulta ser interno identificar a los responsables.
- Modificar las contraseñas, con al menos 8 caracteres, en donde combinen mayúsculas y minúsculas, letras, números y un carácter especial.

ACTIVIDADES DESPUÉS

Medidas Técnicas

- Realizar informes con el siguiente formato:
  - Alcance y objetivos
  - Procedimientos mantenidos.
  - Resultados.
  - Acciones correctivas que tomar.
  - Justificación para futuras revisiones
- El personal encargado del departamento de TI debe tener la capacidad para descubrir el ataque, solucionarlo y recuperar la información que se encuentra involucrada.
- Tener un control de acceso de los usuarios con el siguiente procedimiento:
  - La información que maneja la institución no puede ser revelada a otra institución.
  - La responsabilidad del mantenimiento de control de acceso lógico es del personal encargado del departamento de TI.
- El equipo de infraestructura y soporte técnico deberá anotar en la bitácora los acontecimientos sucedidos.

8.- Vulnerabilidades de los programas (software)

ACTIVIDADES ANTES

Medidas técnicas

En cuanto a programas desarrollados internamente, los desarrolladores deberán:

- Disponer de buenas prácticas al crear líneas de código.
- Administrar el espacio de memoria del programa, para que otras personas no interfieran en su código.
- Utilizar protocolo SSL (Capa de Sockets Seguros), para mantener segura la conexión a internet entre servidores, y así proteger la información confidencial.
- El grupo de infraestructura y soporte debe mantener un inventario de los equipos incluyendo el software, mediante:
  - Lista de todos los activos.
  - Etiquetas para identificación de manera única.

ACTIVIDADES DURANTE

Medidas Técnicas

En cuanto a programas desarrollados internamente:

- El analista de redes debe realizar un escaneo de puertos para verificar cuales se encuentran abiertos en los equipos, ya que por medio de estos pueden obtener informacion.
    - Tener solo los puertos necesarios para que los usuarios puedan acceder a los servicios.
- El analista de seguridad informática debe verificar el normal funcionamiento del firewall para proteger a los equipos de intrusos:
    - Definiendo reglas.
    - Construyendo VPNs.
    - Funcionalidad del acceso remoto.
    - Mitigación de amenazas.

ACTIVIDADES DESPUÉS

Medidas Técnicas

En cuanto a programas desarrollados internamente:

- Realizar un informe detallado con el siguiente formato:
    - Alcance y objetivos.
    - Procedimientos mantenidos.
    - Resultados.
    - Acciones correctivas que tomar.
    - Justificación para futuras revisiones
- No utilizar software pirata o de fuente no confiables, es decir:
    - Manejar licencias perpetuas, utilizando el software para siempre.
    - Una vez adquirido el software se lo aloja en los servidores de la institución.
- Reportar los incidentes (y debilidades) de seguridad lógica mediante el siguiente procedimiento para hacer frente a estos, en el cual debe abarcar:
    - Detección de todos los incidentes de seguridad de la información.

- Registrar e informar a todas las partes involucradas acerca de los incidentes de seguridad de la información.
- Registrar las acciones preventivas y correctivas.
- Evaluación periódica de todos los incidentes de seguridad de la información.
- Realizar mejoras en la seguridad de la información

- El equipo de infraestructura y soporte técnico deberá anotar en la bitácora los acontecimientos sucedidos.

9.- Errores de mantenimiento/ actualización de programas (software)

ACTIVIDADES ANTES

Medidas Técnicas:

- Contra con control de acceso lógico.
- Contar con personal capacitado encargado del departamento de TI para brindar mantenimiento y actualización de programas.
- Realizar mantenimientos de software preventivo y correctivo periódicamente
- Contar con firewall y antivirus actualizado.
- Identificar y establecer zonas de seguridad, como:
  - Instalaciones restringidas para servidores, conmutadores de comunicaciones y cableados relacionados, aire acondicionado y suministros de energía.
  - Instalaciones comunes utilizadas por todo el personal como: área de recepción, sala de reuniones, cafetería y baños.
- Establecer políticas y procedimientos para las instalaciones físicas y de equipo que cubra:
  - Instalación.
  - Puesta en servicio
  - Operación.
  - Reparación.
  - Mantenimiento.
  - Actualización

- Reemplazo.

- Asegurarse que todo el personal esté capacitado cuando exista actualizaciones de:
  - Instalaciones
  - Equipos nuevos.
  - Software de instalación.
  - Cambios de hardware y software.

ACTIVIDADES DURANTE

Medidas Técnicas:

- El personal de soporte técnico de TI debe mantener el software de antivirus actualizado para realizar un análisis a los equipos para:
  - Escanear en tiempo real todos los archivos, aplicaciones y servicios.
  - Escanear los dispositivos de almacenamiento como USB o discos duros externos, pues estos pueden ser portadores de virus.
  - Analizar los tipos de virus.
- El analista de seguridad informática debe verificar el normal funcionamiento del firewall para proteger a los equipos de intrusos:
  - Definiendo reglas.
  - Construyendo VPNs.
  - Funcionalidad del acceso remoto.
  - Mitigación de amenazas.
- El software que se necesita para la recuperación se debe almacenar fuera del Data Center principal con las licencias necesarias.
- El analista de seguridad informática debe realizar parches de seguridad mediante las actualizaciones para corregir errores en lugar de instalar una nueva versión de software.

ACTIVIDADES DESPUÉS

Medidas Técnicas:

- Contra con proveedores que dispongan de repuestos apropiados para la reparación, mantenimiento y remplazo de equipos informáticos, para minimizar la interrupción de las actividades de la institución.
- El equipo de soporte técnico debe mantener el firmware y software actualizados de los equipos e impedir el acceso a su configuración al personal no autorizado.
- Establecer políticas y procedimientos para las instalaciones físicas y de equipo que cubra:
    - Instalación.
    - Puesta en servicio
    - Operación.
    - Reparación.
    - Mantenimiento.
    - Actualización
    - Reemplazo.
- Asegurarse que todo el personal esté capacitado cuando exista actualizaciones de:
    - Instalaciones
    - Equipos nuevos.
    - Software de instalación.
    - Cambios de hardware y software.
- El equipo de desarrollo de software deberá anotar en la bitácora los acontecimientos sucedidos.

10.- Abuso de privilegio de acceso

ACTIVIDADES ANTES

Medidas Humanas

- Establecer procedimientos ante la salida y entrada del personal mediante carnes.

- Solo el personal autorizado del departamento de TI tiene acceso a los sitios restringidos, para resguardar equipo e informacion de ese sitio.
- Establecer acuerdos de confidencialidad con el personal.
- Tener conocimiento sobre las buenas prácticas de seguridad de la información.

Medidas Técnicas

- Mantener un inventario de los equipos informáticos de alta disponibilidad en donde conste:
    - Lista de todos los activos.
    - Etiquetas para identificación de manera única.

      En caso de subcontratación:
    - No se puede poner el nombre de la institución como etiqueta.
    - Se informa a la institución cuando los activos están siendo reubicados.
    - Los activos se devuelven dentro del plazo determinado y acordado.
- Contra con controles de acceso a instalaciones físicas.
- Identificar y segregar las instalaciones de recuperación, en función de sus necesidades:
    - Restricción del acceso físico donde se alojan los principales servicios, su ubicación debe ser independiente para el adecuado control de acceso.
    - Las áreas de trabajo se deben planificar y diseñar de acuerdo con la privacidad y confidencialidad de la información relevante.

ACTIVIDADES DURANTE

Medidas Técnicas

- El personal de infraestructura y soporte técnico debe realizar un monitoreo continuo de las instalaciones físicas para asegurar su disponibilidad.
- Control de acceso físico mediante la categorización de seguridad del personal:
    - Proveedores de servicios.
    - Empleados de la institución.
    - Contratistas.
    - Visitantes.
- El personal autorizado podrá acceder remotamente a la red utilizando la herramienta VPN (‘Virtual Private Network’ Red Privada Virtual) y la

aplicación de TeamViewer, permitiendo el inicio de sesión mediante nombre de usuario y contraseña

ACTIVIDADES DESPUÉS

Medidas Humanas.

- El responsable de seguridad de la informacion deberá informar los incidentes ocurridos.

Medidas Técnicas.

El departamento de TI deberá:

- Mantener copias duplicadas de los planes, procedimientos de desastre o falla y otra información esencial, los cuales deben mantenerse fuera del sitio de fácil acceso.
- Tener un control de acceso de los usuarios con el siguiente procedimiento:
    - La información que maneja la institución no puede ser revelada a otra institución.
    - La responsabilidad del mantenimiento de control de acceso lógico es del personal encargado del departamento de TI.
- Controles de acceso físico para la protección de los sitios de instalaciones, las políticas y los procedimientos deben ser documentados e implementados, acorde con los riesgos evaluados y los servicios de la institución.

11.- Fuego

ACTIVIDADES ANTES

Medidas Humanas

- Realización de simulacros:
    - Una vez al año.
    - Planificarse adecuadamente para evitar la interrupción de las actividades.
    - Tomar medidas para que las situaciones se encuentren bajo control.
    - El director debe ser información antes del inicio de un simulacro.
    - Cronograma para llevar a cabo los simulacros.

- Diseñar rutas de escape con señales de salida que se iluminan durante un incendio para toda la institución.
- Ubicar extintores en sitios en donde requieran protección, como el Data Center, que el personal reciba información del uso, que se pueda alcanzar y activar fácilmente, además deben estar en lugar visible y recibir un mantenimiento adecuado.
- Los gases de represión o extinción de oxígeno pueden poner en peligro al personal.
- Revisar periódicamente las instalaciones eléctricas y el cableado.
- Designar puntos de encuentros seguros para el personal.
- Mantener limpio el espacio de trabajo, libre de papel amontonado, pues existiría propagación del fuego al presentarse un cortocircuito.

Medidas Técnicas

- Mantener una lista de activos (detalle de las versiones de hardware y software), etiquetados, ubicados y mantenidos en ambientes seguros, con buenas condiciones de operación**.**
- Disponer de sistemas antiincendios en sitios restringidos como Data Center, lugar donde se encuentra información relevante para la institución y proporcionar alertas a todo el personal de la institución.
- No tener obstáculos en las rutas de escape para una pronta evacuación de todo el personal que se encuentra comprometido.
- Inspeccionar el aire acondicionado del Data Center para verificar la temperatura y humedad.
- La infraestructura del sitio Data Center debe tener resistencia al fuego.
- Contar con fuentes de alimentación que cumpla los estándares mínimos de confiabilidad, seguridad, redundancia y calidad.
- Contar con un seguro contra incendios.
- Respaldar toda la información en los principales activos del Data Center alterno que posee la institución, mediante:
    - Creación de imágenes de los sistemas operativos.
    - Creación de puntos de restauración.

- Copia de seguridad de archivos, base de datos, aplicaciones y demás información relevante de la institución en equipos de respaldo.

ACTIVIDADES DURANTE

Medidas Humanas

- Garantizar la salud y seguridad del personal mediante:
  - Inspecciones periódicas de seguridad contra incendios.
  - Reducción de la carga de fuego.
  - Rutas de escape desbloqueadas.
  - Iluminación de emergencia.
- Mantener la calma entre todo el personal involucrado.
- No utilizar el ascensor, para movilizarse debe utilizar las vías de evacuación colando las manos sobre la cabeza, de manera ordenada y sin empujones dirigirse a los puntos de encuentros seguros.
- Evacuar a todo el personal que puede ser afectado y dirigirse al punto de encuentro seguro más cercano.
- El personal encargado deber pelear contra el fuego mediante el uso de extintores.
- Si el hecho ocurre en la noche, comunicar inmediatamente al personal encargado.

Medidas Técnicas

- Los sistemas de alarma y detección de humo deben proporcionen alertas tempranas de ocurrencia al personal, donde incluya:
  - Dispositivos de detección conectados las 24 horas.
  - Dispositivos manipulados y administrados localmente.

  Todas las alarmas deben tener vínculos con la policía nacional y los bomberos.
- Asegurarse de contar con fuentes de alimentación alternas en caso de que falle las fuentes normales:
  - Disponer del número necesario de generadores de energía.
  - Los generadores deben contar con mínimos estándares de seguridad, confiabilidad y calidad.

- Los generadores deben ubicarse, por lo general debajo del suelo.
- Disponer del número necesario de generadores de UPS (Fuentes de alimentación ininterrumpida).
- Los UPS deben estar ubicados a una distancia segura de los equipos informáticos de alta disponibilidad.

Además, de garantizar que los cambios de fuentes de energía sean seguros cuando se reanuden.

- Asegurarse que las rutas de escape incluyan:
  - Señales de salida bien marcados e iluminadas.
  - No deben estar obstruidas con objetos.

  Además, todo el personal debe estar informado sobre las rutas de escape en caso de un desastre.
- Todos los materiales de combustible, suministros, repuestos, equipos nuevos deben almacenar en un sitio alejado del Data Center principal.
- Cada personal debe desconectar los equipos de las fuentes de alimentación eléctrica.
- Contar con sistemas de megafonía para informar a todo el personal.
- Trasladar los equipos informáticos de alta disponibilidad a un sitio seguro.

ACTIVIDADES DESPUÉS

Medidas Técnicas

- El analista de seguridad informática debe restaurar las copias de seguridad que realizó previamente.
- Realizar un plan de evacuación por escrito**.**
- Elaborar manuales de alarma de incendios, y capacitar a todo el personal para una pronta acción ante incendios**.**
- Se necesitan rutas alternativas de acceso a los sitios de recuperación.
- Realización de simulacros:
  - Una vez al año.
  - Planificarse adecuadamente para evitar la interrupción de las actividades.
  - Tomar medidas para que las situaciones se encuentren bajo control.

    - El director debe ser información antes del inicio de un simulacro.
    - Cronograma para llevar a cabo los simulacros.
- Reportar los incidentes (y debilidades) mediante el siguiente procedimiento para hacer frente a estos, en el cual debe abarcar:
    - Detección de todos los incidentes de seguridad de la información.
    - Registrar e informar a todas las partes involucradas acerca de los incidentes de seguridad de la información.
    - Registrar las acciones preventivas y correctivas.
    - Evaluación periódica de todos los incidentes de seguridad de la información.
    - Realizar mejoras en la seguridad de la información
- Contactar al proveedor correspondiente para hacer uso del seguro antiincendios.

12.- Daños de agua

ACTIVIDADES ANTES

Medidas Técnicas

- Contar con sensores para detectar presencia de agua en el Data Center.
- Verificar las conexiones de agua del servicio higiénico ubicado al lado del Data Center.
- Monitorear los niveles de humedad para evitar posibles inundaciones en el Data Center.
- Contar con un sistema de sellado en tuberías para impedir fugas de agua o rompimientos en las conexiones.
- Tener precaución con los desagües ubicados en el piso, donde también se encuentran conexiones eléctricas.
- Tener precaución en los meses que en donde se presenta abundantes lluvias en el cantón.
- Contar con un seguro contra inundaciones.
- Respaldar toda la información en los principales activos del Data Center alterno que posee la institución, mediante:
    - Creación de imágenes de los sistemas operativos.

- Creación de puntos de restauración.
- Copia de seguridad de archivos, base de datos, aplicaciones y demás información relevante de la institución en equipos de respaldo.

ACTIVIDADES DURANTE

Medidas Técnicas

- Los sistemas de alarma y detección física deben proporcionen alertas tempranas de ocurrencia al personal, todas las alarmas deben tener vínculos con la policía nacional y los bomberos.
- El personal de soporte técnico encargado del departamento de TI debe verificar los daños físicos que se han presentado en los equipos informáticos, y si necesita reemplazo de algún componente contactarse con los proveedores pertinentes tomando en cuenta los siguientes aspectos:
  - Tiempos de entrega de equipos y repuestos.
  - Garantía en caso de defectos.
  - Soporte en instalación y capacitación.
  - Detallar información para cada componente:
    - Descripción (nombre, serie, fecha de adquisición).
    - Fabricantes.
    - Proveedores.
    - Disponibilidad.
    - Tiempo de entrega e instalación.

ACTIVIDADES DESPUÉS

Medidas Técnicas

- Sistemas de detección y alarma para inundaciones, mediante:
  - Dispositivos de detección conectados las 24 horas.
  - Dispositivos manipulados y administrados localmente
- Verificar que el nivel de humedad sea el adecuado para evitar filtración de agua en equipos informáticos.
- Incluir diseño de protección, como rociadores de tubería seca y detectores automáticos.

- Reportar los incidentes (y debilidades) mediante el siguiente procedimiento para hacer frente a estos, en el cual debe abarcar:
    - Detección de todos los incidentes de seguridad de la información.
    - Registrar e informar a todas las partes involucradas acerca de los incidentes de seguridad de la información.
    - Registrar las acciones preventivas y correctivas.
    - Evaluación periódica de todos los incidentes de seguridad de la información.
    - Realizar mejoras en la seguridad de la información
- Contactar al proveedor correspondiente para hacer uso del seguro antiincendios.

13.- Fenómeno sísmico

ACTIVIDADES ANTES

Medidas Humanas

- Realizar periódicamente simulacros incluyendo a todo el personal de la institución.
    - Una vez al año.
    - Planificarse adecuadamente para evitar la interrupción de las actividades.
    - Tomar medidas para que las situaciones se encuentren bajo control.
    - El director debe ser información antes del inicio de un simulacro.
    - Cronograma para llevar a cabo los simulacros.
- Disponer de vías de evacuación libres de obstáculos y en buenas condiciones.
- Colocar señalética, la misma debe ser clara, coherente, de buen tamaño para guiar al personal.
- Tener al alcance los números telefónicos de emergencias.
- Capacitar a todo el personal para estar al tanto y reacciona de manera inmediata ante esta eventualidad.
- Designar responsables para actuar ante este fenómeno.

Medidas Técnicas

- Asegurar al suelo de modo firme los racks de los servidores, ante movimientos y se mantengan en su posición.
- La infraestructura del edificio donde se encuentra el Data Center debe contar con estructuras antisísmicas.
- Establecer procedimientos para protección de todo el cableado.
- Realizar un inventario de los activos más importante de la institución, donde conste:
    - Lista de todos los activos.
    - Etiquetas para identificación de manera única.

      En caso de subcontratación:
    - No se puede poner el nombre de la institución como etiqueta.
    - Se informa a la institución cuando los activos están siendo reubicados.
    - Los activos se devuelven dentro del plazo determinado y acordado.
- Respaldar toda la información en los principales activos del Data Center alterno que posee la institución, mediante:
    - Creación de imágenes de los sistemas operativos.
    - Creación de puntos de restauración.
    - Copia de seguridad de archivos, base de datos, aplicaciones y demás información relevante de la institución en equipos de respaldo.
- Tener una lista de todos los proveedores y verificar su capacidad.

ACTIVIDADES DURANTE

Medidas Humanas

- El personal debe mantener la calma y transmitir al resto.
- No utilizar el ascensor, para movilizarse debe utilizar las vías de evacuación colando las manos sobre la cabeza, de manera ordenada y sin empujones dirigirse a los puntos de encuentros seguros.

Medidas Técnicas

- Si la situación lo permite el personal del departamento de TI debe apagar los equipos de alta disponibilidad para la institución como son los servidores y desconectar del tomacorriente, si su vida no corre peligro.

- El personal encargado debe dirigir primero los equipos de alta disponibilidad a un sitio seguro.
- Si se produce el corte de suministro eléctrico, contar con generadores a base de Diesel.

ACTIVIDADES DESPUÉS

Medidas Humanas

- Cuando el personal del Centro de Operaciones de Emergencia (COE) haya finiquitado la emergencia, el personal podrá regresar a sus actividades si las circunstancias lo ameritan.

Medidas Técnicas

- Tener cuidado con las posibles réplicas, las mismas que suelen ser con menor intensidad, pero de igual manera pueden causar daño.
- El personal encargado del departamento de TI debe verificar los equipos del Data Center no hayan sufrido daños mayores, para poder levantar los servicios y dar continuidad a las actividades de la institución.
- El personal encargado del departamento de TI debe restaurar las bases de datos y sistemas, utilizando respaldos que se han realizado anteriormente.
- Seleccionar un sitio de recuperación donde no se vea expuesto a este tipo de riesgo natural.
- Reportar los incidentes (y debilidades) mediante el siguiente procedimiento para hacer frente a estos, en el cual debe abarcar:
    - Detección de todos los incidentes de seguridad de la información.
    - Registrar e informar a todas las partes involucradas acerca de los incidentes de seguridad de la información.
    - Registrar las acciones preventivas y correctivas.
    - Evaluación periódica de todos los incidentes de seguridad de la información.
    - Realizar mejoras en la seguridad de la información
- Realización de simulacros:
    - Una vez al año.

- Planificarse adecuadamente para evitar la interrupción de las actividades.
- Tomar medidas para que las situaciones se encuentren bajo control.
- El director debe ser información antes del inicio de un simulacro.
- Cronograma para llevar a cabo los simulacros.

14.- Contaminación mecánica

ACTIVIDADES ANTES

Medidas Humanas

- Contar con personal responsable para la limpieza del departamento de TI y el Data Center.
- Definir políticas para el buen uso del espacio de trabajo del personal del área informática.

Medidas Técnicas

- Contar con herramientas para la limpieza como: franelas, cepillo con cerdas suaves, aire comprimido, entre otros.
- El personal del departamento de TI debe tener limpio y ordenado el lugar de trabajo.
- En el caso de vibraciones debido a trabajos en el piso dentro del área informática, ubicar los equipos en un lugar seguro.
- Contar con áreas específicas para mantenimiento y reparación de equipos informáticos.
- El proveedor correspondiente debe verificar y proporcionar mantenimiento al aire acondicionado del Data Center.
- Contar con procedimientos para la protección de todo el cableado:
    - Los cables de telecomunicaciones y de alimentación deben estar separados para evitar interferencias.
    - Los cables que se encuentran expuestos al público deben estar protegidos con material adecuado para evitar daños físicos.
    - Los cables se seleccionan en cuanto a la función de los requisitos de transmisión y del entorno externo.

- Todo el cableado, bandejas y conductos se comprueban periódicamente para identificar daños o riesgos potenciales.

ACTIVIDADES DURANTE

Medidas Humanas

- Cumplir con el comportamiento del personal:
  - Prohibición de fumar.
  - Prohibición de alimentos y bebidas.
  - Condiciones para el uso de dispositivos que generen radiofrecuencia.
  - Condiciones para el uso de dispositivos de almacenamiento.

Medidas Técnicas

El personal de soporte técnico debe:

- Realizar mantenimientos periódicos de los equipos informáticos.
- Limpiar los componentes (Disco Duro) de los equipos informáticos con el material adecuado para evitar daños mayores.
- Monitorear los valores de temperatura (20ºC y 25ºC) y humedad en un rango del 40-55% hasta 17ºC.
- La limpieza para remover el polvo se debe realizar desde la parte superior a la inferior, incluyendo al cableado, racks y suelo, mediante aspiración eléctrica.

ACTIVIDADES DESPUÉS

Medidas Humanas

- Evitar que la limpieza se realice por personas sin experiencia ya que puede causar averías en los equipos informáticos.

Medidas Técnicas

- Tener limpio e impecable la instalación del Data Center evitará el desgaste y reemplazo de los equipos.
- Planear limpiezas periódicas por el personal capacitado para determinar si necesita un mayor control en equipos informáticos e instalaciones y brindar mayor vida útil.

15.- Corte de suministro eléctrico

ACTIVIDADES ANTES

Medidas Técnicas

- El ambiente de las instalaciones debe ser estable para el normal funcionamiento de los equipos informáticos.
- Contar con UPS para el Data Center y lugares que así lo requieran para evitar la interrupción del funcionamiento de servidores y equipos relacionados por falta de energía.
- Contar con equipos de redundancia para continuar las actividades con normalidad.
- El proveedor eléctrico debe verificar que las conexiones eléctricas se encuentren en óptimas condiciones en las instalaciones en donde se almacena equipos informáticos de alta disponibilidad para la institución.
- Disponer de planes para todo el cableado e identificar puntos de riesgo, mediante:
    - Los cables de telecomunicaciones y de alimentación deben estar separados para evitar interferencias.
    - Los cables que se encuentran expuestos al público deben estar protegidos con material adecuado para evitar daños físicos.
    - Los cables se escogen en cuanto a la función de los requisitos de transmisión y del entorno externo.
    - Todo el cableado, bandejas y conductos se comprueban periódicamente para identificar daños o riesgos potenciales.
- Respaldar toda la información en los principales activos del Data Center alterno que posee la institución, mediante:
    - Creación de imágenes de los sistemas operativos.
    - Creación de puntos de restauración.
    - Copia de seguridad de archivos, base de datos, aplicaciones y demás información relevante de la institución en equipos de respaldo.

ACTIVIDADES DURANTE

Medidas Técnicas

- Guardar toda la información que se está manejando en el momento del corte de suministro eléctrico, luego se procederá a apagar los equipos como servidores, equipos de red, etc., mientras retorna la energía eléctrica o se ha regulado los daños.
- Seguir el procedimiento adecuado de apagado para cada uno de los servidores mediante el emulador de terminal Putty, dando prioridad a los equipos de alta disponibilidad.
- Asegurarse de contar con fuentes de alimentación alternas en caso de que falle las fuentes normales:
    - Disponer del número necesario de generadores de energía.
    - Los generadores deben contar con mínimos estándares de seguridad, confiabilidad y calidad.
    - Los generadores deben ubicarse, por lo general debajo del suelo.
    - Disponer del número necesario de generadores de UPS (Fuentes de alimentación ininterrumpida).

Los UPS deben estar ubicados a una distancia segura de los equipos informáticos de alta disponibilidad.

- Verificar que los equipos que mantienen redundancia se encuentren en buenas condiciones para brindar disponibilidad de los servicios con normalidad.
- El personal de soporte técnico del departamento de TI debe verificar los daños físicos que se han presentado en los equipos informáticos, y si necesita reemplazo de algún componente contactarse con los proveedores pertinentes tomando en cuenta los siguientes aspectos:
    - Tiempos de entrega de equipos y repuestos.
    - Garantía en caso de defectos.
    - Soporte en instalación y capacitación.
    - Detalle de la información para cada componente:
        - Descripción (nombre, serie, fecha de adquisición).
        - Fabricantes.
        - Proveedores.

- Disponibilidad.
- Tiempo de entrega e instalación

ACTIVIDADES DESPUÉS

Medidas Técnicas

- Realizar reuniones con el personal del departamento de TI para notificar los daños en los equipos, y proceder al reemplazo o recuperación de la información de estos, emitiendo informes con el siguiente formato:
  - Alcance y objetivos.
  - Procedimientos.
  - Resultados.
  - Acciones correctivas que tomar.
  - Justificación para futuras revisiones.
- El analista de redes debe realizar un análisis de los puntos de conexión, revisarlos y repararlos si es el caso.
- Todo el personal del departamento de TI debe revisar el área afectada y posteriormente conectar todos los equipos del Data Center.
- El personal de soporte técnico y desarrollo de software del departamento de TI debe reanudar todos los servicios para uso de la ciudadanía.
- El equipo de infraestructura y soporte técnico deberá anotar en la bitácora los acontecimientos sucedidos.

16.- Errores de mantenimiento/actualización de equipos (hardware)

ACTIVIDADES ANTES

Medidas Técnicas

- Contar con el personal o proveedores capacitados para brindar mantenimiento a los equipos.
- Administrar al personal involucrado de la institución mediante:
  - Designación de roles, responsabilidades de todo el personal durante un desastre.
  - Todo el personal debe estar informado de sus tareas de recuperación.
  - Planes de respaldo para el personal durante un desastre.

- Capacitación de todo el personal.
- Designación de coordinadores para supervisar a la institución durante un desastre.
- Lista del personal de la institución.

- El mantenimiento debe ser preventivo y exhaustivo para todo el Data Center.
- Contar con instalaciones, equipos y repuestos especializados para brinda un correcto mantenimiento a los equipos para minimizar interrupciones y continuar con las actividades.
- Contar con memoria RAM disponible y suficiente para que todos los procesos trabajen de manera correcta.
- Respaldar toda la información en los principales activos del Data Center alterno que posee la institución, mediante:
  - Creación de imágenes de los sistemas operativos.
  - Creación de puntos de restauración.
  - Copia de seguridad de archivos, base de datos, aplicaciones y demás información relevante de la institución en equipos de respaldo.

En el caso del Disco Duro:

- Revisar que el espacio del disco duro no esté al límite de su capacidad.
- Eliminar archivos innecesarios o temporales ya que estos provocan lentitud al momento de procesar información.
- Contar con sistemas RAID.

ACTIVIDADES DURANTE

Medidas Técnicas

El personal de soporte técnico del departamento de TI deberá:

- Realizar todos los intentos necesarios para reparar el equipo antes de llevarlo al proveedor el mismo que incluye:
  - Reparación y reemplazo de repuestos del equipo.
  - Identificación de equipos no cubiertos por el seguro.
  - Condiciones para retirar los equipos de alquiler.
- Tener a la mano los repuestos y accesorios adecuados para el mantenimiento de los equipos informáticos.

- Verificar que el disco duro se encuentre sujetado y libre de polvo y suciedad.
- Ubicar el disco duro con daños, analizar y verificar si funciona como de costumbre, si no es el caso, reemplazarlo, formatearlo y particionarlo.
- Informar del daño de manera inmediata al personal encargado.

ACTIVIDADES DESPUÉS

Medidas Técnicas

El personal del departamento de TI debe:

- Tener un control de acceso físico mediante la categorización de seguridad del personal:
    - Proveedores de servicios.
    - Empleados de la institución.
    - Contratistas.
    - Visitantes.
- Contar con equipos que proporcionen redundancia para mantenimiento de los equipos y prevenir impactos en los servicios.
- Establecer procedimientos para la protección de todo el cableado:
    - Los cables de telecomunicaciones y de alimentación deben estar separados para evitar interferencias.
    - Los cables que se encuentran expuestos al público deben estar protegidos con material adecuado para evitar daños físicos.
    - Los cables se seleccionan en cuanto a la función de los requisitos de transmisión y del entorno externo.
    - Todo el cableado, bandejas y conductos se comprueban periódicamente para identificar daños o riesgos potenciales.

En el caso del Disco Duro:

- Realizar el trámite pertinente por parte del analista de seguridad informática para la adquisición con la siguiente información para cada componente:
    - Descripción (nombre, serie, fecha de adquisición).
    - Fabricantes.
    - Proveedores.
    - Disponibilidad.

- Tiempo de entrega e instalación.

- Restaurar la última copia de seguridad**.**
- Verificar la integridad de los datos.
- El equipo de infraestructura y soporte técnico deberá anotar en la bitácora los acontecimientos sucedidos.

17.-Fallo de los servicios de comunicación

ACTIVIDADES ANTES

Medidas Técnicas

- Disponer de proveedores de servicio que cumpla los estándares mínimos de redundancia, confiabilidad, seguridad y calidad.
- Contar con mapas de todo el cableado de la institución para encontrar puntos de falla.
- Poseer gran ancho de banda para la comunicación entre equipos.
- Contar con analistas especializados en redes y seguridad informática.

ACTIVIDADES DURANTE

Medidas Técnicas

- El personal de soporte técnico revisará los fallos que se presenten en los equipos de redes de comunicación.
- El analista de redes debe revisar que el direccionamiento de IP este correctamente asignado mediante:
    - Tipo de clase.
    - Direcciones públicas o privadas.
- El analista de redes debe comprobar la configuración de los equipos de red.
- El profesional en el área debe establecer procedimientos para la protección del cableado y verificar si está defectuoso o dañado mediante:
    - Los cables de telecomunicaciones y de alimentación deben estar separados para evitar interferencias.
    - Separa el cable de fibra de otros cables.
- Si excede el tiempo de interrupción de acceso a internet, comunicarse con el proveedor para que resuelva el problema.

ACTIVIDADES DESPUÉS

Medidas Técnicas

- El analista de redes debe asegurarse que no haya puntos de fallas de instalaciones de red.
- El analista de redes debe probar que existir enlaces de red alternativos que permitan la conmutación.
- El profesional en el área debe asegurarse que todo el cableado de telecomunicaciones que soporta datos/ información y servicios dentro de la institución estén protegidos contra interferencias, intercepciones o daños.
- El analista de redes debe asegurarse que los equipos son idóneos de prestar enlaces de telecomunicaciones con capacidad y conectividad suficiente para que la institución se conecte sin retrasos.
- El analista de redes deberá anotar en la bitácora los acontecimientos sucedidos.

CAPÍTULO 4

CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

- Por acuerdo de confidencialidad con la institución no se detalla las características de cada uno de los activos involucrados, para salvaguardar la integridad de la información brinda a la ciudadanía.

- Por medio de la Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (MAGERIT), se identificó los activos de mayor relevancia y las amenazas que afectan a los mismos, realizando un análisis de riesgos para identificar el impacto que provocaría si llegara a materializarse.

- Se investigó la norma ISO 2476:2008 que ofrece técnicas de seguridad y directrices para la recuperación en caso de desastres de tecnología de la información y las comunicaciones.

- Se identificó y analizó los riesgos muy altos y altos para cada tipo de activo, siendo estos de mayor prioridad, ya que, si ocurre, tienen un algo grado de impacto que puede afectar las actividades de la institución.

- Se concretó actividades antes, durante y después mediante medidas humanas y técnicas dependiendo el tipo de riesgo.

- Mediante el diseño del plan de contingencia informático basado en la norma ISO 24762:2008, permite técnicas de seguridad antes desastres de origen humano o natural.

- Se asignó roles y responsabilidades al personal de departamento de TI, para una mejor organización al momento de algún tipo de falla que pueda interrumpir los principales servicios que brinda la institución a la ciudadanía.

4.2 Recomendaciones

- Realizar reuniones para capacitar a todo el personal del departamento de TI sobre la seguridad de la información para tener mejores prácticas al dar uso a los activos informáticos.

- El personal del departamento de TI y la autoridad pertinente debe analizar el presente plan de contingencia informático para su rápida implementación.

- Identificar un sitio de recuperación adecuado, lejos de los riesgos identificados para salvaguardar los equipos y la información.

- Mantener el plan de contingencia informático, al menos una vez al año, para identificar de manera oportuna los nuevos riesgos que se pueden afectar a la institución.

Bibliografía

[1] D. L. Chamba Jose, «ESPOL, Repositorio,» 17 Noviembre 2017. [En línea]. Available: https://www.dspace.espol.edu.ec/retrieve/101831/D-106264.pdf. [Último acceso: 6 Enero 2021].

[2] A. H. F. Alvarez, «Repositorio PUCE,» Diciembre 2014. [En línea]. Available: http://repositorio.puce.edu.ec/bitstream/handle/22000/7863/TesisAndresHernandez.pdf?sequence=1&isAllowed=y. [Último acceso: 6 Enero 2021].

[3] R. D. Lara Santán, «Repositorio Institucional de la Universidad de las Fuerzas Armadas ESPE,» 2010. [En línea]. Available: https://repositorio.espe.edu.ec/handle/21000/312. [Último acceso: Abril 2021].

[4] M. S. C. Renán, «Repositorio Institucional Uniandes,» 2018. [En línea]. Available: http://dspace.uniandes.edu.ec/handle/123456789/9060. [Último acceso: Abril 2021].

[5] «Inter-American Development Bank,» 2020. [En línea]. Available: https://publications.iadb.org/publications/spanish/document/Reporte-Ciberseguridad-2020-riesgos-avances-y-el-camino-a-seguir-en-America-Latina-y-el-Caribe.pdf. [Último acceso: Abril 2021].

[6] I. F. d. Comunicaciones, «ift,» Agosto 2018. [En línea]. Available: http://www.ift.org.mx/sites/default/files/conocenos/pleno/otrosdocumentos/javier-juarez-mojica/vf-ticsensituacionesdeemergencia300718.pdf. [Último acceso: 4 Enero 2021].

[7] J. Estacio, «Los riesgos tecnológicos en el DMQ: la paradoja del desarrollo urbano y el síndrome de,» [En línea]. Available: https://www.flacsoandes.edu.ec/web/imagesFTP/1218664438.Ponencia_final_de_Jairo_Estacio.pdf. [Último acceso: 4 Enero 2021].

[8] G. M. AMBATO, «GAD MUNICIPALIDAD AMBATO,» 2020. [En línea]. Available: https://ambato.gob.ec/2020/11/08/vision-mision/. [Último acceso: 4 Enero 2021].

[9] C. H. Tarazona, «Amenazas informáticas y Seguridad de la Información,» 2018. [En línea]. Available: https://revistas.uexternado.edu.co/index.php/derpen/article/download/965/915/. [Último acceso: abril 2021].

[10] K. A. M. Luis D. Narváez, «Repositorio Digital Universidad Tecnica del Norte,» [En línea]. Available: http://repositorio.utn.edu.ec/bitstream/123456789/4514/2/04%20RED%20062%20informe%20tecnico.pdf. [Último acceso: Abril 2021].

[11] «Organización institucional para el aseguramiento de la calidad e inocuidad de los alimentos: el caso de la Región Andina,» AECI, 1999, p. 99.

[12] P. A. Lopez, de Seguridad Informática, EDITEX, 2010, p. 241.

[13] J. V. Márquez, «Dialnet,» 2010. [En línea]. Available: http://www.ejournal.unam.mx/ibi/vol24-50/IBI002405008.pdf. [Último acceso: 2021].

[14] S. Castro, B. Guzmán y D. Casado, «redalyc,» 2007. [En línea]. Available: https://www.redalyc.org/pdf/761/76102311.pdf. [Último acceso: 13 Enero 2021].

[15] «ISO27000.es,» 2005. [En línea]. Available: https://www.iso27000.es/glosario.html. [Último acceso: Mayo 2021].

[16] P. A. Lopez, Seguridad Informática, Editex.

[17] G. B. Urbina, Introduccion a la Seguridad Informatica, Mexico: Patria, 2016.

[18] L. Huertas, «Universidad Técnica de Ambato,» 2005. [En línea]. Available: https://elibro.net/es/ereader/uta/96010?page=8.. [Último acceso: 2021].

[19] M. d. A. E. y. T. Digital, «Portal Administracion Electrónica,» [En línea]. Available: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html. [Último acceso: 2021].

[20] «ISO 24762:2008,» [En línea]. Available: https://www.iso.org/standard/41532.html.

[21] U. E. d. Milagro, «Normas de control interno de la Contraloría General del Estado,» [En línea]. Available: https://www.unemi.edu.ec/wp-content/uploads/2019/11/NORMAS-DE-CONTROL-INTERNO-DE-LA-CONTRALORIA.pdf.

[22] «MAGERIT- Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información,» [En línea]. Available: http://administracionelectronica.gob.es/.

[23] J. C. A. M. Miguel Angel Amutio Gómez, «Libro 1 de MAGERIT,» de Metodologia de Análisis y Gestión de Riesgos de los Sistemas de Información, Madrid, Ministerio de Hacienda y Administraciones Públicas, 2012, p. 127.

[24] J. C. J. M. Miguel Angel Amutio Gómez, «MAGERIT LIBRO II,» Octubre 2012. [En línea]. Available: http://administracionelectronica.gob.es.

[25] J. C. A. M. Miguel Angel Amutio Gómez, «MAGERIT- Libro III,» [En línea]. Available: http://administracionelectronica.gob.es/.

[26] G. M. d. Ambato, «GAD Municipalidad de Ambato,» [En línea]. Available: https://ambato.gob.ec/vision-mision/.

[27] G. M. d. Ambato, «Plan de Desarrollo y Ordenamiento Territorial,» [En línea]. Available: https://ambato.gob.ec/transparencia-2021/.

[28] G. M. d. Ambato, «Dirección de Tecnologías de la Informacion,» [En línea]. Available: https://ambato.gob.ec/direccion-de-tecnologias-de-la-informacion/.

[29] «ISO/IEC 24762:2008,» [En línea]. Available: https://www.qal-iran.ir/WebsiteImages/iso/20.PDF. [Último acceso: 2021].

[30] R. R. D. R. R. P. Gema Escrivá Gascó, «Universidad Técnica de Ambato,» 2013. [En línea]. Available: https://elibro.net/es/ereader/uta/43260?page=15. [Último acceso: Noviembre 2021].

[31] J. F. R. Buendia, «eLibro,» 2013. [En línea]. Available: https://elibro.net/es/ereader/uta/50243?page=8. [Último acceso: 2021].

[32] G. Baca Urbina, «Universiadad Tecnica de Ambato,» 2016. [En línea]. Available: https://elibro.net/es/ereader/uta/40458?page=21. [Último acceso: 2021].

[33] G. B. Urbina, «Introduccion a la Seguridad Informatica,» Universidad Técnica de Ambato, 2016. [En línea]. Available: https://elibro.net/es/ereader/uta/40458. [Último acceso: 2021].

ANEXOS

LISTA DE PROVEEDORES

LISTA DE PROVEEDORES			
N.º	**NOMBRE**	**TIPO**	**CONTACTO**
1	FRECANVAL	Telecomunicaciones Fibra óptica	0994933222
2	AKROS CIA LTDA DECISIONES PARA EL FUTURO	Tecnología de la Información	(02)397-6800
3	SECURITY DATA	Soluciones tecnológicas	(02)392-2169
4	ALLIANCE TECH DEL ECUADOR CIA. LTDA	Alquiler de equipos Adquisición	(02)225-3211
5	ESRI ECUADOR S. A	Servicio de Ingeniería	(02)450-0230
6	DOS S. A	Tecnología	0996312061
7	INSTAL RED	Telecomunicaciones	0933227193
8	EDISON TERAN	Redes	0998522669
9	CLICKNET SA	Servicio de Internet	0998522669
10	CNT	Servicio de Internet	(03)241-1100
11	TELCONET	Telecomunicaciones	0987592220

IDENTIFICACIÓN Y VALORACIÓN DE ACTIVOS

Código:		**Nombre:**	
Descripción:			
Tipo:		Nivel:	
Valoración			
Valor	Confidencialidad [C]	Integridad [I]	Disponibilidad [D]
Valor del Activo			
Valor Heredado			
Valor Total			
Amenazas			

REGISTRO DE MANTENIMIENTO

Fecha	Autor	Tipo	Versión	Referencia de cambio

ACCESO A SITIOS RESTRINGIDOS

Cargo	Nombre	Teléfono

SOFTWARE PARA RESTAURACION

Nombre	Descripción

CONTROL DE ACCESO LÓGICO

Nombre	Usuario	Contraseña	Perfil	Acciones (escritura, lectura, actualización, eliminación)

FORMATO PARA ADQUISICION DE EQUIPO

Nombre	Serie	Fecha adquisición	Fabricante	Proveedor	Disponibilidad

REGISTRO DE INCIDENTES

REGISTRO DE INCIDENTES			
Fecha:	**Hora:**		
Identificación de activos			
Riesgos identificados			
Método o herramientas utilizadas	**Versión**		
	Tipo		
	Descripción		
Responsable			
Firma			

COPIAS DE SEGURIDAD

Código	Fecha	Frecuencia	Lugar de almacenamiento	Medio de almacenamiento	Responsable