UNIVERSIDAD ESTATAL
PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

MODALIDAD: EXÁMEN COMPLEXIVO

Componente Práctico, previo a la obtención del Título de:

INGENIERO EN TECNOLOGÍAS

DE LA INFORMACIÓN

TEMA:

"DESARROLLO DE UN PLAN DE CONTINGENCIAS INFORMÁTICO PARAEL CENTRO DE DATOS Y COMUNICACIONES DE LA EMPRESA AGUAPEN-EP MEDIANTE EL USO DE NORMAS INTERNACIONALES"

AUTOR:

GONZABAY TOMALÁ RONALD ENRIQUE

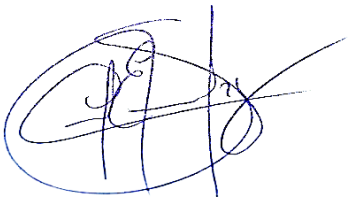
LA LIBERTAD – ECUADOR

PAO 2021-2

APROBACIÓN DEL TUTOR

En mi calidad de Tutor del trabajo de titulación denominado: "**DESARROLLO DE UN PLAN DE CONTINGENCIAS INFORMÁTICO PARA EL CENTRO DE DATOS Y COMUNICACIONES DE LA EMPRESA AGUAPEN-EP MEDIANTE EL USO DE NORMAS INTERNACIONALES**", elaborado por la estudiante **RONALD ENRIQUE GONZABAY TOMALÁ** de la carrera de Tecnologías de la Información de la Universidad Estatal Península de Santa Elena, me permito declarar que luego de haber orientado, estudiado y revisado, la apruebo en todas sus partes y autorizo al estudiante para que inicie los trámites legales correspondientes.

La libertad, febrero del 2022



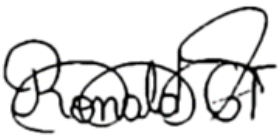
…….

Ing. Carlos Sánchez, Mgti.

Tutor

DECLARACIÓN

El contenido del presente componente práctico del examen de carácter complexivo es de mi responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de Santa Elena.



…….

Ronald Enrique Gonzabay Tomalá

AGRADECIMIENTO

Agradezco a Dios por ser mi guía y brindarme esa fortaleza para no decaer y seguir adelante para poder culminar esta etapa de mi vida profesional.

A mi maravillosa familia, por apoyarme incondicionalmente y estar siempre presente en cada momento importante de mi vida.

A mis compañeros y amigos de aula por estar siempre en las buenas y malas apoyándonos en el proceso de aprendizaje.

Agradezco a todos aquellos docentes de la Facultad de Sistemas y Telecomunicaciones por haberme impartido sus conocimientos y dedicación en cada hora de clase, en especial al ingeniero Carlos Sánchez Centenaro por haberme guiado y extenderme su mano amiga para llevar a cabo mi trabajo de titulación.

Ronald Gonzabay Tomalá.

DEDICATORIA

Éste trabajo se lo dedico a la memoria de mi hermano Carlos Gonzabay Tomalá, aunque hoy no pueda abrazarlo físicamente, lo abrazo con el alma. A mis padres Orlando Gonzabay González y Rosa Tomalá Malavé, por su amor, trabajo y sacrificio para hacer de mí una persona de principios y valores. A mi querida hermana Lourdes Gonzabay, Joselyn Muñoz y mi cuñada Laura Roca por su apoyo incondicional, y a mis queridos sobrinos Rodrigo, Ezequiel y Karla por su aprecio y cariño que con su inocencia llenan mis días de felicidad.

A cada una de las personas que me motivaron a seguir y creyeron en mí.

Ronald Gonzabay Tomalá.

TRIBUNAL DE GRADO

Ing. Washington Torres Guin, Mgti.
DIRECTOR DE LA CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN

Ing. Carlos Castillo Yagual, Mgti.
DOCENTE ESPECIALISTA

Ing. Carlos Sánchez, Mgti.
DOCENTE TUTOR

Ing. Marjorie Coronel, Mgti.
DOCENTE GUÍA UIC

RESUMEN

El presente trabajo de titulación fue desarrollado para él departamento de coordinación de tecnologías de la información de la empresa Aguapen Ep, el cual actualmente no había realizado un minucioso análisis de posibles amenazas naturales, físicas, humanas que atenten contra la seguridad de la información convirtiéndose en riesgos que podrían afectar la continuidad de sus operaciones.

Por tal razón resultó imprescindible la implementación de un plan de contingencias informático que contemple un conjunto de directrices técnicas, humanas y administrativas para minimizar y prevenir el grado de afectación de posibles riesgos que se presenten conforme a las directrices de la norma ISO 31000 RISK MANAGEMENT, identificando controles en base a normas de seguridad de la información como ISO 27000, ISO 27002, Plantillas de políticas de seguridad del Instituto SANS y el planteamiento de salvaguardas antes, durante y después de las emergencias, así como también los roles y responsabilidades por parte de los encargados de la ejecución del plan para precautelar la integridad, confidencialidad y disponibilidad de los activos de información.

ÍNDICE

ÍNDICE DE FIGURA

ÍNDICE DE TABLA

LISTA DE ANEXOS

INTRODUCCIÓN

En la actualidad los activos informáticos son el pilar fundamental de las organizaciones para obtener una correcta ejecución de las operaciones, esto se debe a que en ellos reposan los sistemas, datos e información, los cuales tienden a estar expuestos a posibles amenazas que atenten contra la seguridad de la información. En el área de coordinación de Tecnologías de la Información ubicado en la empresa AGUAPE EP, es necesario la elaboración de un plan de contingencias que admita o especifique medidas de seguridad óptimas, necesarias y apropiadas para salvaguardar los activos de información del centro de datos para reducir altos índices de riesgo [1].

Las normativas y estándares internacionales referentes a la seguridad de la información y el análisis de riesgos contribuyen en el desarrollo e implementación de un plan de contingencias efectivo que den respuesta a casos de emergencia y prevención derivados principalmente por la presencia de amenazas, e incidentes informáticos.

La finalidad del proyecto conlleva principalmente a la realización de un análisis y uso eficiente de estándares, normas o leyes internacionales de seguridad como ISO/IEC 27002, ISO 31000 y SANS Security Policy, que proporcionen una efectiva identificación de amenazas en torno a la seguridad de la información y establecer estrategias o acciones dentro de un plan de contingencias para afrontar eventualidades de emergencia.

CAPITULO I

FUNDAMENTACIÓN

1.1 ANTECEDENTES

En la provincia de Santa Elena existen un sinnúmero de Pymes y MiPymes, entre ellas se encuentra la empresa AGUAPEN-EP, creada el 14 de diciembre de 1999, la cual se encuentra ubicada en el cantón salinas, en la Av. Carlos Espinoza Larrea y Calle San José, dedicada a la prestación de servicios públicos de agua potable, alcantarillado sanitario, alcantarillado pluvial, entre otro tipo de servicios en beneficio de la comunidad. La empresa Aguapen EP cuenta con el respaldo de los Gobiernos Autónomos Descentralizados Municipales de los cantones de Santa Elena, La Libertad y Salinas, cuyos alcaldes apoyan constantemente la gestión del Gerente General, la cual, en febrero del año 2013, se constituyó como la empresa Pública Municipal Mancomunada de Agua Potable [2].

Cabe recalcar que la información es considerada parte esencial que toda empresa pública o privada debe proteger frente a escenarios de riesgo, esto implica la necesidad del desarrollo de un plan de contingencias que contribuya a mantener el funcionamiento normal de las operaciones de la empresa. Resulto necesario el hizo uso de métodos de recolección de información como: observación de forma directa (ver Anexo 1), y entrevistas dirigidas al equipo encargado del funcionamiento del departamento de TI (ver Anexo 2), obteniendo como resultado que:

El departamento de TI carece de documentación escrita, precisa y optima sobre un plan de contingencia que contenga políticas y controles que sirvan de apoyo para precautelar la continuidad de sus operaciones debido a que no se ha ejecutado un proceso para identificar riesgos que podrían causar daños sobre los diferentes activos del centro de datos y que atenten a la confidencialidad, integridad y disponibilidad de la información.

El centro de datos de la Empresa AGUAPEN-EP dispone de varios activos informáticos que proveen diferentes servicios a los usuarios como brindar acceso a los sistemas de información financiero y comercial, acceso al sistema de correo y gestión documental de la empresa, aplicaciones web, comunicaciones alámbricas e inalámbricas, entre otras

indispensables para el correcto funcionamiento de la institución, los cuales pueden estar expuestos ante diferentes tipos de amenazas ocasionando graves perjuicios sobre las estrategias e imagen de la empresa.

Según las estadísticas publicadas por ESET Security Report 2020 de los datos suministrados por organizaciones de toda Latinoamérica se pueden afirmar que un 60% de las organizaciones y empresas sufrió al menos un incidente de seguridad durante el año 2019, obteniendo grandes pérdidas por no contar con planes de contingencia para tener una pronta respuesta ante los sucesos que puedan ocurrir [3].

1.2 DESCRIPCIÓN DEL PROYECTO

El presente proyecto de titulación consiste en identificar los diferentes agentes de amenazas que generen riesgos sobre los activos de información para la generación de un plan de contingencias informáticas basado en normas internacionales debido a la carencia de políticas y procedimientos para el tratamiento de los posibles riesgos que pueden obstaculizar el cumplimiento normal de los procesos de la empresa. Teniendo presente el estudio de métodos de recolección de información realizados mediante, entrevistas y observación directa mediante las visitas efectuadas en el área de coordinación de TI para obtener resultados reales, valorizando las amenazas y poder elaborar contramedidas para evadir incidentes que podrían afectar al departamento de TI.

Durante el desarrollo del proyecto se hace uso de estándares para llevar a cabo el objetivo propuesto como: la normativa ISO 31000:2018 [4], la cual ofrece directrices y principios para llevar a cabo una adecuada y eficiente gestión del riesgo, a su vez, se consideran a elección los 14 dominios, 35 objetivos de control y 114 controles de seguridad correspondientes a la serie ISO/IEC 27002:2013 [5] y las políticas o controles que brinda el Instituto de seguridad de la información SANS [6].

El proyecto aborda las siguientes fases establecidas en la sección 2.4 metodología de desarrollo del proyecto escogida y ajustada sobre la norma ISO 31000 [4]:

FASE 1: ESTABLECER EL CONTEXTO

Esta fase se realiza obteniendo información relevante de la empresa mediante el uso de metodologías de recolección de información como el método de observación directa en el centro de datos y entrevistas dirigidas al coordinador de Tecnologías de la Información,

al Jefe de Infraestructura Tecnológica, logrando a su vez identificar los activos que soportan los procesos y servicios que brinda el departamento de TI, la infraestructura de red actual de la empresa, lo que permitirá obtener los lineamientos y directrices para definir los riesgos.

FASE 2: EVALUACIÓN DE RIESGOS

Esta fase permitirá identificar el nivel de impacto que tendría la materialización de los riesgos sobre los servicios que soportan dichos activos del centro de datos que obstaculizarían la consecución de los objetivos de la empresa en relación con su nivel de confidencialidad, integridad y disponibilidad.

Posteriormente se procede a realizar el análisis y valoración del riesgo identificando la probabilidad de ocurrencia de los riesgos, para poder priorizarlos con las mediciones de grado: alto, medio, bajo, generando la matriz de evaluación de riesgos.

FASE 3: TRATAMIENTO DE LOS RIESGOS

En esta fase se procede a generar un plan de contingencias ante desastres en el centro de datos del área de Tecnologías de la Información de la empresa AGUAPEN-EP permitiendo establecer controles mediante el uso de controles de la normativa ISO 27002 y SANS.

El proyecto se ajusta a la siguiente línea de investigación de la Facultad de sistemas y Telecomunicaciones de UPSE que establece entre otros aspectos lo siguiente:

Relacionado con temas de infraestructura y seguridad de las tecnologías de la información, a través de las redes de comunicación, sistemas informáticos y gestión de seguridad de la información que permitan generar información indispensable para la toma de decisiones [7].

1.3 OBJETIVOS

1.3.1 Objetivo General

Elaborar un plan de contingencias mediante la identificación de riesgos y el uso de dominios de control basadas en normativas internacionales para el departamento de Tecnologías de la información de la empresa Aguapen EP.

1.3.2 Objetivos específicos

- Identificar riesgos que generen daños sobre los activos de información del departamento de TI mediante la norma internacional ISO 31000.
- Elaborar un plan de contingencias dirigido al departamento de Tecnologías de la información para actuar ante situaciones de emergencia.
- Proponer controles bajo normas internacionales para minimizar el impacto del riesgo y apoyar la continuidad de las operaciones.

1.4 JUSTIFICACIÓN

Hoy en día, es un hecho que la gran mayoría de procesos y operaciones son soportados, y gestionados por los activos informáticos, lo cual, implica la existencia de factores de riesgo que podrían afectar dichos activos [8]. Mediante el desarrollo del plan de contingencias se entregará documentación como respuesta ante casos de emergencia, catalogándolo como instrumento para la gestión administrativa de las TI, y que servirá como requerimiento para futuras certificaciones a las que sea sometido el departamento de coordinación de TI.

En caso de dificultad, el departamento de TI puede minimizar muchos de los daños pueden afectar gracias al plan de contingencias permitiéndole minimizar el impacto de los riesgos. El enfoque basado en el riesgo ayuda a la organización a tomar mejores decisiones cuando debe elegir acciones para controlar las falencias en base a la seguridad de la información, beneficiando indirectamente al personal administrativo que hace uso de los servicios que brinda el centro de datos a cargo del departamento de Tecnologías de la Información.

El uso de estándares internacionales ofrece una serie de beneficios [9], como:

- Generar un eficaz manejo de la administración de los procesos de la organización, promover una gestión de riesgos proactiva, enfocada en la prevención antes que en la reacción.
- Reducir tiempos para reaccionar pronto a posibles incidentes de seguridad.

- Disminuye la ocurrencia de incidentes de impacto negativo.
- Permite crear una cultura de prevención, implicando a todo el personal que la conforman.
- Establece una base confiable para la toma de decisiones.

El proyecto está alineado entorno a los objetivos del Plan Creación de Oportunidades, haciendo énfasis en la política A. Acceso equitativo a servicios y reducción de brechas territoriales, el cual detalla lo siguiente:

A4. Fortalecer la conectividad y el acceso a las TIC como una vía para mejorar el acceso a otros servicios [10].

1.5 RESULTADOS ESPERADOS

- Mitigación de posibles amenazas sobre las que pueda estar sometido el centro de datos.
- Mayor protección e integridad de los activos de información.
- Disponibilidad de documentación para ejecutar controles y salvaguardas plan de contingencias ante emergencias.

1.6 ALCANCE

El plan de contingencias está diseñado para minimizar riesgos que afecten a los diferentes activos del centro de datos y comunicaciones de la empresa AGUAPEN-EP los cuales soportan los servicios indispensables para el desarrollo de las operaciones institucionales, evaluados mediante el análisis del riesgo, pues al no contar con un plan de contingencia podrían obtener efectos negativos que podrían obstaculizar el cumplimiento de sus objetivos.

El contenido que contempla el desarrollo del proyecto se enmarca en las siguientes fases:

Fase 1: Establecer el contexto

- En la primera fase se desarrollarán los siguientes puntos que abarcan aspectos esenciales para reconocer el área de estudio:
- Identificar la estructura organizacional.

- Identificar los procesos y servicios del departamento de TI.
- Reconocer los activos de información.
- Identificar la infraestructura de red.

Fase 2: Evaluación del riesgo

- Analizar riesgos que podrían causar afectaciones a los activos del centro de datos.
- Identificar el nivel de probabilidad e impacto del riesgo sobre los servicios que soportan dichos activos del centro de datos, en relación con su nivel de confidencialidad, integridad y disponibilidad.
- Generación de la matriz de evaluación de riesgos, para priorizar las amenazas que provocarían un riesgo alto, medio y bajo.

FASE 3: Tratamiento de los riesgos

Desarrollar el plan de contingencias ante desastres en el centro de datos del área de Tecnologías de la Información estableciendo controles en base a la normativa ISO 27002 y SANS.

Cabe recalcar que el presente proyecto no contempla la adquisición, implementación de equipos de hardware o software como servidores firewalls, proxys o zonas desmilitarizadas para controlar la seguridad lógica del centro de datos, debido a que solo aborda el desarrollo del proceso del plan de contingencia para apoyar la correcta y oportuna recuperación de los procesos de la empresa.

CAPITULO II

LA PROPUESTA

2.1. MARCO CONTEXTUAL

2.1.1. Aguapen E-P

Inició como una compañía privada que fue constituida legalmente el 14 de diciembre de 1999, con el objeto de dedicarse a la prestación de servicios públicos de alcantarillado sanitario, tratamiento de agua potable y alcantarillado pluvial en la Provincia de Santa Elena. El Gerente General junto al talento humano que conforma esta empresa, están comprometidas en brindar una atención con respeto y responsabilidad a los usuarios y la comunidad en general [2].

2.1.1.2. Visión

Lograr el reconocimiento a nivel nacional de los servicios de agua potable, alcantarillado pluvial y sanitario [11].

2.1.1.3. Misión

Dotar servicios de agua potable, alcantarillado sanitario y pluvial de calidad, cantidad y continuidad en nuestra área de cobertura dentro de la Provincia de Santa Elena [11].

2.1.1.4. Objetivos

Obtener un posicionamiento positivo de imagen institucional a través de un servicio integral y de calidad a la ciudadanía [12].

2.1.2. Base Legal

2.1.2.1 Normas de Control Interno - República del Ecuador

Las normas de control interno están dirigidas al Sector Público del Ecuador estableciendo guías generales que fueron emitidas por la contraloría general del estado [13]. Las normas que fueron consideradas para el desarrollo de planes de contingencias informáticos están manifestadas mediante:

2.1.2.2. Normativa 300. Evaluación de riesgos

Esta normativa menciona que: el nivel directivo y administrativo de una entidad pública es responsable de ejecutar procesos de administración de riesgos, que involucra estrategias, técnicas y procedimientos, mediante los cuales se identificarán, analizarán potenciales eventos que pudieran afectar el logro de sus objetivos y la ejecución de sus procesos [14].

2.1.2.3. Normativa 410-11 Plan de Contingencias

Es responsabilidad de la unidad de tecnología de información de cualquier empresa, el desarrollar e implementar un plan de contingencias que describa acciones a poner en marcha ante una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado [14].

2.2. MARCO CONCEPTUAL

2.2.1. Seguridad de la Información

La normativa ISO 27000 lo define como el hecho de preservar la confidencialidad, integridad y disponibilidad de la información de la empresa u organización [15], denominados a su vez como los tres pilares fundamentales de la seguridad de la información.

2.2.2. Confidencialidad

En todas las etapas del procesamiento de la información, ésta se debe mantener protegida u oculta contra personal externo o accesos no autorizados, procurando que se deriven en alteración o robo de información, evitando su divulgación a personas y entidades no autorizadas [16].

2.2.3. Integridad

Término que hace referencia a el hecho de tener la información intacta, exacta y completa, para que no sea objeto de manipulación, tanto en procesos como de personas que no tengan la autorización [16].

2.2.4. Disponibilidad

Es una característica relacionada con la disposición de quienes tienen acceso a la información, en el momento en que así lo requieran [16].

2.2.5. Activo

Un activo es un componente que tiene valor y que forma parte del diario operar de las organizaciones y, por tanto, que requiere protección [17].

2.2.6. Amenaza

Definida como causa potencial de un incidente que no es deseado y que puede ocasionar un daño a una organización, sistema o persona [18].

2.2.7. Vulnerabilidad

Considerada como una debilidad de un activo que puede ser explotado o aprovechado con la finalidad de causar afectaciones o daños [18].

2.2.8. Riesgo

Definida como la posibilidad de que una amenaza pueda aprovechar una vulnerabilidad para causar daño a un activo de información. Es considerado también como la probabilidad de ocurrencia de un evento y sus consecuencias [18].

2.2.9. Plan de contingencia

Es un instrumento de gestión para el buen gobierno de las Tecnologías de la Información en el dominio del soporte y el desempeño definiendo acciones y controles a implementar, recursos a utilizar y personal a emplear ante un acontecimiento que degrade los recursos informáticos [19]. Una organización debe contar con un plan de contingencias en base a un análisis de diferentes amenazas que generen riesgos y contrarrestar posibles afectaciones.

2.2.10. Políticas de Seguridad de la Información.

Una política de seguridad es un plan y un conjunto de reglas para el mantenimiento de cierto nivel de seguridad, la intención de una política de seguridad es poder informar al personal sobre pasos a cumplir por cada uno de ellos para proteger la propiedad intelectual de la empresa e información [19]. Debe estar accesible de tal forma que los usuarios estén al tanto y acojan dichas disposiciones.

2.2.11. Instituto de seguridad de la información (SANS)

Este instituto reúne profesionales en el ámbito de Sistemas, Auditoria, Redes y Seguridad con el fin de ofrecer capacitación y certificación en el ámbito de la seguridad informática brindando diferentes políticas y controles sobre seguridad. [20].

Figura 1: Instituto de Auditoria, Redes y Seguridad.

Fuente: Instituto SANS

Los recursos del instituto SANS no tiene ningún costo, el objetivo principal es conceder plantillas y herramientas necesarias concernientes con el desarrollo de políticas de seguridad de la información. Los recursos de esta organización fueron escogidos para la elaboración del plan dirigido al área de coordinación de TI de la empresa AGUAPEN EP ya que existe libre acceso para su implementación.

2.2.12. Descripción de la Norma ISO/IEC 27002

Es un estándar para la seguridad de la información, publicado por la organización internacional de normalización y la comisión electrotécnica internacional. El principal objetivo de la ISO 27002 es establecer directrices, y prácticas de gestión de seguridad de la información, incluida la selección, implementación y gestión de controles, teniendo en cuenta el entorno de riesgo de seguridad de la información de la organización [21].

Figura 2: Estructura del Estándar ISO/IEC 27002:2013.

Fuente: INCIBE. Instituto Nacional de Ciberseguridad de España

El uso de la norma ISO 27002 en el área de coordinación de TI, permitirá aplicar controles, lineamientos y directrices para el manejo de los activos físicos e integridad de los datos, en especial aportará buenas prácticas que gestionen y reduzcan los niveles de ocurrencia de incidentes que puedan afectar la continuidad de las operaciones de la empresa.

2.3. MARCO TEÓRICO

2.3.1. El riesgo tecnológico en base a ISO 27005 e ISO 31000, aportes en la continuidad del negocio.

En un artículo científico realizado por Castro A, cuyo objeto de estudio es la Gestión de Riesgos tecnológicos en base a la normativa ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios se demostró que los planes de seguridad deben enfatizar en crear conciencia en seguridad para prevenir riesgos y buscar estrategias para obtener el apoyo de la alta dirección con el fin de cumplir con los objetivos y asegurar la información crítica, adicional la gestión adecuada de los riesgos permite evitar en gran medida la ocurrencia de incidentes y con ello evitar la activación de planes de continuidad [22].

2.3.2. Gestión de Riesgos Empresariales: Marco de Revisión ISO 31000.

En una investigación ejecutada en el 2017 por Lizarzaburu Edmundo; Ampuero Gabriela; Noriega Luis; para la revista Espacios denominada Gestión de Riesgos Empresariales: Marco de Revisión ISO 31000, detallan que esta norma permite conocer los riesgos de manera eficiente y a ordenarlos para un buen análisis y gestión. Por lo tanto, cuando se

implementa dentro de la organización la gestión de riesgos debe ser capaz de lograr ciertos objetivos, como tomar conciencia de las amenazas causadas por los riesgos, ser capaz de gestionar los riesgos dentro de la organización, tener la capacidad de asignar y hacer uso efectivo de los recursos de manera eficiente como respuesta a emergencias. De la misma manera, poder lograr una correcta gestión de incidentes mejorando el rendimiento y la eficiencia operativa. [23].

2.3.3. Gestión de incidentes informáticos de seguridad ISO 27002

Con este artículo se da a conocer lo que es un incidente de seguridad, la importancia de generar políticas y normas para controlar la aparición de los mismos en una organización basada en la norma ISO 27001:2005 y apoyado en los anexos de la ISO 27002, lo cual permite a las organizaciones establecer procesos de control para la resolución de contingencias [24].

En Cuenca - Ecuador para el año 2011 en la Universidad de Cuenca se desarrolló un trabajo de pregrado titulado “Diseño de un plan de contingencias de TI para la empresa CENTRO SUR” [25]. Elaborada por Andrea Granda. Donde se utilizó la metodología Magerit que proporciona una guía para la identificación de los activos, amenazas y salvaguardas o controles de seguridad, que impacten a la continuidad del negocio, en conjunto con los controles de seguridad de la norma ISO 27001.

En Ibarra – Ecuador en el año 2015, en la Universidad Técnica del Norte se desarrolló la tesis titulada “Plan de Contingencia para la Unidad de Sistemas y Tecnología de información del G.A.D. Antonio basado en la norma ISO/IEC 27002 [26]”. Elaborado por Karina Méndez Luna. El cual analiza una metodología para desarrollar un plan de contingencia evaluando los escenarios de contingencia y así brindar soluciones que permitan garantizar la continuidad de las actividades; presentando el plan de contingencia de TI basada en su propia experiencia y guías de buenas prácticas de seguridad de TI.

En la Provincia de Santa Elena, se desarrolló un trabajo de grado para la Universidad Estatal Península de Santa Elena, en el año 2017 cuyo tema es “Evaluación de riesgos y desarrollo de un plan de recuperación ante desastres informáticos [27]”, el cual proporciona una comprensión general sobre planes de contingencia que permitan la reanudación de las operaciones de manera eficiente, teniendo como base principal la implantación de controles de seguridad en base a estándares internacionales,

indispensable para tomar conciencia en la necesidad de asegurar y garantizar la confidencialidad, disponibilidad e integridad de la información, asegurando el logro de los objetivos de la entidad.

Todos estos trabajos de grado permiten comprender metodologías, métodos, metas a cumplir, normas internacionales de buenas prácticas que se deben considerar para la elaboración de planes de contingencias, entre otros aspectos de vital importancia para el desarrollo de este proyecto.

2.4 METODOLOGÍA DEL PROYECTO

2.4.1 Metodología de investigación

Debido a que actualmente no ha sido desarrollado un plan de contingencias informático para el centro de datos del departamento de coordinación de TI de la empresa AGUAPEN EP, se utilizó la metodología de investigación de tipo exploratorio [28], las cuáles se efectúan cuando no se han realizado investigaciones previas o existe poca información acerca del objeto de estudio. Indagando información de trabajos relacionados con esta línea de desarrollo, comparando su estructura para establecer diferencias y semejanzas frente al trabajo propuesto.

Además, se hizo uso de la metodología de investigación de tipo diagnóstica [28], para conocer los procesos y situación actual de la empresa, utilizando técnicas de recolección de información como la observación directa y entrevista realizada al jefe coordinador de Tecnologías de la Información para conocer si existen medidas preventivas ante posibles riesgos informáticos.

2.4.2. Variable del proyecto

Evidenciar la cantidad de controles y salvaguardas que existen actualmente en el departamento de coordinación de TI ante diferentes situaciones de emergencia, en relación, con la cantidad de controles y salvaguardas que se establecerán con el desarrollo del proyecto.

2.4.3. Técnicas de recolección de información

La técnica de observación directa (Ver Anexo 1), consiste básicamente en observar el objeto de estudio dentro de una situación particular. Todo esto se hace sin necesidad de

intervenir o alterar el ambiente del objeto de estudio [28], la cuál fue de gran ayuda para identificar la estructura organizacional, los activos del área de tecnologías de la información y la infraestructura de red actual de la empresa AGUAPEN EP.

Se estableció un conjunto de preguntas abiertas durante la entrevista dirigida al jefe del departamento de Tecnologías de la Información (Ver Anexo 2), quien es la autoridad encargada de administrar la infraestructura de TI de la empresa y precautelar la seguridad e integridad de los datos que se manejan en torno a los sistemas informáticos en la institución [28].

El conjunto de personas a quienes beneficiara este proyecto se detalla en la siguiente tabla:

Beneficiados		**Cantidad**
Directos	Gerente de la Empresa.	1
	Coordinador de Tecnologías de la Información.	1
	Analista administrador de redes y telecomunicaciones.	1
	Analistas de desarrollo de software	2
	Administrador de Base de datos.	1
	Asistente de soporte técnico.	1
Indirectos	Encargados del área administrativa de la empresa	243
TOTAL		250

Tabla 1: Beneficiaros del Proyecto. Elaboración propia

2.4.4. Metodología de desarrollo del proyecto

La norma internacional ISO 31000:2018 [4], establece una serie de fases necesarias para realizar un eficiente proceso de gestión del riesgo, creando estrategias que permitirán abordar y minimizar las amenazas, abarcando la mejora de la toma de decisiones en torno a los riesgos que se presenten en el desarrollo de los procesos de la empresa. Las metodologías de gestión de riesgo son desarrolladas con la finalidad de identificar la falta de control y la elaboración de planes de contingencia.

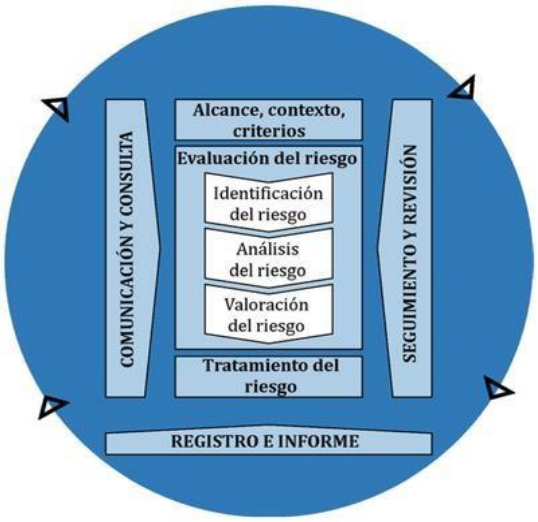


Figura 3:Proceso de Gestión de riesgo. Fuente: ISO 3100:2018 (es)

En la parte inferior se muestra la metodología para la gestión de riesgo seleccionada y ajustada a partir de ISO 31000:2018(es), utilizada en el presente proyecto:

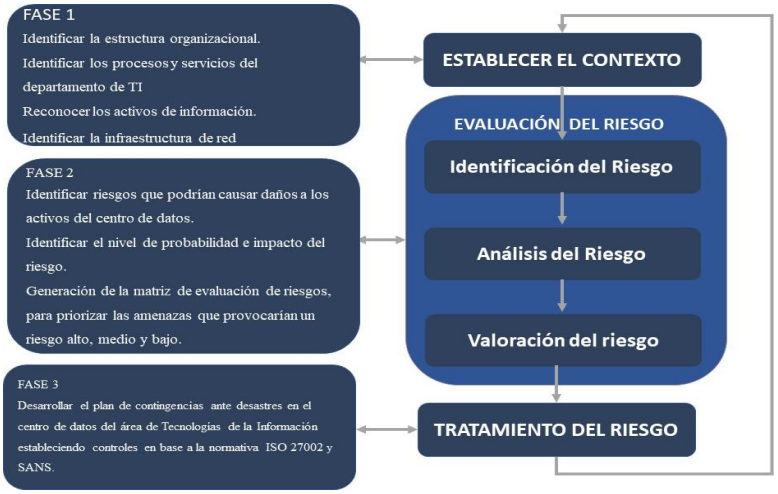


Figura 4: Metodología para el análisis de riesgos basado y ajustado a partir de ISO 31000(es). Elaboración Propia

CAPITULO III

ANÁLISIS DE RIESGOS EN EL CENTRO DE DATOS DEL DEPARTAMENTO DE COORDINACION DE TI.

3.1 FASE 1: ESTABLECER EL CONTEXTO

3.1.1 Situación actual del departamento de Coordinación de TI.

El departamento de Tecnologías de Información y Comunicación se encarga del cumplimiento de las actividades diarias técnicas y administrativas brindando los servicios informáticos al usuario institucional.

Está conformada por las siguientes áreas:

- Coordinación de TICS:

Encargado de dirigir, organizar y supervisar la ejecución de las actividades del departamento, responsable global del suministro y uso de las TIC en la empresa.

- Área de Infraestructura tecnológica, redes y seguridades:

Responsables de la administración de la infraestructura tecnológica, precautelando la disponibilidad del equipamiento, hardware, software y comunicaciones, manteniendo la colaboración con el departamento de coordinación de TI a nivel institucional.

- Área de administración de sistemas de información y nuevas tecnologías:

Responsables de planificar y supervisar todas las tareas involucradas con el desarrollo y mantenimiento de software de los sistemas de información a nivel institucional.

- Área de Administración de base de datos:

Responsable del control, mantenimiento y desarrollo de bases de datos, monitoreando el desempeño de la BD para garantizar que se manejen parámetros adecuados y brinde respuestas en tiempo real a los usuarios.

3.1.2 Organigrama Estructural del departamento de TI.

Según el documento: “Organigrama de Puestos de TI”, de la Dirección de tecnologías de la información y comunicación, a cargo del Coordinador de TICS el Ingeniero Roberto

Balón, se muestra en la Figura 6, el organigrama estructural donde se detalla la distribución el departamento de TI en cuanto a niveles jerárquicos o cargos profesionales.

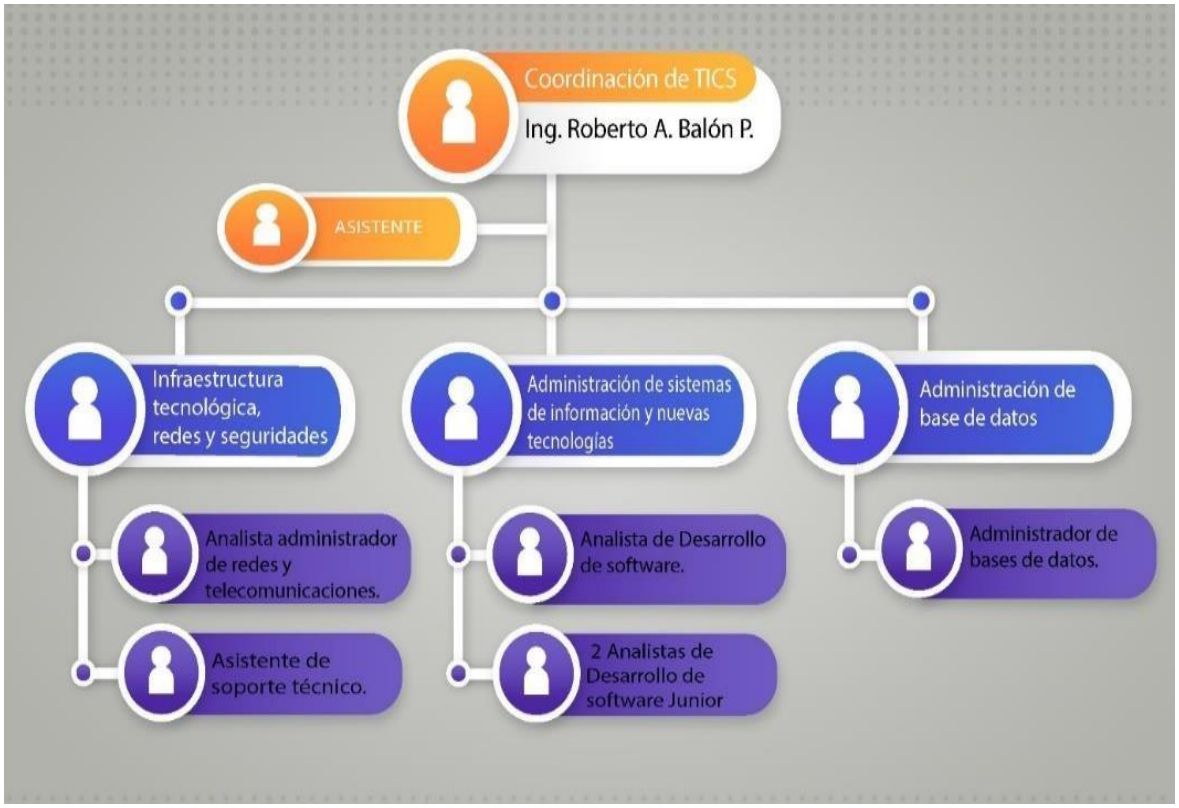


Figura 5: Organigrama Estructural del departamento de TI.

3.1.3 Organigrama Estructural de la compañía

A nivel organizacional la empresa AGUAPEN está dividida en 5 niveles, el nivel legislativo, el nivel ejecutivo, nivel asesor, nivel de apoyo y control, y el nivel operativo como se muestra a continuación:

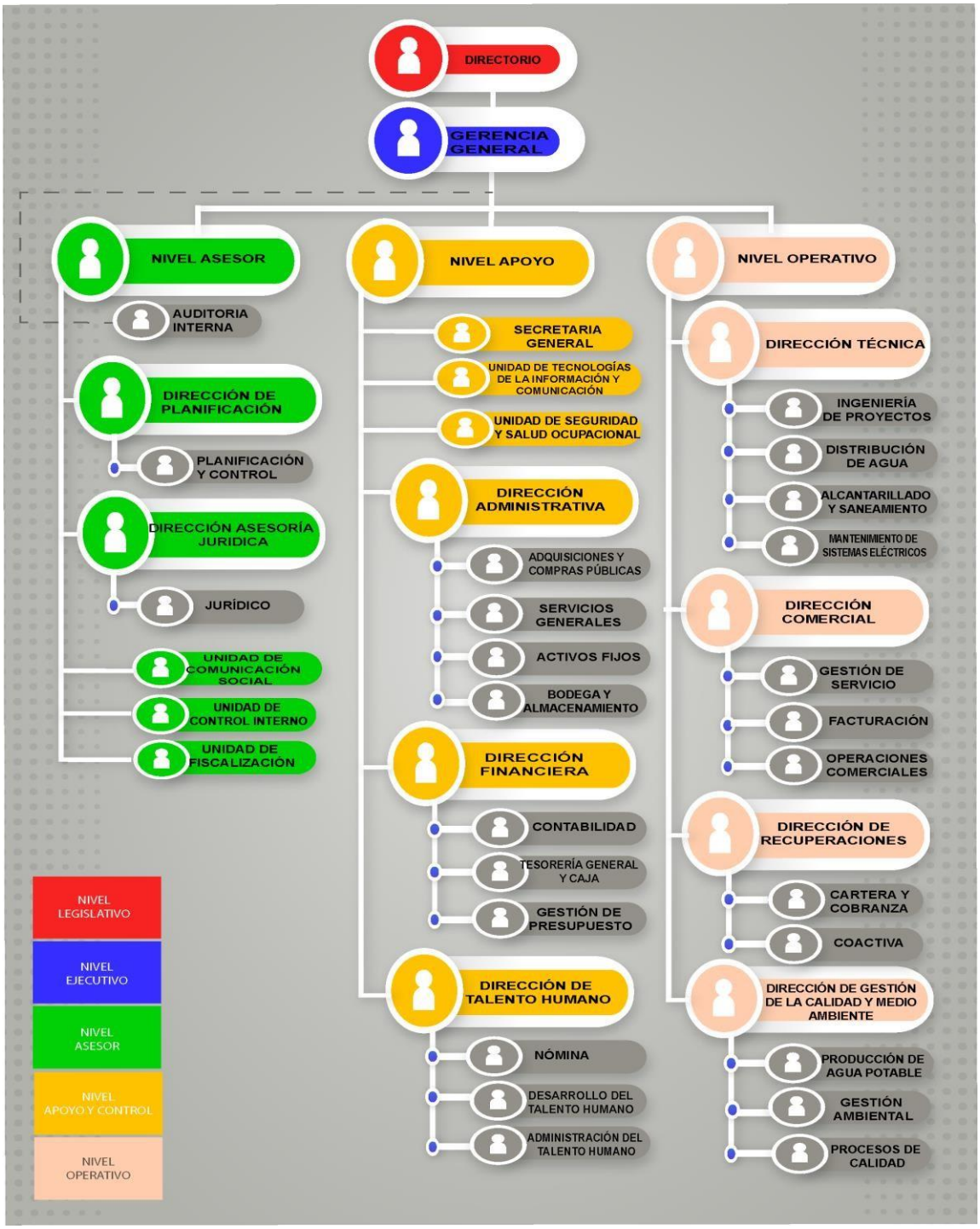


Figura 6: Organigrama Estructural de la compañía. Elaboración Propia

3.1.4 Diagrama de red de la institución.

A continuación, se presenta el diagrama de red actual de la empresa, así como también el equipamiento Core conformado por dispositivos y equipos de comunicación, proveedores

de internet y medios de transmisión (Fibra Óptica y Cable UTP) efectuados en los diferentes sectores de institución para el correcto funcionamiento de los servicios existentes en la compañía.

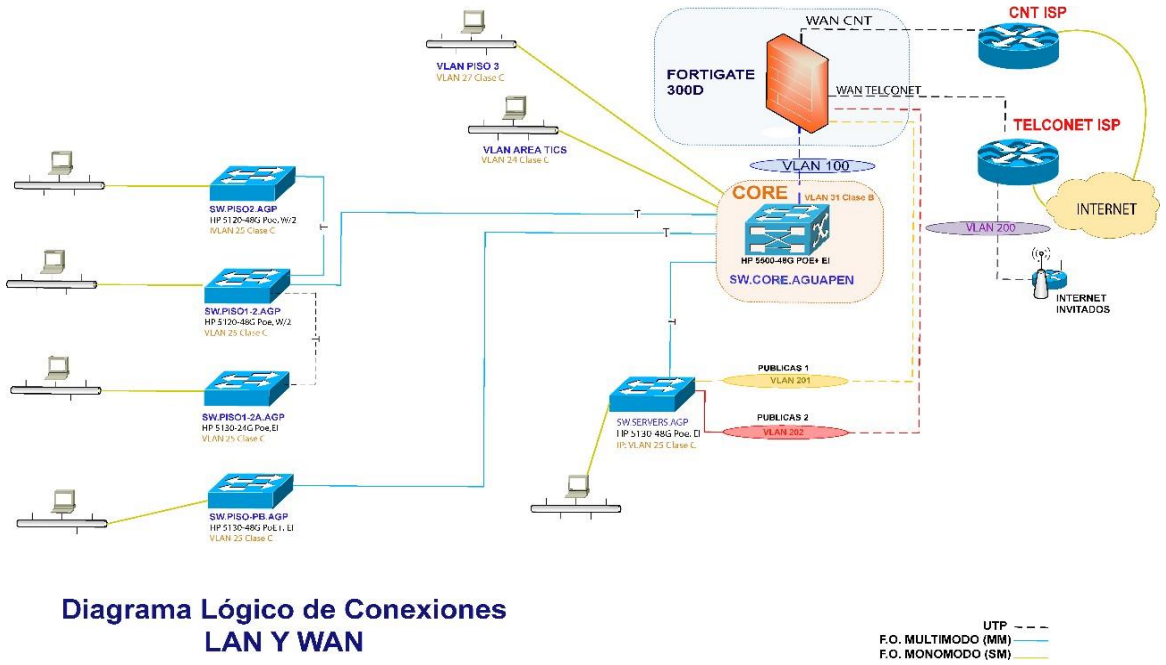


Figura 7: Diagrama de Red de la empresa. Elaboración Propia.

3.1.5 Servicios Funcionales

Para el cumplimiento de esta fase se realizaron visitas periódicas y entrevistas a los responsables de las funciones del departamento de TI de la compañía AGUAPEN EP, quienes permitieron recolectar la información. Para realizar la valoración de los activos, resulta necesario que la institución identifique los distintos servicios que se apoyan de los activos presentes en el área de TI.

El centro de datos del área de Tecnologías de la Información proporciona los siguientes servicios:

- Sistema Financiero
- Sistema Comercial

- Bases de datos
- Correo Electrónico Institucional.
- Servicios Web.
- Servicios de digitalización.
- Controlador de Dominio
- Internet.
- Cableado Estructurado.
- Redes Inalámbricas.
- Equipos de cómputo.
- Soporte técnico.

3.1.6 Caracterización de los activos

Resulta imprescindible identificar y clasificar los activos de información, ya sean de software, hardware, redes, infraestructura dentro de la institución, precisar su valoración mediante las dimensiones de seguridad establecidas y determinar las dependencias entre ellos

Identificación de los Tipos de Activos

Tipos de activos	Descripción
Software	Herramientas que permiten manejar los datos.
Hardware y aplicaciones.	Equipos informáticos que permiten alojar datos, servicios
Comunicaciones, Redes.	Redes y dispositivos que permiten transmitir e intercambiar datos.
Equipamiento Auxiliar	Son complementos necesarios para los elementos informáticos.
Infraestructura	Parte esencial para la instalación de los sistemas de información y comunicaciones.
Personal	Personas encargadas del manejo, administración y control de la información.

Tabla 2: Tipos de activos. Elaboración propia

Mediante técnicas de recolección de información, se identificó los activos de información asociados a los procesos del centro de datos de la Empresa AGUPEN-EP.

TIPO DE ACTIVO	ID	Activo	DESCRIPCIÓN	FUNCIONARIO QUE RESGUARDA	FUNCIONARIO RESPONSABLE
INFRAESTRUCTURA	ACT001	SERVIDOR HP PROLIANT DL380 GEN 9	Servidor físico principal que contiene a los demás servidores virtuales	Jefe de Infraestructura Tecnológica	Coordinador de Tecnologías de la Información.
	ACT002	SERV_SISTEMA_FINANCIERO	Servidor que contiene el sistema financiero bajo el lenguaje JAVA	Jefe de Infraestructura Tecnológica	Analista de desarrollo de software.
	ACT003	SERV_BD_SISTEMA_FINANCIERO	Servidor que contiene la base de datos del sistema financiero bajo ORACLE DATABASE	Jefe de Infraestructura Tecnológica	Administrador de base de datos
	ACT004	SERV_SISTEMA_COMERCIAL	Servidor virtualizado que contiene el sistema comercial bajo el lenguaje C#	Jefe de Infraestructura Tecnológica.	Analista de desarrollo junior.
	ACT005	SERV_BD_SISTEMA_COMERCIAL	Servidor que contiene la base de datos del sistema comercial bajo SQL SERVER	Jefe de Infraestructura Tecnológica	Administrador de base de datos
	ACT006	SERV_CORREO_ELECTRONICO	servidor de correo ZIMBRA utilizado por el personal administrativo.	Jefe de Infraestructura Tecnológica	Jefe de Infraestructura Tecnológica
	ACT007	SER_PAGINA_WEB	Servidor web utilizado para la página institucional de la compañía	Jefe de Infraestructura Tecnológica	Analista de desarrollo junior.
	ACT008	SERV_DOMINIO	Servidor de dominio de las máquinas de los funcionarios bajo el sistema operativo WINDOWS SERVER 2016	Jefe de Infraestructura Tecnológica	Jefe de Infraestructura Tecnológica
	ACT009	SERV_FTP	Servidor de transferencia de archivos bajo WINDOWS SERVER 2016	Jefe de Infraestructura Tecnológica	Jefe de Infraestructura Tecnológica
	ACT010	SERV_DIGITALIZACION	Servidor centralizado para digitalización de archivos OPENSOURCE	Jefe de Infraestructura Tecnológica	Jefe de Infraestructura Tecnológica

	ACT011	SERV_ KERIO	Servidor VPN -para túneles con conexión a tenencias exteriores bajo WINDOWS 7	Jefe de Infraestructura Tecnológica	Jefe de Infraestructura Tecnológica
	ACT012	SERV_BIOMETRICO	Servidor centralizado para marcaciones de ingreso del personal de la institución.	Jefe de Infraestructura Tecnológica	Jefe de Infraestructura Tecnológica
COMUNICACIONES, REDES.	ACT013	SWITCH CORE HP 5500AF48G-POE	Switch Core o switch principal	Jefe de Infraestructura Tecnológica	Asistente de soporte técnico.
	ACT014	SWITCH ACCESS HP 5120AF48G-POE	Switches secundario	Jefe de Infraestructura Tecnológica	Asistente de soporte técnico.
	ACT015	SWITCH CISCO CATALYST 2960	Switches utilizados para los departamentos de la compañía	Jefe de Infraestructura Tecnológica	Asistente de soporte técnico.
	ACT016	ROUTER CNT ISP	Router primario de internet, Servicio CNT	Jefe de Infraestructura Tecnológica	Asistente de soporte técnico.
	ACT017	ROUTER TELCONET ISP	ROUTER secundario de internet utilizado cuando el primario no está disponible Servicio TELCONET	Jefe de Infraestructura Tecnológica	Asistente de soporte técnico.
	ACT018	WIRELESS ROUTER HUAWEI	WIRELESS ROUTER para brindar internet a los usuarios externos o invitados	Jefe de Infraestructura Tecnológica	Asistente de soporte técnico.
HARDWARE Y APLICACIONES.	ACT019	CPU DELL CORE I5 OCTAVA GENERACION	CPU de la máquina del jefe coordinador de TI	Asistente de soporte técnico.	Asistente de soporte técnico.
	ACT020	CPU HP CORE I7 SEPTIMA GENERACION	CPU de la máquina del jefe de infraestructura tecnológica	Asistente de soporte técnico.	Asistente de soporte técnico.
	ACT021	CPU DELL CORE I7 SEPTIMA GENERACION	CPU de la máquina del administrador de base de datos	Asistente de soporte técnico.	Asistente de soporte técnico.
	ACT022	CPU DELL CORE I7 SEPTIMA GENERACION	CPU de la máquina del analista de desarrollo de software	Asistente de soporte técnico.	Asistente de soporte técnico.
	ACT023	CPU DELL CORE I7 SEPTIMA GENERACION	CPU de la máquina del desarrollo junior	Asistente de soporte técnico.	Asistente de soporte técnico.

	ACT024	CPU DELL CORE I5 SEPTIMA GENERACION	CPU de la máquina del analista de soporte técnico	Asistente de soporte técnico.	Asistente de soporte técnico.
	ACT025	CENTRAL TELEFONICA IP PANASONIC HIBRIDA KX-NS500	CPU de la máquina del jefe de infraestructura tecnológica	Asistente de soporte técnico.	Asistente de soporte técnico.
	ACT026	IMPRESORA HP PAGEWIDE PRO 477	Impresora utilizada en el departamento de TI	Asistente de soporte técnico.	Coordinador de Tecnologías de la Información.
EQUIPAMIENTO AUXILIAR	ACT027	UPS COMPUTER PONER 3KVA	Ups utilizados como sistema de alimentación ininterrumpida	Asistente de soporte técnico.	Asistente de soporte técnico.
	ACT028	NVR HIKVISION	NVR marca HIKVISION utilizado para el monitoreo de las cámaras de seguridad de la institución	Asistente de soporte técnico.	Asistente de soporte técnico.
	ACT029	Cableado	Cable estructurado implementado en la infraestructura de red de la institución	Asistente de soporte técnico.	Asistente de soporte técnico.
	ACT030	Aire Acondicionado	Aires acondicionados utilizados en el departamento de TICS y en el Data Center	Asistente de soporte técnico.	Asistente de soporte técnico.
SOPORTES DE INFORMACIÓN	ACT031	Discos Duros Externos.	Discos duros de almacenamiento sin espacio que almacenan formación de equipos de cómputo y servidores	Asistente de soporte técnico.	Asistente de soporte técnico.
	ACT032	Blu-ray Disk	Discos Blu-ray con documentación del departamento	Asistente de soporte técnico.	Asistente de soporte técnico.
	ACT033	Memorias USB	Memorias USB que almacenan información del talento humano del departamento de TICS	Asistente de soporte técnico.	Asistente de soporte técnico.
	ACT034	Resmas de papel impresas.	Utilizadas para impresiones de datos y documentos del departamento de TICS	Asistente de soporte técnico.	Asistente de soporte técnico.
PERSONAL	ACT035	TALENTO HUMANO	Personal de TICS encargados del desarrollo de las	Coordinador de Tecnologías de la Información.	Coordinador de Tecnologías

			actividades del departamento.		de la Información.

Tabla 3: Matriz de identificación de activos. Elaboración propia

3.2. FASE 2: EVALUACIÓN DEL RIESGO

Una vez definidos los procesos y activos de información se identifican las amenazas que generan riesgos y pueden afectar dichos activos.

3.2.1. Tipos de amenazas

Según Tarazona 2019[28], los tipos de amenazas pueden ser:

3.2.1.1 Causadas por la naturaleza

Hay accidentes naturales (sismos, inundaciones) en donde la información es víctima pasiva, pero no por ser pasivos hay que permanecer indefensos [29].

3.2.1.2 Causados por fallas en la tecnología

Nacen o surgen en el equipamiento propio de la infraestructura por defectos en su diseño o implementación, generando consecuencias negativas sobre la información. Frecuentemente se denominan vulnerabilidades técnicas [29].

3.2.1.3 Causadas por errores u omisiones

Las personas con acceso a los sistemas de información pueden ser el origen de problemas no intencionados o simplemente causados por el cometimiento de un error [29].

3.2.1.4. Causadas por los humanos

Los usuarios con acceso a los sistemas de información pueden ser origen de problemas intencionado tales como hacking, ataques ransomware, virus; con ánimo de beneficiarse indebidamente, o por el simple hecho de causar daños y perjuicios a la propiedad intelectual [29].

3.2.2. Identificación de Amenazas

A continuación, se definió un listado de las posibles amenazas que podrían afectar a los activos de información en conjunto con el responsable de redes y seguridades del departamento de TI. Las amenazas fueron clasificadas considerando si las mismas son

causadas por: la naturaleza, los humanos, errores u omisiones, y fallas de la tecnología, así como a qué elementos afectan:

CLASIFICACIÓN	NO. REFERENCIA AMENAZA	AMENAZA	AGENTE DE AMENAZA
Causados por la naturaleza	A-002	Sismo	Natural
	A-003	Polvo	Natural
	A-004	Inundación	Natural
	A-005	Incendio	Personal / falla
	A-006	Temperaturas excesivamente altas	Natural
	A-007	Epidemias	Personal
Causados por humanos	A-008	Acceso de terceros a los servidores.	Hacker / Cracker
	A-009	Denegación de Servicio DDOS	Hacker / Cracker
	A-011	Inyección por SQL	Hacker / Cracker
	A-013	Format string bugs	Personal de Desarrollo
	A-014	Acceso no autorizado	Personal Descontento
	A-015	Sabotaje	Personal Descontento
	A-016	Fuga de datos	Personal
	A-017	Ataque Cross-Site Scripting	Hacker / Cracker
	A-018	Ataques DNS basados en botnets	Hacker / Cracker
	A-019	Password Spaying	Hacker / Cracker
	A-020	Manipulación de archivos compartidos	Hacker / Cracker
	A-021	Malware	Hacker / Cracker
	A-022	Ataque Man in the middle	Scriptkiddie
	A-023	Errores en la administración	Empleado sin experiencia
	A-024	Hurto	Personal Descontento
	A-025	Phishing	Hacker / Cracker
	A-026	Ingeniería social	Hacker / Cracker
Causados por errores u omisiones	A-027	Acceso no autorizado	Personal Descontento
	A-028	Errores en la organización	Empleado sin experiencia

	A-029	Sobrecargas y cortes de energía eléctrica	Suministrador de energía eléctrica / falla
	A-030	Variaciones de voltaje	Material (falla)
	A-031	Limitado espacio en centro de cómputo	Material (falla)
	A-032	Virus en computadoras de los encargados del departamento de TIC	Hacker / Cracker
Causados por fallas de la tecnología	A-033	Filtración de componentes en estado liquido	Material (falla)
	A-034	Infección del sistema	Scriptkiddie
	A-035	fallos operativos	Proveedor
	A-036	Intrusos en la red wifi	Scriptkiddie
	A-037	Carencia de equipos de videovigilancia	Falta de financiamiento
	A-038	Fallos en cámaras de videovigilancia	Falta de financiamiento
	A-039	Periféricos o Componentes defectuosos	Material (falla)

Tabla 4: Elementos Afectados por el tipo de amenaza. Elaboración Propia.

3.2.3 Amenazas, vulnerabilidades y riesgo en los activos de la información.

A continuación, se identifican las amenazas, vulnerabilidades y por ende el riesgo inherente al que están expuestos los activos de información:

TIPO DE ACTIVO	ID	ACTIVO	CÓDIGO AMENAZA	AMENAZA	AGENTE DE AMENAZA	VULNERABILIDAD	RIESGO
INFRAESTRUCTU	ACT001	SERVIDOR HP PROLIANT DL380 GEN 9	A-008	Acceso de terceros al servidor.	Hacker / Cracker	Puertos abiertos en el servidor	Uso puertos abiertos para escala de privilegios / robo de información
			A-009	Denegación de Servicio DDOS	Hacker / Cracker	Infecciones en la red	Inaccesibilidad a los servicios del servidor

			A-002	Sismo	Natural	Techo falso en mal estado	Daños físicos/ destrucción
			A-029	Sobrecargas y cortes de energía eléctrica	Suministrador de energía eléctrica / falla	Partes del hardware del servidor con falencias	Daños a nivel lógico y físico de los componentes y servicios
			A-004	Inundación	Natural	Carencia de medidas preventivas	Pérdida material afectaciones directas en el servidor físico
			A-027	Acceso no autorizado	Personal Descontento	Data Center sin adecuada protección de acceso	Cambios, modificación, destrucción
	ACT002	SERV_SISTEMA_FINANCIERO	A-034	Infección de sistema	Scriptkiddie	Fallo en el sistema	Pérdida de información
			A-030	Variaciones de voltaje	Material (falla)	Indisponibilidad del sistema por periodo de inactividad	Fallo y daños a nivel operativo
	ACT003	SERV_BD_SISTEMA_FINANCIERO	A-011	Inyección por SQL	Hacker / Cracker	Carencia de un saneamiento de entrada adecuado.	Robo de información
	ACT004	SERV_SISTEMA_COMERCIAL	A-012	Infección de sistema	Scriptkiddie	Fallo en el sistema	Pérdida de información
			A-013	Format string bugs	Personal de desarrollo	Errores de cadena de formato / ejecución de código arbitrario	Revelación de información.
	ACT005	SERV_BD_ SISTEMA_COMERCIAL	A-011	Inyección por SQL	Hacker / Cracker	Carencia de un saneamiento de entrada adecuado.	Robo de información
			A-015	Sabotaje	Personal Descontento	Personal de confianza que quiera acceder a la base de datos	Pérdida de datos
	ACT006	SERV_CORREO_ELECTRONICO	A-016	Fuga de datos	Personal	Falta de cifrado de protocolos SMTP, POP3 e IMAP	Perdida de datos
			A-009	Denegación de Servicio DDOS	Hacker / Cracker	Carencia de la limitación de conexiones al servidor SMTP	Inaccesibilidad a los servicios del servidor
	ACT007	SER_PAGINA_WEB	A-017	Ataque Cross-Site Scripting	Hacker / Cracker	Datos sin validar	Robo de información
			A-011	Inyección por SQL	Hacker / Cracker	Carencia de un saneamiento de entrada adecuado.	Robo de información

	ACT008	SERV_DOMINIO	A-018	Ataques DNS basados en botnets	Hacker / Cracker	Ordenadores conectados posiblemente infectados	Pérdida de datos
			A-019	Password Spaying	Hacker / Cracker	Contraseñas de acceso al servicio de Active Directory comúnes entre los usuarios	Robo de información
	ACT09	SERV_FTP	A-020	Manipulación de archivos compartidos	Hacker / Cracker	Carece de encriptación y autenticación	Pérdida de datos
			A-021	Malware	Hacker / Cracker	Desactualización de parches de seguridad	Robo de información
	ACT010	SERV_ DIGITALIZACION	A-004	Inundación	Natural	Carencia de medidas preventivas	Daños a nivel lógico y físico de los componentes y servicios
	ACT011	SERV_ KERIO	A-021	Malware	Hacker / Cracker	Uso de VPN por funcionarios desde sus hogares con máquinas vulnerables a malware	Intercepción de datos
	ACT012	SERV_BIOMETRICO	A-033	Filtración de componentes en estado liquido	Material (falla)	Equipo descontinuado (averías)	Daños en el hardware
COMUNICACIONES, REDES.	ACT013	SWITCH CORE HP 5500AF48G-POE	A-022	Ataque Man in the middle	Hacker / Cracker	Desactualización de firmware / parches de seguridad	leer, insertar y modificar información
			A-003	Polvo	Natural	carencia de fechas fijas para mantenimiento preventivo	Daños a nivel lógico y físico de los componentes y servicios
	ACT014	SWITCH ACCESS HP 5120AF48G-POE	A-022	Ataque Man in the middle	Hacker / Cracker	Desactualización de firmware / parches de seguridad	leer, insertar y modificar información
			A-004	Inundación	Natural	Carencia de medidas preventivas	Daños a nivel lógico y físico de los componentes y servicios
	ACT015	SWITCH CISCO CATALYST 2960	A-022	Ataque Man in the middle	Scriptkiddie	Desactualización de firmware / parches de seguridad	leer, insertar y modificar información
			A-004	Inundación	Material (falla)	Carencia de medidas preventivas	Daños a nivel lógico y físico de los componentes y servicios
	ACT016	ROUTER CNT ISP	A-035	Fallos operativos	Proveedor	Desactualización de firmware / parches de seguridad	Pérdida de información

			A-004	Inundación	Material (falla)	Carencia de medidas preventivas	Daños a nivel lógico y físico de los componentes y servicios
	ACT017	ROUTER TELCONET ISP	A-035	Fallos operativos	Proveedor	Desactualización de firmware /parches de seguridad	Pérdida de información
	ACT018	WIRELESS ROUTER HUAWEI	A-035	Intrusos en la red wifi	Scriptkiddie	Protocolos de cifrado descontinuados	Robo de información
HARDWARE Y APLICACIONES.	ACT019	CPU DELL CORE I5 OCTAVA GENERACION	A-032	Virus en pc del Coordinador de TIC	Hacker / Cracker	Presencia de malware en la red	Robo de información
			A-003	Polvo	Natural	carencia de fechas fijas para mantenimiento preventivo	Daños en el hardware
	ACT020	CPU HP CORE I7 SEPTIMA GENERACION	A-032	Virus en pc del Administrador de base de datos	Hacker / Cracker	Presencia de malware en la red	Robo de información
	ACT021	CPU DELL CORE I7 SEPTIMA GENERACION	A-032	Virus en pc del Jefe de Infraestructura	Hacker / Cracker	Presencia de malware en la red	Robo de información
			A-003	Polvo	Natural	carencia de fechas fijas para mantenimiento preventivo	Daños en el hardware
	ACT022	CPU DELL CORE I7 SEPTIMA GENERACION	A-032	Virus en pc del Desarrollador	Falta de financiamiento	Discos defectuosos	Pérdida de información
			A-003	Polvo	Natural	carencia de fechas fijas para mantenimiento preventivo	Daños a nivel lógico y físico de los componentes y servicios
	ACT023	CPU DELL CORE I5 SEPTIMA GENERACION	A-032	Virus en pc del Desarrollador Junior	Falta de financiamiento	Discos defectuosos	Pérdida de información
			A-003	Polvo	Natural	carencia de fechas fijas para mantenimiento preventivo	Daños a nivel lógico y físico de los componentes y servicios
	ACT024	CENTRAL TELEFONICA IP PANASONIC	A-004	Inundación	Natural	Carencia de medidas preventivas	Daños en el hardware
			A-003	Polvo	Natural	carencia de fechas fijas para mantenimiento preventivo	Daños a nivel lógico y físico de los componentes y servicios
	ACT025	IMPRESORA HP PAGEWIDE PRO 477	A-004	Inundación	Natural	Carencia de medidas preventivas	Daños en el hardware

EQUIPAMIENTO AUXILIAR	ACT026	UPS COMPUTER PONER 3KVA	A-030	Variaciones de voltaje	Material (falla)	UPS descontinuado	Fallo y daños a nivel operativo
	ACT027	NVR HIKVISION	A-037	Carencia de equipos de seguridad	Falta de financiamiento	Puntos Ciegos (sin monitoreo)	Intrusión de terceros al departamento de mantenimiento y bodega
			A-038	Fallos en cámaras de videovigilancia	Natural	Indisponibilidad del sistema por periodo de inactividad	Grabaciones incompletas
	ACT028	CABLEADO	A-028	Errores en la organización	Empleado sin experiencia	Interrupciones constantes / ruido	Pérdida de datos
			A-014	Acceso no autorizado	Personal sin experiencia	Deficiente o nulo etiquetado del cable	Desorientación para realizar mantenimiento a cableado estructurado
	ACT029	AIRE ACONDICIONADO	A-003	Polvo	Natural	Carencia de fechas fijas para mantenimiento preventivo	Daños en el hardware
			A-004	Inundación	Natural	Carencia de medidas preventivas	Daños en el hardware
Soportes de Información	ACT030	DISCOS DUROS EXTERNOS	A-024	Hurto	Personal Descontento	Carencia de fechas fijas para mantenimiento preventivo	Robo de información
			A-015	Sabotaje	Personal Descontento	Libre acceso a discos duros en el área de soporte	Robo de información
	ACT031	BLU-RAY DISK	A-024	Hurto	Personal Descontento	Carencia de fechas fijas para mantenimiento preventivo	Robo de información
			A-015	Sabotaje	Personal Descontento	Libre acceso a discos blu-ray en el área de soporte	Robo de información
	ACT032	MEMORIAS USB	A-039	Periféricos o Componentes defectuosos	Material (falla)	Dispositivos con averías físicas	Robo de información
			A-024	Hurto	Personal Descontento	Libre acceso a dispositivos USB en el área de soporte	Robo de información
	ACT033	PAPEL IMPRESO.	A-005	Incendio	Personal / falla	Documentación sin respaldo en la nube	Pérdida de información
			A-024	Hurto	Personal Descontento	Falta de organización de documentos en folders	Robo de información
PERSO	ACT034	TALENTO HUMANO	A-007	Epidemias	Personal	Contagios COVID-19	Riesgos de contagios del personal

			A-025	Phishing	Hacker / Cracker	Falta de capacitación sobre ciberseguridad	Robo de información
			A-026	Ingeniería social	Hacker / Cracker	Falta de capacitación sobre ciberseguridad	Robo de información

Tabla 5: Identificación de Amenazas, vulnerabilidades y riesgos en los activos de la información. Elaboración propia.

3.2.4 Cálculo del impacto sobre los activos de información

A continuación, se presentan los niveles establecidos para la valoración del impacto que tendrían las amenazas sobre los activos de la información.

3.2.4.1 Valor del impacto en términos de la pérdida de la confidencialidad

CONFIDENCIALIDAD	CRITERIO
Alto (3)	La divulgación no autorizada de la información tiene un efecto crítico para la institución Ej. Divulgación de información confidencial o sensible.
Medio (2)	La divulgación no autorizada de la información tiene un efecto limitado para la institución Ej. Divulgación de información de uso interno
Bajo (1)	La divulgación de la información no tiene ningún efecto para la institución Ej. Divulgación de información pública.

Valoración del impacto en términos de la confidencialidad. [30]

3.2.4.2 Valor del impacto en términos de la pérdida de la integridad

INTEGRIDAD	CRITERIO
Alto (3)	La destrucción o modificación no autorizada de la información tiene un efecto severo para la institución
Medio (2)	La destrucción o modificación no autorizada de la información tiene un efecto considerable para la institución
Bajo (1)	La destrucción o modificación de la información tiene un efecto leve para la institución

Valoración del impacto en términos de la integridad. [30]

3.2.4.3 Valor del impacto en términos de la pérdida de la disponibilidad

DISPONIBILIDAD	CRITERIO
Alto (3)	La interrupción al acceso de la información o los sistemas tienen un efecto severo para la institución
Medio (2)	La interrupción al acceso de la información o los sistemas tienen un efecto considerable para la institución
Bajo (1)	interrupción al acceso de la información o los sistemas tienen un efecto mínimo para la institución

Valoración del impacto en términos de la disponibilidad [30]

3.2.4.4 Valoración del impacto sobre el activo (VA)

La valoración del impacto sobre un activo (VA), es el cálculo del promedio de los valores de la Gestión de la Seguridad de la Información:

$$\mathbf{VA} = \frac{\mathbf{C} + \mathbf{I} + \mathbf{D}}{\mathbf{3}}$$

En referencia a las valoraciones antes mencionadas, se procede a la valorar el impacto medido en relación con la confidencialidad, integridad y disponibilidad sobre los activos, ya que estas son las dimensiones en que se basa la seguridad de la información.

TIPO DE ACTIVO	ID	ACTIVO	Valoración de impacto **C**: Confidencialidad **I**: Integridad **D**: Disponibilidad				VALORACIÓN DE IMPACTO CID	NIVEL DE IMPACTO
			C	**I**	**D**	TOTAL		
INFRAESTRUCTURA	ACT001	SERVIDOR HP PROLIANT DL380 GEN 9	3	3	3	9	3	ALTO
	ACT002	SERV_SISTEMA_FINANCIERO	3	3	3	9	3	ALTO
	ACT003	SERV_BD_SISTEMA_FINANCIERO	3	3	3	9	3	ALTO
	ACT004	SERV_SISTEMA_COMERCIAL	3	3	3	9	3	ALTO
	ACT005	SERV_BD_ SISTEMA_COMERCIAL	3	3	3	9	3	ALTO
	ACT006	SERV_CORREO_ELECTRONICO	3	3	3	9	3	ALTO
	ACT007	SER_PAGINA_WEB	2	3	3	8	2,67	ALTO
	ACT008	SERV_DOMINIO	3	3	3	9	3	ALTO
	ACT009	SERV_FTP	2	2	3	7	2,33	ALTO
	ACT010	SERV_ DIGITALIZACION	1	2	3	6	2	MEDIO
	ACT011	SERV_ KERIO	3	3	3	9	3	ALTO
	ACT012	SERV_BIOMETRICO	1	2	2	5	1,67	BAJO
COMUNICACIONES, REDES.	ACT013	SWITCH CORE HPE 5500AF48G-POE	2	2	3	7	2,33	ALTO
	ACT014	SWITCH ACCESS HPE 5120AF48G-POE	2	3	3	8	2,67	ALTO

	ACT015	SWITCH CISCO CATALYST 2960	2	3	3	8	2,67	ALTO
	ACT016	ROUTER CNT ISP	2	2	3	7	2,33	ALTO
	ACT017	ROUTER TELCONET ISP	2	2	3	7	2,33	ALTO
	ACT018	WIRELESS ROUTER HUAWEI	2	3	3	8	2,67	ALTO
HARDWARE Y APLICACIONES.	ACT019	CPU DELL CORE I5 OCTAVA GENERACION	2	2	3	7	2,33	ALTO
	ACT020	CPU HP CORE I7 SEPTIMA GENERACION	2	2	3	7	2,33	ALTO
	ACT021	CPU DELL CORE I7 SEPTIMA GENERACION	2	2	3	7	2,33	ALTO
	ACT022	CPU DELL CORE I7 SEPTIMA GENERACION	2	2	3	7	2,33	ALTO
	ACT023	CPU DELL CORE I5 SEPTIMA GENERACION	2	2	3	7	2,33	ALTO
	ACT024	CENTRAL TELEFONICA IP PANASONIC HIBRIDA KX-NS500	2	2	3	7	2,33	ALTO
	ACT025	IMPRESORA HP PAGEWIDE PRO 477	2	2	3	7	2,33	ALTO
EQUIPAMIENTO AUXILIAR	ACT026	UPS COMPUTER PONER 3KVA	2	3	3	8	2,67	ALTO
	ACT027	NVR HIKVISION	2	3	3	8	2,67	ALTO
	ACT028	CABLEADO	2	3	3	8	2,67	ALTO
	ACT029	AIRE ACONDICIONADO	1	2	3	6	2	MEDIO
SOPORTES DE INFORMACIÓN	ACT030	DISCOS DUROS EXTERNOS	2	2	3	7	2,33	ALTO
	ACT031	BLU-RAY DISK	2	2	3	7	2,33	ALTO
	ACT032	MEMORIAS USB	2	2	3	7	2,33	ALTO
	ACT033	PAPEL IMPRESO	2	2	2	6	2	MEDIO
PERSONAL	ACT034	TALENTO HUMANO	2	2	3	7	2,33	ALTO

Tabla 6: Nivel de impacto CID. Elaboración Propia

3.3 Cálculo de la probabilidad de ocurrencia

Luego de identificar el nivel de impacto, se hace uso del análisis de tipo cualitativo, el cual usa una escala de calificación de atributos para describir la magnitud de las consecuencias potenciales (por ejemplo, baja, media y alta) y la probabilidad de esas consecuencias.

A continuación, se detallan los criterios calificativos y valores numéricos a ser asignados para la valoración de la probabilidad de amenazas que podrían resultar en una vulnerabilidad existente.

3.3.1 Criterio de probabilidad de ocurrencia de vulnerabilidades

NIVEL DE VULNERABILIDAD	CRITERIO	EJEMPLO
Alto (3)	No existe ninguna medida de seguridad implementada para prevenir la ocurrencia de la amenaza	No se utilizan contraseñas para que los usuarios ingresen a los sistemas
Medio (2)	Existen medidas de seguridad implementadas que no reducen la probabilidad de ocurrencia de la amenaza a un nivel aceptable	Existen normas para la utilización de contraseñas, pero no se implementa
Bajo (1)	La medida de seguridad es adecuada	Existen normas para la utilización de contraseñas y es aplicada

Criterio de probabilidad de ocurrencia de vulnerabilidad [30]

3.3.2 Criterio de probabilidad de ocurrencia de amenazas

Nivel de amenazas	Criterio por probabilidad	Criterio por condición de ocurrencia	Criterio por atractivo	Ejemplo
Alto (3)	La ocurrencia es muy probable (probabilidad > 50%)	Bajo circunstancias normales	El atacante se beneficia en gran medida por el ataque, tiene la capacidad técnica para ejecutarlo y la vulnerabilidad es fácilmente explotable	Código malicioso
Medio (2)	La ocurrencia es probable (probabilidad =50%)	Por errores descuidos	El atacante se beneficia de alguna manera por el ataque, tiene la capacidad técnica para ejecutarlo y la vulnerabilidad es fácilmente explotable	Falla de hardware
Bajo (1)	La ocurrencia es menos probable (probabilidad >0 y <50%)	En rara ocasión	El atacante no se beneficia del ataque	Desastres naturales

Criterio de probabilidad de ocurrencia de amenaza [30]

3.3.3 Calculo del nivel de probabilidad de ocurrencia.

TIPO DE ACTIVO	ID	ACTIVO	CODIGO AMENAZA	AMENAZA	AGENTE DE AMENAZA	VULNERABILIDAD	PROBABILIDAD DE OCURRENCIA DE AMENAZA		PROBABILIDAD DE OCURRENCIA DE VULNERABILIDAD	
INFRAESTRUCTURA	ACT001	SERVIDOR HP PROLIANT DL380 GEN 9	A-008	Acceso de terceros al servidor.	Hacker / Cracker	Puertos abiertos en el servidor	3	ALTO	2	MEDIO
			A-009	Denegación de Servicio DDOS	Hacker / Cracker	Infecciones en la red	3	ALTO	2	MEDIO
			A-002	Sismo	Natural	Techo falso en mal estado	2	MEDIO	3	ALTO
			A-029	Sobrecargas y cortes de energía eléctrica	Suministrador de energía eléctrica / falla	Partes del hardware del servidor con falencias	2	MEDIO	3	ALTO
			A-004	Inundación	Natural	Carencia de medidas preventivas	2	MEDIO	3	ALTO
			A-027	Acceso no autorizado	Personal Descontento	Data Center sin adecuada protección de acceso	2	MEDIO	2	MEDIO
	ACT002	SERV_SISTEMA_FINANCIERO	A-034	Infección de sistema	Scriptkiddie	Fallo en el sistema	3	ALTO	3	ALTO
			A-030	Variaciones de voltaje	Material (falla)	Indisponibilidad del sistema por periodo de inactividad	2	MEDIO	3	ALTO
	ACT003	SERV_BD_SISTEMA_FINANCIERO	A-011	Inyección por SQL	Hacker / Cracker	Carencia de un saneamiento de entrada adecuado.	2	MEDIO	3	ALTO
	ACT004	SERV_SISTEMA_COMERCIAL	A-012	Infección de sistema	Scriptkiddie	Fallo en el sistema	2	MEDIO	3	ALTO
			A-013	Format string bugs	Desarrollador	Errores de cadena de formato / ejecución de código arbitrario	2	MEDIO	3	ALTO
	ACT007	SERV_BD_SISTEMA_COMERCIAL	A-011	Inyección por SQL	Hacker / Cracker	Carencia de un saneamiento de entrada adecuado.	2	MEDIO	3	ALTO

			A-015	Sabotaje	Personal Descontento	Personal de confianza que quiera acceder a la base de datos	2	MEDIO	2	MEDIO
	ACT008	SERV_CORREO_ELECTRONICO	A-016	Fuga de datos	Hacker / Cracker	Falta de cifrado de protocolos SMTP, POP3 e IMAP	3	ALTO	2	MEDIO
			A-009	Denegación de Servicio DDOS	Hacker / Cracker	Carencia de la limitación de conexiones al servidor SMTP	3	ALTO	2	MEDIO
	ACT009	SER_PAGINA_WEB	A-017	Ataque Cross-Site Scripting	Hacker / Cracker	Datos sin validar	3	ALTO	3	ALTO
			A-011	Inyección por SQL	Hacker / Cracker	Carencia de un saneamiento de entrada adecuado.	3	ALTO	3	ALTO
	ACT009	SERV_DOMINIO	A-018	Ataques DNS basados en botnets	Hacker / Cracker	Ordenadores conectados posiblemente infectados	3	ALTO	2	MEDIO
			A-019	Password Spaying/	Hacker / Cracker	Contraseñas de acceso al servicio de Active Directory comúnes entre los usuarios	3	ALTO	2	MEDIO
	ACT010	SERV_FTP	A-020	Manipulación de archivos compartidos	Hacker / Cracker	Carece de encriptación y autenticación	3	ALTO	2	MEDIO
			A-021	Malware	Hacker / Cracker	Desactualización de parches de seguridad	3	ALTO	2	MEDIO
	ACT011	SERV_DIGITALIZACION	A-004	Inundación	Natural	Carencia de medidas preventivas	2	MEDIO	3	ALTO
	ACT012	SERV_KERIO	A-021	Malware	Hacker / Cracker	Uso de VPN por funcionarios desde sus hogares con máquinas vulnerables a malware	3	ALTO	2	MEDIO
	ACT013	SERV_BIOMETRICO	A-033	Filtración de componentes en estado liquido	Material (falla)	Equipo descontinuado (averías)	2	MEDIO	3	ALTO

COMUNICACIONES, REDES.	ACT014	SWITCH CORE HP 5500AF48 G-POE	A-022	Ataque Man in the middle	Hacker / Cracker	Desactualización de firmware / parches de seguridad	3	ALTO	2	MEDIO
			A-003	Polvo	Natural	carencia de fechas fijas para mantenimiento preventivo	3	ALTO	2	MEDIO
	ACT015	SWITCH ACCESS HP 5120AF48 G-POE	A-022	Ataque Man in the middle	Hacker / Cracker	Desactualización de firmware / parches de seguridad	3	ALTO	2	MEDIO
			A-004	Inundación	Natural	Carencia de medidas preventivas	2	MEDIO	3	ALTO
	ACT016	SWITCH CISCO CATALYST 2960	A-022	Ataque Man in the middle	Scriptkiddie	Desactualización de firmware / parches de seguridad	3	ALTO	2	MEDIO
			A-004	Inundación	Material (falla)	Carencia de medidas preventivas	2	MEDIO	2	MEDIO
	ACT017	ROUTER CNT ISP	A-035	Fallos operativos	Proveedor	Desactualización de firmware / parches de seguridad	3	ALTO	3	ALTO
			A-004	Inundación	Material (falla)	Carencia de medidas preventivas	3	ALTO	2	MEDIO
	ACT018	ROUTER TELCONET ISP	A-035	Fallos operativos	Proveedor	Desactualización de firmware /parches de seguridad	3	ALTO	3	ALTO
	ACT019	WIRELESS ROUTER HUAWEI	A-036	Intrusos en la red wifi	Scriptkiddie	Protocolos de cifrado descontinuados	3	ALTO	3	ALTO
HARDWARE Y APLICACIONES.	ACT020	CPU DELL CORE I5 OCTAVA GENERACION	A-032	Virus en pc del Coordinador de TIC	Hacker / Cracker	Presencia de virus informático	1	BAJO	2	MEDIO
			A-003	Polvo	Natural	carencia de fechas fijas para mantenimiento preventivo	2	MEDIO	2	MEDIO
	ACT021	CPU HP CORE I7 SEPTIMA GENERACION	A-032	Virus en pc del Administrador de base de datos	Hacker / Cracker	Presencia de virus informático	1	BAJO	2	MEDIO

	ACT022	CPU DELL CORE I7 SEPTIMA GENERACION	A-032	Virus en pc del Jefe de Infraestructura	Hacker / Cracker	Presencia de virus informático	1	BAJO	2	MEDIO
			A-003	Polvo	Natural	Carencia de fechas fijas para mantenimiento preventivo	2	MEDIO	2	MEDIO
	ACT023	CPU DELL CORE I7 SEPTIMA GENERACION	A-032	Virus en pc del Desarrollador	Hacker / Cracker	Presencia de virus informático	1	BAJO	2	MEDIO
			A-003	Polvo	Natural	carencia de fechas fijas para mantenimiento preventivo	2	MEDIO	2	MEDIO
	ACT024	CPU DELL CORE I5 SEPTIMA GENERACION	A-032	Virus en pc del Desarrollador Junior	Falta de financiamiento	Discos defectuosos	1	BAJO	2	MEDIO
			A-003	Polvo	Natural	carencia de fechas fijas para mantenimiento preventivo	2	MEDIO	2	MEDIO
	ACT025	CENTRAL TELEFONICA IP PANASONIC HIBRIDA KX-NS500	A-004	Inundación	Material (falla)	Carencia de medidas preventivas	2	MEDIO	3	ALTO
			A-003	Polvo	Natural	carencia de fechas fijas para mantenimiento preventivo	2	MEDIO	2	MEDIO
	ACT026	IMPRESORA HP PAGEWIDE PRO 477	A-004	Inundación	Natural	Carencia de medidas preventivas	2	MEDIO	3	ALTO
EQUIPAMIENTO AUXILIAR	ACT027	UPS COMPUTER PONER 3KVA	A-030	Periféricos o Componentes defectuosos	Material (falla)	UPS descontinuado	3	ALTO	2	MEDIO
	ACT028	NVR HIKVISION	A-037	Carencia de equipos de videovigilancia	Falta de financiamiento	Puntos Ciegos (sin monitoreo)	3	ALTO	3	ALTO
			A-038	Fallos en cámaras de videogilancia	Falta de financiamiento	Indisponibilidad del sistema por periodo de inactividad	3	ALTO	3	ALTO
	ACT029	Cableado	A-028	Errores en la organización	Empleado sin experiencia	Interrupciones constantes / ruido	3	ALTO	2	MEDIO

			A-014	Acceso no autorizado	Personal sin experiencia	Deficiente o nulo etiquetado del cable	2	MEDIO	2	MEDIO
	ACT030	Aire Acondicionado	A-003	Polvo	Natural	Carencia de fechas fijas para mantenimiento preventivo	2	MEDIO	3	ALTO
			A-004	Inundación	Natural	Carencia de medidas preventivas	2	MEDIO	3	ALTO
Soportes de Información	ACT031	Discos Duros Externos.	A-024	Sabotaje	Personal Descontento	Carencia de fechas fijas para mantenimiento preventivo	2	MEDIO	3	ALTO
			A-015	Hurto	Personal Descontento	Libre acceso a discos duros en el área de soporte	2	MEDIO	3	ALTO
	ACT032	Blu-ray Disk	A-024	Sabotaje	Personal Descontento	Carencia de fechas fijas para mantenimiento preventivo	2	MEDIO	3	ALTO
			A-015	Hurto	Personal Descontento	Libre acceso a discos blu-ray en el área de soporte	2	MEDIO	3	ALTO
	ACT033	Memorias USB	A-039	Periféricos o Componentes defectuosos	Material (falla)	Dispositivos con averías físicas	2	MEDIO	2	MEDIO
			A-024	Hurto	Personal Descontento	Libre acceso a dispositivos USB en el área de soporte	2	MEDIO	3	ALTO
	ACT034	Resmas de papel impresas.	A-005	Incendio	Personal / falla	Documentación sin respaldo en la nube	2	MEDIO	3	ALTO
PERSONAL	ACT035	TALENTO HUMANO	A-007	Epidemias	Personal	Contagios COVID-19	3	ALTO	2	MEDIO
			A-025	Phishing	Hacker / Cracker	Falta de capacitación sobre ciberseguridad	3	ALTO	3	ALTO
			A-026	Ingeniería social	Hacker / Cracker	Falta de capacitación sobre ciberseguridad	3	ALTO	3	ALTO

Tabla 7: Cálculo de la probabilidad de ocurrencia

3.3.4 Criterio del nivel de Riesgo

Del resultado de la probabilidad de ocurrencia de una amenaza, la probabilidad de ocurrencia de vulnerabilidades y el valor del impacto del activo de la información (CID), se obtiene el nivel de riesgo sobre cada activo de información. Calculado mediante la siguiente forma:

Nivel de riesgo = Valor del Activo (CID) * Nivel de amenaza * Nivel de vulnerabilidad

Imagen 1 : Valoración del nivel de riesgo. [30]

Para todo este proceso resultó necesario realizar la matriz de evaluación de riesgo medido por la probabilidad vs impacto (Ver Anexo 5) . Producto de esta evaluación, se determinó que las principales amenazas que provocan un riesgo alto (>=18) sobre varios activos de información, son:

AMENAZAS DE RIESGO ALTO		
No. referencia amenaza	AMENAZA	CÁLCULO NR
A-008	Acceso de terceros a los servidores	ALTO
A-002	Sismo	ALTO
A-005	Incendio	ALTO
A-026	Ingeniería social	ALTO
A-029	Sobrecargas y cortes de energía eléctrica	ALTO
A-034	Infección de sistema	ALTO
A-030	Variaciones de voltaje	ALTO
A-009	Denegación de Servicio DDOS	ALTO
A-011	Inyección por SQL	ALTO
A-013	Format string bugs	ALTO

A-016	Fuga de datos	ALTO
A-017	Ataque Cross-Site Scripting	ALTO
A-018	Ataques DNS basados en botnets	ALTO
A-019	Password Spaying/	ALTO
A-021	Malware	ALTO
A-035	Fallos operativos	ALTO
A-036	Intrusos en la red wifi	ALTO
A-038	Fallos en cámaras de videovigilancia	ALTO
A-037	Carencia de equipos de videovigilancia	ALTO
A-025	Phishing	ALTO

Tabla 8: Identificación de riesgo alto. Elaboración Propia

Las principales amenazas que provocan un riesgo medio (>=9 y <= 17) sobre los activos de información, son:

AMENAZAS DE RIESGO MEDIO		
No. referencia amenaza	Amenaza	Cálculo NR
A-004	Inundación	MEDIO
A-007	Epidemias	MEDIO
A-024	Hurto	MEDIO
A-039	Periféricos o Componentes defectuosos	MEDIO
A-027	Acceso no autorizado	MEDIO
A-020	Manipulación de archivos compartidos	MEDIO
A-033	Filtración de componentes en estado liquido	MEDIO
A-028	Errores en la organización	MEDIO
A-15	sabotaje	MEDIO
A-022	Ataque Man in the middle	MEDIO

Tabla 9 : Identificación de riesgo medio. Elaboración Propia.

Las principales amenazas que provocan un nivel de riesgo bajo (<=8) sobre los activos de información, son:

AMENAZAS DE RIESGO BAJO		
No. referencia amenaza	Amenaza	Cálculo Nivel Riesgo
A-003	Polvo	MEDIO

A-032	Virus en pc del Coordinador de TIC	BAJO
A-032	Virus en pc del Administrador de base de datos	BAJO
A-032	Virus en pc del jefe de Infraestructura	BAJO
A-032	Virus en pc del Desarrollador	BAJO
A-032	Virus en pc del Desarrollador Junior	BAJO

Tabla 10: Identificación de amenazas de riesgo baja. Elaboración Propia.

3.3.5 Estadísticas de los resultados del cálculo del nivel de riesgo

A continuación, se muestra un gráfico estadístico de los 37 riesgos evaluados, evidenciando que existe un 54% de riesgos considerados como alto, un 32% de riesgo medio, dejando apenas un 14% de riesgo considerado como bajo.

ALTO	20
MEDIO	11
BAJO	6
TOTAL	37

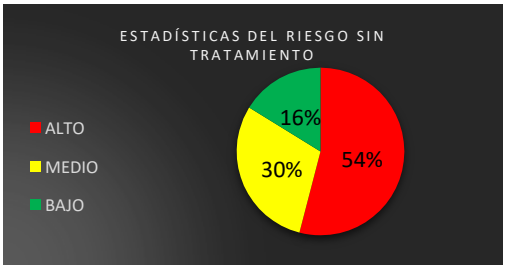


Figura 8: Resultados del nivel de riesgo. Elaboración propia.

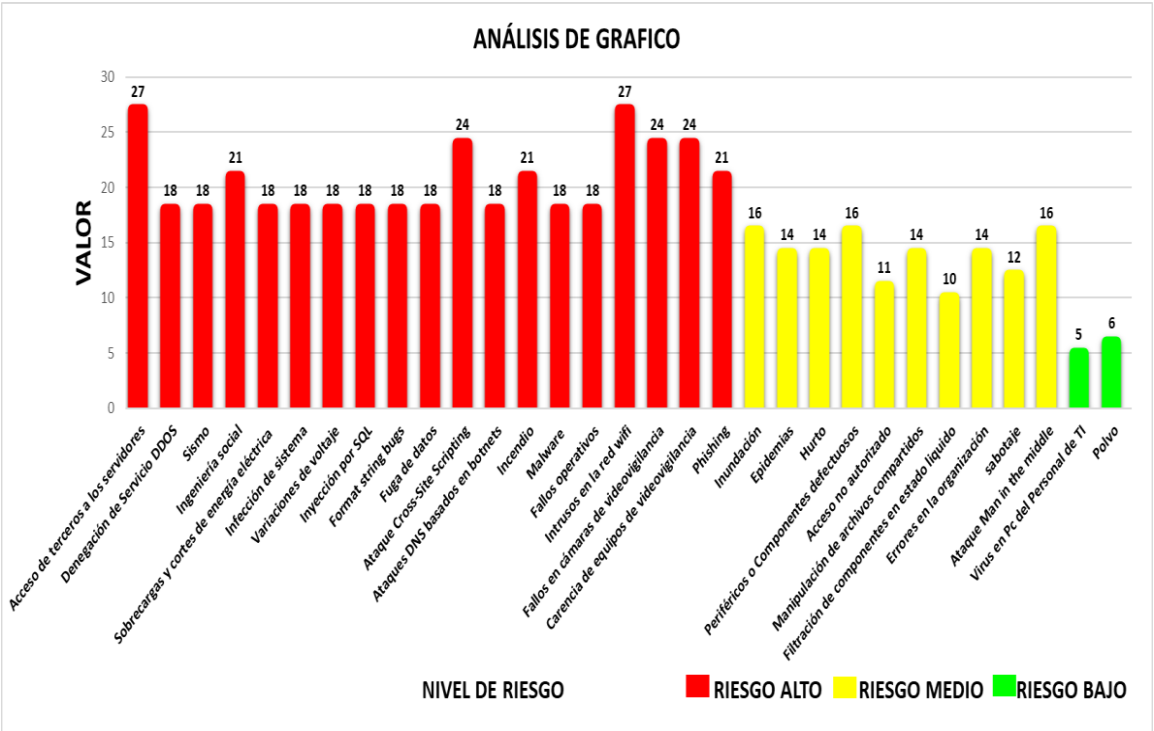


Figura 9: Gráfico estadístico de niveles de riesgo según su clasificación. Elaboración propia.

3.3.6 Análisis del costo por pérdidas de activos de información.

En cuanto a valores monetarios se puede estimar los siguientes costos por posibles afectaciones a los activos de información:

Problema	Valor	Descripción	Costo
Daños en los servidores	$4.899,00	Existen 3 servidores HP PROLIANT DL380 GEN 9 en el centro de datos.	$ 14.697,00
Daño de Switches backbone.	$ 870,00	Se tienen actualmente 3 switches HPE 5500-48G-PoE administrables de 48 puertos dentro del centro de datos.	$ 2.610,00
Daños switches áreas de trabajo.	$ 385,00	Existen 10 switches para el uso de las comunicaciones de los departamentos de la empresa.	$ 3.850,00
Daños del rack del centro de datos.	$ 370.00	Existen 2 racks que permiten alojar equipamiento informático y de comunicaciones.	$ 740,00
Afectaciones del cableado al centro de datos.	$ 25,00	De cada piso se cablea al centro de datos, son 7 pisos por $25 cada punto.	$ 175,00
Afectaciones del cableado para las áreas de trabajo	$ 25,00	Son 250 puntos a $25.	$ 6.250,00
Pérdidas de Documentos, Manuales, licencias de Software, Documentos de Consultorías.	$ 20.000,00	Se estima conforme a la documentación que podría perderse debido a una contingencia.	$ 20.000,00
Pérdida de los códigos fuentes y ejecutables de los sistemas de información	$ 60.000,00	Se estima conforme a la pérdida de código fuente de sistemas utilizados por el personal administrativo.	$ 60.000,00
Pérdida de Datos	$ 5,00	Por un día de trabajo de 8 horas de 250 personas,	$ 10.000,00
Pérdida de los respaldos de datos	$ 12.000,00	Si se perdiera la información de un año comercial 360 días equivaldría a este costo.	$ 4.320.000,00
TOTAL			$ 4.438.322,00

Tabla 11: Costo por pérdidas o daños en activos de información

Debido a que los niveles de riesgo alto y medio superan a los riesgos de nivel bajo y el cálculo en cuanto a perdidas monetarias es alto, resulta necesario realizar un tratamiento oportuno de los riesgos para disminuir el nivel de criticidad mediante un plan de contingencia que contenga una serie de directrices, lineamientos, y controles para contribuir en la continuidad de las operaciones de la empresa.

3.3.7 Responsabilidad y tiempo de ejecución

Dentro de este punto se desglosan las etapas, el seguimiento de las políticas, y el recurso humano involucrado quienes ejecutarán los procesos en el tiempo que se determine para cada una de las fases a cumplir bajo la dirección de los directivos del departamento de coordinación de TI de la empresa.

PLAN DE EJECUCIÓN				
Fase	**Política**	**Recurso Humano**	**Ejecución**	**Tiempo**
Redacción	Planificación y documentación de salvaguardas y políticas de seguridad.	Comité de seguridad Informática	Coordinador de Tecnologías de la Información, jefe de infraestructura, jefe de desarrollo y base de datos, representantes legales de la empresa.	25 días
Revisión	Evaluación Independiente de las salvaguardas y política.	Comité de evaluación de políticas de seguridad	Jefe coordinador de Tics, jefe de redes y seguridades, auditor informático externo.	7 días
Aprobación	Obtener aprobación de las salvaguardas y política.	Jefe de Coordinación de tics y gerente de la empresa AGUPEN EP	Gerente de la empresa, jefe coordinador de Tics.	5 días
Comunicación	Difundir salvaguardas y políticas.	Oficial de seguridad Informática	Departamento de Tecnologías de la información.	3 días
Cumplimiento	Ejecutar salvaguardas preventivas y hacer cumplir las políticas.	Jefe de Coordinación de tics	Todo el personal de la institución	Diariamente.
Monitoreo	Seguimiento y reportes en bitácoras	Auditor Informático	Auditor Informático y jefe de seguridad.	3 días
Actualización	Revisiones periódicas	Comité de seguridad Informática.	Coordinación de Tics, deptos. Encargados.	Anual.

Tabla 12: Plan de ejecución de política de seguridad.

4. CAPITULO IV

4.1 PLAN DE CONTINGENCIAS INFORMÁTICO DEL CENTRO DE DATOS DE LA EMPRESA “AGUAPEN EP”

PLAN DE CONTINGENCIAS INFORMÁTICO PARA EL CENTRO DE DATOS Y COMUNICACIONES DE LA EMPRESA “AGUAPEN-EP”

Aguapen-EP

4.1.1 Introducción

Toda organización debe planificar y desarrollar un Plan de Contingencia cuando todavía no es necesario, es decir, antes de que ocurra una emergencia. Gracias a la planificación se aumenta la habilidad y capacidad de la empresa para mantener la continuidad de sus operaciones en caso de un incidente, proporcionando una serie de acciones que se deben realizar para una adecuada respuesta al riesgo.

El Plan de Contingencia debe tener en cuenta al personal que participa en su Implementación y aquellos que participarán operativamente en el momento en que se presente el incidente. Este debe detallar los roles de los encargados de la contingencia y sus responsabilidades.

La protección de la información y la continuidad de las operaciones en caso de una situación de emergencia es una de las principales estrategias que deben llevarse a cabo, ya sea en empresas públicas o privadas debido a que de ello depende el cese de los servicios brindados en la empresa especialmente ante eventos inesperados como desastres naturales, errores u omisiones o fallos en la tecnología.

El presente documento consta de lineamientos, obligaciones, controles y salvaguardas esenciales para permitir la continuidad de las operaciones ante contingencias que se presenten en el centro de datos del área de coordinación de Tecnologías de la Información de la empresa AGUAPEN EP.

4.1.2 Alcance del plan

El presente plan de contingencia establece los lineamientos para poder actuar en eventos de emergencia que se presenten en el centro de datos del departamento de coordinación de TI de la empresa AGUAPEN EP, debido a amenazas físicas, lógicas y del entorno que ocasionen riesgos que atenten contra la seguridad de la información.

4.1.3 Objetivos del plan

4.1.3.1 Objetivo General

Definir un conjunto de responsabilidades, roles y controles para la ejecución de procedimientos técnicos durante situaciones de emergencia.

4.1.3.2 Objetivos Específicos

- Detallar especificaciones generales del plan de contingencias.
- Establecer controles, procedimientos o acciones a tomar frente a una contingencia.
- Delegar roles y responsabilidades para el equipo encargado del cumplimiento del plan.

4.1.4 Condiciones generales

Es responsabilidad principal del jefe del departamento de Coordinación de TI:

- Difundir los procesos y procedimientos del plan de contingencia.
- Capacitar al personal sobre el plan de contingencia.
- Verificar el cumplimiento de salvaguardas.
- Realizar el llenado del cronograma de revisión de cumplimiento de salvaguardas preventivas. (Ver Anexo 8)

El departamento de coordinación de TI, debe aplicar las políticas y procedimientos de seguridad de la información establecidas para la correcta gestión de la información almacenada, generada y procesada dentro de la empresa.

Los directivos encargados del plan de contingencia deben hacer cumplir las políticas establecidas con el ánimo de ejecutar un correcto uso de las tecnologías de información.

El equipo encargado de la ejecución del plan de contingencia debe realizar una revisión y actualización del plan cada año para verificar si resulta necesario una modificación por cambios o adquisiciones informáticas.

Es obligación del equipo de trabajo llevar el control del registro de todo lo ejecutado o actuado concerniente a anomalías o emergencias suscitadas en donde resulto necesario el uso del plan de contingencia para la toma de decisiones en mejoras futuras del plan. (Ver Anexo 9)

4.1.5 Estructura organizacional ante contingencia

Resulta adecuado ejecutar la siguiente estructura organizacional que incluya roles y responsabilidades apropiados al personal del área de coordinación de Tecnologías de Información para la correcta ejecución del plan de contingencia ante incidentes.

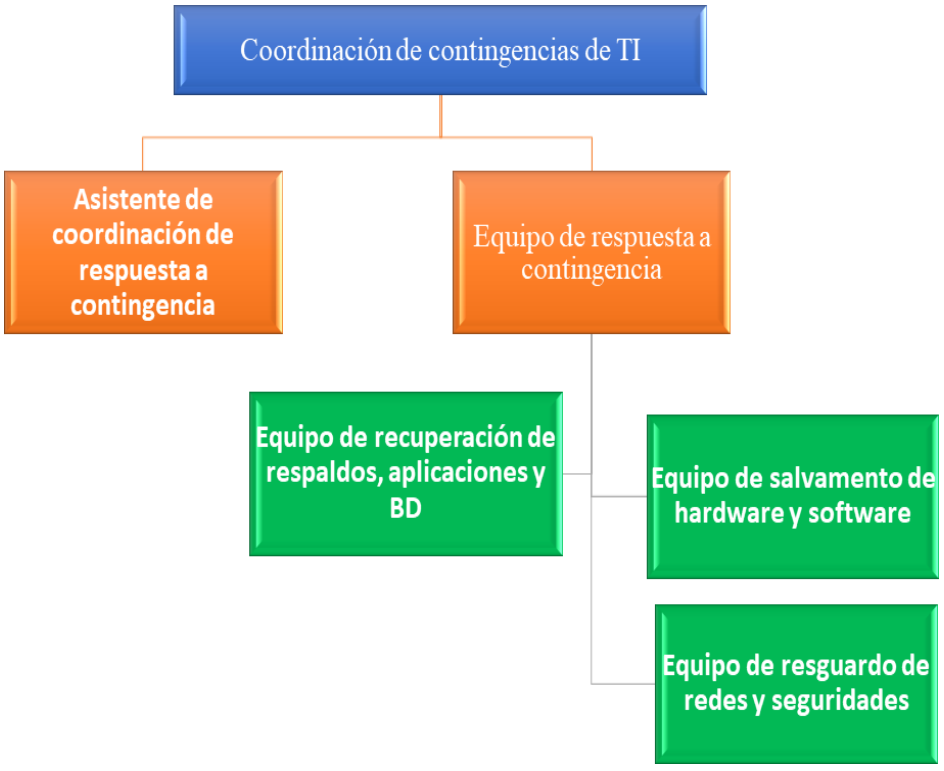


Figura 1010: Estructura organizacional para ejecución del plan contingencia.

4.1.6 Información de contacto del equipo encargado de la ejecución del Plan decontingencia.

Cuando ocurre un evento de emergencia, es necesario notificar de manera oportuna a los miembros responsables, por tal razón como se muestra en la tabla el correo electrónico de los encargados del cumplimiento del plan.

Estructura Organizativa	Teléfono	Contacto
Coordinador de recuperación de TI	09	adrianB@aguapen.gob.ec
Asistente de coordinación de respuesta a emergencia	09	kettyR@aguapen.gob.ec
Equipo de recuperación de respaldos, aplicaciones y BD	09	luisG@aguapen.gob.ec
Equipo de salvamento de hardware y software.	09	williamR@aguapen.gob.ec
Equipo de resguardo de redes y seguridades	09	angelT@aguapen.gob.ec

Tabla 13: Contacto de equipo encargado de aplicación del plan de contingencia.

4.2 Roles y Responsabilidades

4.2.1 Coordinador de contingencias de TI

La coordinación de aplicación de los procedimientos y controles es compromiso del jefe del departamento de coordinación de tecnologías de la información, quien tendrá como responsabilidad hacer cumplir todas las acciones y salvaguardas a seguir ante un suceso de emergencia de acuerdo con el plan de contingencia.

Entre sus responsabilidades se encuentra:

- Administrar y guiar al personal de Coordinación de recuperación de TI bajo escenarios de contingencias.
- Implementar controles para salvaguardas la confidencialidad, integridad y disponibilidad de los datos e información.
- Supervisar el cumplimiento de los controles y procedimientos establecidos en el plan de contingencia.
- Informar a la alta gerencia de la empresa acerca alguna eventualidad durante la ejecución del plan.
- Corroborar que el cronograma establecido se cumpla en la cantidad de días establecidos.
- Coordinar la realización del proceso de respaldo de la información en el centro de datos alterno.
- Liderar la gestión tecnológica de manera activa y segura.
- Determinar las necesidades y prioridades a alta gerencia y al personal para el proceso de recuperación.
- Comunicar la efectividad de los controles establecidos y ejecutados durante la emergencia.
- Cumplir y hacer cumplir las políticas e instrucciones concernientes con la seguridad de la información.

4.2.3 Asistente de coordinación de respuesta a contingencia

- Apoyar al jefe coordinador de Tics en la divulgación de procedimientos e información.
- Coordinar acciones a realizar.
- Llevar el control del inventario de activos de información.

4.2.4 Equipo de recuperación de respaldos, aplicaciones y BD

- Verificar los procedimientos que se emplean para almacenar y recuperar los datos (proceso de backup).
- Revisar que no exista alguna modificación en algún componente de software y aplicaciones que impliquen daños a la integridad de los datos.

4.2.5 Equipo de salvamento de hardware y software

- Identificar los diferentes activos de información hardware o software que hayan sido dañados por una contingencia.
- Coordinar el cumplimiento de los contratos de mantenimiento, garantía y soporte con los proveedores.
- Instalar, configurar y ajustar todo el software que haya sido dañado por una contingencia.
- Comprobar el correcto funcionamiento del equipamiento de hardware que hayan sido restaurados o reemplazados.

4.2.6 Equipo de resguardo de redes y seguridades

- Identificar los elementos de comunicaciones que han obtenido dañados por la contingencia e detectar problemas de conectividad dentro del centro de datos.
- Coordinar reparaciones o cambios de las afectaciones a las comunicaciones para que los usuarios puedan seguir utilizando los servicios.
- verificar el acceso a los recursos del centro de datos por parte del personal administrativo de la empresa.

4.3 Ejecución de salvaguardas.

4.3.1 Salvaguardas preventivas ante contingencia.

RIESGO	SALVAGUARDAS
Incendio	Identificar y señalar adecuadamente las rutas de evacuación.
	Instalación de sistemas de alarmas contra incendio.
	Instalación de extintores o rociadores contra incendios.
	Capacitar al personal de Tecnologías de la información sobre el uso correcto de extintores.
	Adquirir un seguro contra incendios.
	Identificar documentación importante y trasladarlas cajas de seguridad para cintotecas, digitalizarlos y contratar servicios de alojamiento de archivos en la nube.
	Establecer un listado de contactos telefónicos de emergencia que incluya al cuerpo de bomberos y ambulancias.
Inundación	Adquirir bolsas de plástico para cubrir equipos informáticos.
	Realizar simulacros de inundaciones mínimo 2 veces por año.
	Verificar que las instalaciones eléctricas se mantengan a la altura adecuada para prevenir cortocircuitos provocados por agua.
	Implementar techo impermeable, para evitar daños por lluvias prolongadas.
	Implementar un sistema de drenaje adecuado para el área de coordinación de TI.
	Identificar lugares susceptibles a inundaciones y gestionar las medidas de seguridad necesarias.
	Planificar proceso de backup diario en instalaciones externas (sede secundaria).
Sismo	Contratar personal para reparar fisuras y grietas existentes en el cuarto de servidores.
	Fijar al piso o paredes equipamiento de hardware de gran tamaño y peso para evitar colapsos sobre el personal de TI.
	Contar con equipos de protección adecuados para el personal.

	Asegurar que las rutas de evacuación estén libres de obstáculos para desalojar de manera oportuna el departamento de TI.
	Capacitar al personal sobre primeros auxilios.
Epidemias	Establecer medidas de bioseguridad.
	Planificar teletrabajo obligatorio al personal que labora en la institución si llega a padecer de alguna enfermedad.
	Realizar formato de solicitud para traslado de equipos de trabajo hasta domicilios de personal afectado para cumplir con sus obligaciones desde el hogar.
Sobrecargas y cortes de energía eléctrica	Verificar el estado de UPS, brindar mantenimiento adecuado y que las características sean adecuadas para soportar una operación continua de 10 minutos mínimo.
	Realizar pruebas periódicas del correcto funcionamiento de los reguladores de voltaje.
	Contar con una planta secundaria que suministre energía para este tipo de eventualidades.
	Ejecución de procesos de respaldos de la información.
Acceso no autorizado al Data Center	Precautelar que se realice un proceso de identificación para los visitantes del área de TI y el centro de Datos,
	Videovigilancia del acceso al cuarto de comunicaciones las 24h del día.
	Brindar al personal de Tecnologías de la información tarjetas de Identificación tipo colgantes para su identificación.
Intrusión en la red	Realizar procesos de monitoreo del tráfico de red.
	Mantener los diagramas de red de la institución formalizados y actualizados.
	Supervisar los hosts activos en la red a fin de encontrar posibles conexiones ocultas.
	Verificar el correcto funcionamiento de las tarjetas de red y dispositivos de comunicaciones como switch, router, Access point.
	Centralizar y monitorear redes Alámbricas e Inalámbricas.

	Adquirir equipos con cifrado WPA3.
	Realizar mantenimiento punto a punto de la red, para evitar problemas de transmisión y saturación del canal.
Ataques cibernéticos.	Implementar zonas desmilitarizadas.
	Monitorear los logs almacenados en los servidores.
	Monitorear constantemente el acceso mediante puertos en los servidores.
	Adquisición de firewall físico, establecer listas negras y restringir el acceso a paginas sin protocolos https.
	Adquirir licencias antivirus de al menos 2 proveedores distintos.
	Gestionar contraseñas de acceso robustas.
	Realizar cambio de contraseña como mínimo cada mes.
	Limitar la posibilidad de instalación de software de terceros.
	Programar horarios para actualizar software, versiones de sistemas operativos, pluggins e instalar los últimos parches de seguridad.
	Brindar el respectivo proceso de verificación libre de virus sobre dispositivos flash o discos duros externos.
Fallos en los sistemas informáticos	Solicitar una auditoría de sistemas y bases de datos.
	Solicitar la realización de un proceso de Hacking ético a sistemas informáticos.
Robo de Información	Implementar en un lugar, copias de seguridad de los documentos, sistemas, respaldos de la institución.
	Incrementar cámaras de vigilancia interiores y exteriores para la dirección de TIC’s
	Hacer uso de sistemas y procesos de encriptado de mensajes, para asegurar la protección y privacidad de toda esa información.
	Comprobar siempre la autenticidad de enlaces recibidos e identificar a los emisores de los mismos para no ser víctima de phishing.
	Restringir limite aforo de personal dentro del área de Tics.
	Registrar la salida de equipos previa autorización del jefe coordinador de TI.

	Prohibir facilitar información del personal o información confidencial de la institución.
	Definir la documentación para permitir la destrucción de discos duros obsoletos que almacenen información confidencial.

4.3.2 Salvaguardas durante la contingencia

RIESGO	SALVAGUARDAS
Incendio	Seguir las rutas de evacuación (salidas de emergencia).
	Desalojar el centro de cómputo.
	Si es posible apagar inmediatamente los servidores
	Activación del sistema de alarmas contra incendios en caso de presentarse una emergencia de humo o fuego.
	Activación de rociadores contra incendios automáticos.
	Hacer uso del drenaje del depto. de TI.
	Dirigirse a lugares susceptibles a inundaciones y gestionar las medidas de seguridad necesarias.
Sismo	Dirigirse a las zonas de escape o emergencia
	Colocarse equipos de protección y llevar el botiquín de primeros auxilios.
	Seguir rutas de evacuación y emergencia.
	Si es posible aplicar primeros auxilios.
Epidemias	Uso de mascarillas y guantes de latex, alcohol o gel antiséptico.
	Permitir la facultad de realizar teletrabajo al personal.
	Trasladar equipos de trabajo pc, impresora, hasta el domicilio de los afectados para cumplir con sus obligaciones desde el hogar.
Sobrecargas y cortes de energía eléctrica	Hacer uso de los UPS que soportan una operación continua de 15 minutos para apagar los equipos del centro de datos para evitar daños.
	Puesta en marcha de la Planta energética de emergencia.
Acceso no autorizado al Data Center	Comunicar al personal encargado de la seguridad de la empresa por personal que accedió sin autorización al centro de datos.
	Videovigilancia del acceso al cuarto de comunicaciones las 24h del día.
	Otorgar tarjetas de identificación al personal de Tecnologías de la información.
	Dar de baja a hosts de origen desconocido que están ejecutándose en segundo plano dentro de la red.

Intrusión en la red	Anunciar la contingencia hasta verificar el estado de la red corporativa.
	Monitorear el tráfico entrante y saliente mediante un análisis de red identificando host que no procedan de la empresa.
Ataques cibernéticos.	Dar de baja puertos abiertos en los servidores para terminar conexiones de terceros.
	Contratar servicios de Hacker Ético certificado para manejar el ataque en conjunto con el administrador de redes y seguridades de la institución.
	Buscar el origen del ataque, obtener dirección Ip y su ubicación para informar a las autoridades competentes.
	Revisión de registros almacenados en firewall del acceso a sitios inseguros y descargas realizadas por personal administrativo.
	Realizar un análisis completo para identificar el agente causante de la amenaza o intento de sabotaje.
	Desconectar el origen de la intrusión de la red de la institución.
	Desconectar toda la infraestructura de red.
Robo de Información	Reportar el robo al jefe coordinador del departamento de TI.
	Revisión de cámaras de videovigilancia ubicadas en los interiores y exteriores del departamento de coordinación de TI.

4.3.3 Salvaguardas después de la contingencia

RIESGO	SALVAGUARDAS
Incendio	El jefe coordinador de TI deberá dar cabida a el análisis de daños, afectaciones en la infraestructura para comunicarse con el gerente general y determinar si es posible o no continuar utilizando las instalaciones
	Verificación de la reparación o reemplazo de los componentes dañados.
	En caso de haber personal afectado físicamente con lesiones graves o leves que no pueda realizar sus labores se debe enviar inmediatamente a urgencias y guardar reposo.
Inundación	Verificar documentos, archivos, equipos informáticos afectados por la inundación.
	Dirigirse a lugares despejados y seguros, haciendo uso de medidas de seguridad.
Sismo	Revisar daños coaccionados en la infraestructura física, lógica para verificar si es el departamento esta apto para reanudar las operaciones, en caso contrario operar en la sede secundaria.
	Efectuar la evaluación de pérdidas de equipos informáticos y presentarlas al jefe coordinador de TI.
	Verificar el estado actual de los servidores, racks y bastidores y emitir un informe por migración de los servicios.
	Restablecer respaldos en caso de ser necesario.
Epidemias	Conocer el estado de recuperación del personal en teletrabajo para coordinar su regreso en su área de trabajo.
	Coordinar el retorno de equipos de trabajo pc, impresora, entregadas por teletrabajo.
Sobrecargas y cortes de energía eléctrica	Evaluar los daños de los equipos por posibles daños eléctricos.
	Dar a conocer a los usuarios sobre el restablecimiento de los servicios.
	Reestablecer los servicios en caso de no haberse presentado daños a la infraestructura.

Acceso no autorizado al Data Center	Verificar cualquier intento de daño o sabotaje por el personal que accedió sin autorización.
	Generar un informe sobre el estado actual del Data center.
	Generar un informe de la grabación guardada en los dispositivos de videovigilancia.
Intrusión en la red	Dar de baja a hosts de origen desconocido que están ejecutándose en segundo plano dentro de la red.
	Definir reglas de bloqueo en el firewall para host de origen desconocido.
Ataques cibernéticos.	Identificar las fallas de seguridad que utilizaron terceros para efectuar el ataque y aplicar los correctivos.
	Reforzar áreas de vulnerabilidad en la seguridad perimetral.
	Generar un informe de afectaciones realizadas a nivel lógico de la infraestructura.
	Llevar a cabo una auditoría de sistemas y bases de datos para identificar agujeros de vulnerabilidad.
	Realizar un Hacking ético a sistemas informáticos para verificar el nivel de seguridad.
Fallos en los sistemas informáticos	Comunicar resultados del proceso de auditoría de sistemas y base de datos para coordinar las respectivas correcciones a agujeros de seguridad.
	Comunicar resultados del proceso de hacking ético para proceder a reforzar los niveles de seguridad.
Robo de Información	Presentar un informe de documentación, dispositivos de almacenamiento e inventario de activos faltantes en el departamento de TI.
	Generar un informe luego de la revisión de cámaras de videovigilancia interiores y exteriores del departamento de coordinación de TI.
	Generar un informe sobre la información robada que se almacenaba en los servidores de base de datos si llego a suceder.

4.4 Selección de controles

A continuación, se detalla los controles asignados para los tipos de amenazas

Clasificación	Descripción de la amenaza	Controles ISO 27002	Controles Sans Security
Causados por la naturaleza	Sismo	11.1.4 Protección contra las amenazas externas y ambientales.	Adquisición de Póliza de seguros. Centro de cómputo externo.
	Inundación	A.12.3.1 Respaldo de la información	Respaldos en centro de cómputo externo.
	Incendio	11.1.5 El trabajo en áreas seguras.	Instalar un sistema de extinción automática de fuegos/humos.
	Polvo	11.2.4 Mantenimiento de los equipos. 11.2.1 Emplazamiento y protección de equipos.	Realizar mantenimiento preventivo a equipos e infraestructura.
	Epidemias	6.2.2 Teletrabajo. 6.2 Dispositivos para movilidad y teletrabajo.	Permitir al personal realizar su jornada laboral desde su hogar.
Causados por humanos	Acceso de terceros a los servidores.	11.1.3 Seguridad de oficinas, despachos y recursos.	Cámaras de seguridad en el interior del centro de Datos.
	Acceso no autorizado al Data Center	11.1.2 Controles físicos de entrada.	Establecer control de acceso biométrico al centro de datos.
	Intrusos en la red wifi	14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.	Actualización de firmware y parches de seguridad. Cambio de equipos y tecnologías inalámbricas con cifrado WPA2 por WPA3.
	Infección del sistema	12.7.1 Controles de auditoría de sistemas. 13.1.2 Mecanismos de seguridad asociados a servicios en red.	Auditoria de aplicaciones y bases de datos.

	Ingeniería social, malware, Phishing, Inyección por SQL, Denegación de Servicio DDOS, Format string bugs.	7.2.2 Concienciación, educación y capacitación en seguridad de la información 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas. 9.1.2 Control de acceso a las redes y servicios asociados.	Capacitación del personal administrativo sobre seguridad informática, malware, Phishing, Inyecciones SQL.
	Fuga de datos, Ataque Cross-Site Scripting, Ataques DNS basados en botnets	13.1.2 Mecanismos de seguridad asociados a servicios en red. 14.2.5 Uso de principios de ingeniería en protección de sistemas. 9.4.1 Restricción del acceso a la información.	Monitoreo de cambios en las configuraciones de la red.
	Password Spaying	9.4.2 Procedimientos seguros de inicio de sesión. 9.4.3 Gestión de contraseñas de usuario.	Gestión de contraseñas de usuario.
	Ataque Man in the middle, Sabotaje.	10.1.1 Política de uso de los controles criptográficos. 10.1.2 Gestión de claves. 13.1.3 Segregación de redes.	Segmentación de red y servicios VPN
	Manipulación de archivos compartidos, hurto	13.2.1 Políticas y procedimientos de intercambio de información. 13.2.2 Acuerdos de intercambio. 13.2.4 Acuerdos de confidencialidad y secreto.	Uso de niveles de acceso a archivos compartidos.
Causados por errores u omisiones	Errores en la organización del cableado	11.2.3 Seguridad del cableado.	Verificar el cumplimiento de normativas de cableado estructurado.

	Sobrecargas y cortes de energía eléctrica	15.2.1 Supervisión de servicios prestados por terceros.	Adquisición de generadores eléctricos de emergencia para planta.
	Variaciones de voltaje	12.1.1 Documentación de procedimientos de operación	Uso de UPS y reguladores de voltaje.
	Virus en computadoras	12.2.1 Controles contra el código malicioso.	Adquisición de licencias Antivirus.
	Filtración de componentes en estado liquido	11.2.4 Mantenimiento de los equipos.	Política de no ingreso de componentes líquidos al centro de datos.
Causados por fallas de la tecnología	fallos operativos	12.1.2 Gestión de cambios, actualizaciones.	Mantenimiento preventivo de los equipos de cómputo e infraestructura tecnológica cada semana.
	Carencia de equipos de videovigilancia	15.1.3 Cadena de suministro de tecnologías de la información.	Adquisición de componentes o dispositivos electrónicos de vigilancia.
	Fallos en cámaras de videovigilancia	11.2.2 Instalaciones de suministro. 11.2.4 Mantenimiento de los equipos.	Adquisición y reemplazo de equipos de videovigilancia.
	Periféricos o Componentes defectuosos	8.3 Manejo de los soportes de almacenamiento. 8.3.1 Gestión de soportes extraíbles.	Cambio de dispositivos manejo de dispositivos flash de respaldo.

Tabla 14: Controles establecidos con el uso de normas internacionales

4.4.1 Inversión por plan de contingencia.

4.4.2 Factibilidad Económica

En el caso de la factibilidad económica por recursos tecnológicos es necesario manifestar que el uso de las plantillas del Instituto SANS no tiene costo alguno y solo se tendría que optar por la adquisición de los controles establecidos en la norma ISO/IEC 27002.

Categoría	Descripción	Costo	Cantidad	Total
Recursos Tecnológicos	Norma ISO/IEC 27002:2013	$ 110,78	1	
	SANS Plantillas de políticas de seguridad	$ 0	1	
		TOTAL		$ 110,78

Tabla 15: Costo de Políticas implementadas

En el caso de recursos y materiales se opta por establecer la cantidad de meses en donde resulto necesaria su adquisición.

Categoría	Descripción	Costo	Mes	Total
Recursos y Materiales	Materiales y Suministros	$ 100,00	2	
		TOTAL		$ 200,00

Tabla 16: Costos recursos y materiales

En cuanto a valores para el talento humano no se ha considerado la contratación del personal puesto que el recurso humano necesario forma parte del proyecto, a su vez se recalca que el plan de contingencias fue elaborado por el estudiante – tesista y por ende no es necesario el pago de honorarios puesto que es desarrollado como componente practico para la obtención del título universitario y solo se adjunta un valor tentativo.

Categoría	Descripción	Costo	Mes	Total
Recurso Humano	Auditor (Tesista)	$ 1000,00	4	
		TOTAL		$4000

Tabla 17: Costo recurso humano

Categoría	Descripción	Costo	Mes	Total
Servicios Básicos	(Luz, teléfono e internet)	$ 70,00	4	
		TOTAL		$ 280,00

Tabla 18: Costo servicios básicos

Categoría	Descripción	Costo	Mes	Total
Movilización	Transporte	$ 5,00	4	
		TOTAL		$ 20,00

Tabla 19: Costo movilización

Además, se detallan costos de implementación de un centro de datos alterno que se sugiere como una estrategia de respuesta en el plan de contingencias.

Categoría	Descripción	Cantidad	P. Unit.	Total
Implementación de centro de datos externo	Servidores	3	$4.899,00	$ 14.697
	Firewall	1	$ 452	$ 452
	Switches	3	$ 385,00	$ 1.155
	Racks	2	$ 370.0	$ 740
	Varios	1	$ 300	$ 300
		TOTAL		$ 17.344

Tabla 20: Costo de implementación de centro de datos externo

A continuación, se detalla el total de costos de implementación del plan de contingencias.

Descripción	Costos
Recursos Tecnológicos	$ 110,78
Recursos Materiales	$ 200,00
Recurso Humano	$ 4000,00
Servicios Básicos	$ 280,00
Movilización	$ 20,00
Centro de datos externo.	$ 17344,00
TOTAL	$ 21.954,78

Tabla 21: Costos Totales de Implementación

CONCLUSIONES

Mediante el desarrollo del plan de contingencias se logró favorecer al departamento de coordinación de Tecnologías de la información de la empresa AGUAPEN EP, debido a que no se habían establecido procesos, salvaguardas, roles y responsabilidades que facilite actuar de manera eficiente ante posibles emergencias que se presenten en el centro de datos, permitiéndoles tomar acciones preventivas y correctivas para precautelar la continuidad de las operaciones beneficiando indirectamente al personal administrativo.

La incorporación de normas internacionales como las normativas ISO 31000, ISO 27002 y Sans Security Policies, permitieron el desarrollo del plan de contingencias planteando controles para el tratamiento de los riesgos, lo cual destaca a toda institución como un elemento diferenciador sobre otra por el acatamiento y compromiso en la protección de la seguridad de la información.

Gracias al desarrollo del presente proyecto se logró establecer controles y salvaguardas tanto sugeridos como establecidos por la normativa ISO 27002 y dadas por el instituto SANS, para brindar una correcta gestión de la seguridad de la información y salvaguardar la confidencialidad integridad y disponibilidad de los datos.

RECOMENDACIONES

Se debe realizar y evaluar las pruebas necesarias del plan de contingencias informáticas realizado para el departamento de coordinación de TI, con el fin de verificar nivel de cumplimiento del plan y realizar actualizaciones periódicas a políticas internas.

Considerar la certificación de estándares como: ISO, COBIT e ITIL normas para la gobernabilidad, gestión y control del uso de las Tecnologías de la información.

Actualizar constantemente roles y responsabilidades, controles, métricas y procedimientos del plan de contingencias por posibles cambios del personal, en la infraestructura tecnológica y nuevas amenazas que generen riesgos que atenten contra la seguridad de la información.

BIBLIOGRAFÍA

[1] A. T. A. Johnny A . Tamayo Arias, «PLAN DE CONTINGENCIAS INFORMÁTICO,» [En línea]. Available: https://repositorio.unal.edu.co/bitstream/handle/unal/59988/plandecontingenciasinformatico.pdf?sequence=1&isAllowed=y. [Último acceso: 29 Noviembre 2021].

[2] AGUAPEN EP, «SITIO WEB INSTITUCIONAL DE AGUAPEN-INSTITUCION-QUIENES-SOMOS,» 2018. [En línea]. Available: http://www.aguapen.gob.ec/index.php/institucion/quienes-somos. [Último acceso: 29 Noviembre 2021].

[3] ESET SECURITY, «Eset Security Report 2020 - WeLiveSecurity,» 2020. [En línea]. Available: https://www.welivesecurity.com/wp-content/uploads/2020/08/ESET-Security-Report-LATAM_2020.pdf. [Último acceso: 08 Junio 2021].

[4] ISO RISK MANAGEMENT, «Gestión del riesgo ISO 31000:2018(es),» [En línea]. Available: https://www.iso.org/obp/ui#iso:std:iso:31000:ed-2:v1:es. [Último acceso: 04 Julio 2021].

[5] ISO/IEC 27002:2013, «ISO/IEC 2700,» 2005. [En línea]. Available: https://www.iso27000.es/iso27002.html.

[6] SANS, «Plantillas de políticas de seguridad,» [En línea]. Available: https://www.sans.org/information-security-policy/. [Último acceso: 11 Agosto 2021].

[7] UNIVERSIDAD ESTATAL PENINSULA DE SANTA ELENA, «Facsistel,» [En línea]. Available: http://facsistel.upse.edu.ec/. [Último acceso: 17 Junio 2021].

[8] F. Baño y D. Maldonado, «Repositorio institucional UNIANDES,» Diciembre 2013. [En línea]. Available: https://dspace.uniandes.edu.ec/handle/123456789/4522. [Último acceso: 26 Diciembre 2021].

[9] ISOTools Excellence, «La norma en Gestión de Riesgos ISO 31000 y sus beneficios,» 15 Octubre 2017. [En línea]. Available: https://www.isotools.org/2017/10/15/gestion-de-riesgos-iso-31000-y-sus-beneficios/. [Último acceso: 04 Julio 2021].

[10] República del Ecuador, «Plan Creación de oportunidades 2021 - 2025,» 2021. [En línea]. Available: https://www.planificacion.gob.ec/wp-content/uploads/2021/09/Plan-de-Creacio%CC%81n-de-Oportunidades-2021-2025-Aprobado.pdf. [Último acceso: 15 Noviembre 2021].

[11] AGUAPEN EP, «SITIO WEB INSTITUCIONAL DE AGUAPEN-INSTITUCION-MISION-VISION,» 2018. [En línea]. Available: http://www.aguapen.gob.ec/index.php/institucion/mision-vision. [Último acceso: 29 Noviembre 2021].

[12] A. EP, «SITIO WEB INSTITUCIONAL DE AGUAPEN-INSTITUCION-OBJETIVOS,» 2018. [En línea]. Available: http://www.aguapen.gob.ec/index.php/institucion/objetivos. [Último acceso: 29 Noviembre 2021].

[13] República del Ecuador. Contraloría General del Estado, «Fundamento Legal. Constitución Política de la República del Ecuador,» 2020. [En línea]. Available: https://www.contraloria.gob.ec/LaInstitucion/FundamentoLegal. [Último acceso: 29 Noviembre 2021].

[14] Contraloría General del Estado, «NORMAS DE CONTROL INTERNO DE LA CONTRALORIA,» [En línea]. Available: https://www.oas.org/juridico/PDFs/mesicic5_ecu_ane_cge_12_nor_con_int_400_cge.pdf. [Último acceso: 02 Julio 2021].

[15] ISO27000, «Lista de términos relacionados con la serie ISO 27000 y la seguridad de la información,» Febrero 2018. [En línea]. Available: https://www.iso27000.es/glosario.html. [Último acceso: 30 Noviembre 2021].

[16] G. Baca, Introducción a la Seguridad Informática, PRIMERA EDICIÓN ed., MÉXICO: Grupo Editorial Patria, 2016, p. 361.

[17] J. Fajardo, «SEGURIDAD DE LA INFORMACIÓN, LA RELACIÓN ENTRE CLASIFICACIÓN,» [En línea]. Available: http://repository.unipiloto.edu.co/bitstream/handle/20.500.12277/6266/00005217.pdf?sequence=1&isAllowed=y. [Último acceso: 30 Noviembre 2021].

[18] Ministerio de Telecomunicaciones y de la sociedad de la información, «GUÍA PARA LA GESTION DE RIESGOS DE SEGURIDAD DE LA INFORMACIÓN,» [En línea]. Available: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/GU%C3%8DA-PARA-LA-GESTI%C3%93N-DE-RIESGOS-DE-SEGURIDAD-DE-LA-INFORMACI%C3%93N-ABRIL-2020.pdf. [Último acceso: 30 Noviembre 2021].

[19] I. Bermeo, «"ELABORACIÓN DE UN PLAN DE CONTINGENCIA PARA EL CENTRO DE DATOS,» Quito.

[20] SANS Institute, «Cyber Security Training, Certifications, Degrees and Resources,» [En línea]. Available: https://www.sans.org/. [Último acceso: 30 Noviembre 2021].

[21] ISO, «ISO / IEC 27002: 2013 Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información,» Octubre 2013. [En línea]. Available: https://www.iso.org/standard/54533.html. [Último acceso: 30 Noviembre 2021].

[22] A. Ramírez y Z. Ortiz, «Gestión de Riesgos tecnológicos basada en ISO 31000 e ISO 27005 y su aporte a la continuidad de negocios,» vol. 16, nº 2, pp. 56-66, 2011.

[23] E. Lizarzaburu, A. Gabriela, N. Luis, L. Luciano y P. Mejía, «Gestión de Riesgos Empresariales:,» *Revista Espacios*, vol. 38, nº 59, p. 8, 2017.

[24] Y. López, «ISO 27002:2005 Anexo 13: Gestión de incidentes informáticos de seguridad.,» Colombia, 2010.

[25] A. J. G. Juca, «Diseño de un plan de contingencias del TICs para la Empresa Eléctrica Centrosur,» M.S. Thesis, Cuenca, 2011.

[26] K. A. M. Luna, «Plan de contingencia para la unidad de sistemas y tecnología de información del gobierno Autónomo Descentralizado Antonio Ante en base a la Norma ISO/IEC 27002,» B.S. Thesis, 2015.

[27] A. Paltán y D. Quirumbay, « Evaluación de riesgos y Desarrollo de un plan de recuperación ante desastres informáticos aplicado al Centro de Datos y Comunicaciones de la UPSE.,» La Libertad, 2017.

[28] R. Hernandez, C. Fernandez y P. Baptista, Metodologia de la investigacion (CUARTA EDICIÓN), Mexíco: McGRAW-HILL INTERAMERICANA EDITORES, S.A. DE C.V., 2010.

[29] Instituto Caro y Cuervo, «GUÍA METODOLÓGICA PARA LA GESTIÓN DE RIESGOS DE SEGURIDAD DIGITAL,» 31 Julio 2019. [En línea]. [Último acceso: 12 Noviembre 2021].

[30] M. d. t. y. d. l. s. d. l. informacion, «gobiernoelectronico,» 2020. [En línea]. Available: https://www.gobiernoelectronico.gob.ec/wp-content/uploads/2020/04/GU%C3%8DA-PARA-LA-GESTI%C3%93N-DE-RIESGOS-DE-SEGURIDAD-DE-LA-INFORMACI%C3%93N-ABRIL-2020.pdf. [Último acceso: Agosto 2021].

[31] Consejo Nacional de Planificación, «Plan Nacional de Desarrollo 2017-2021-Toda una Vida,» Senplades, 2017. , [En línea]. Available: https://observatorioplanificacion.cepal.org/sites/default/files/plan/files/EcuandorPlanNacionalTodaUnaVida20172021.pdf. [Último acceso: 04 Julio 2021].

[32] A. Hernández, «Elaboración de un plan de contingencia para las tecnologías de información - caso de estudio "Banco del Estado",» Quito, 2014.

[33] I. Casares y E. Lizarzaburu, Introducción a la gestión integral de riesgos empresariales enfoque ISO 31000, Lima, Peru: Platinum Editorial, 2016.

Anexo 1: Ficha de observación directa realizada en coordinación con el departamento de coordinación de TI.

FICHA DE OBSERVACION			
Fecha de observación:		**No días de observación:**	
Tipo de observación:			
Departamento:			
Nombre del observador:			

Ronald Gonzabay Tomalá

0928122126

Anexo 2: Entrevista realizada al jefe coordinador de TI de la empresa Aguapen Ep.

ENTREVISTA AL JEFE DEL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA COMPAÑÍA AGUAPEN-EP.

ENTREVISTA		
Dirigido a:	Ing Roberto Balón Perero	**Cargo:** Director de TIC's
Realizado por:	Ronald Gonzaboy Tomalá	
Objetivo:	Conocer la situación actual del departamento de Tecnologías de la información de la compañía AGUAPEN-EP, en relación con la seguridad de la información y la gestión de riesgos informáticos.	

Para la entrevista se tomó en consideración al responsable del departamento de Tecnologías de la Información, las preguntas establecidas para dicha entrevista fueron las siguientes:

- ¿Cuántas personas se encargan de la ejecución de los procesos del departamento de Tecnologías de la información y comunicación en la compañía?
- ¿El departamento de Tecnologías de información y comunicación cuenta con algún proceso para controlar incidentes de seguridad?
- ¿Actualmente, el departamento de TI tiene claramente definido los procesos críticos e identificado los activos de tecnologías, aplicaciones e infraestructura, más esenciales de la institución?
- ¿La empresa cuenta con algún tipo de control o firewall para restringir o bloquear el acceso hacia la red por parte de personal no autorizado?
- ¿Considera que el personal administrativo de la institución está capacitado para salvaguardar la integridad de la información de la institución?

- ¿La empresa en la actualidad cuanta con algún servicio de Backups para tener respaldo de la información relevante de los procesos de la empresa ante algún incidente de seguridad?

- ¿Considera que la infraestructura de TI está totalmente protegida?

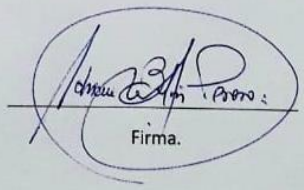
- ¿Considera usted que están preparados para mitigar múltiples fallas en los sistemas en un mismo periodo de tiempo?

- ¿Cómo maneja la empresa el control de acceso a internet por parte de los trabajadores?

- ¿Con qué frecuencia son cambiadas las claves de acceso a los equipos en la institución?

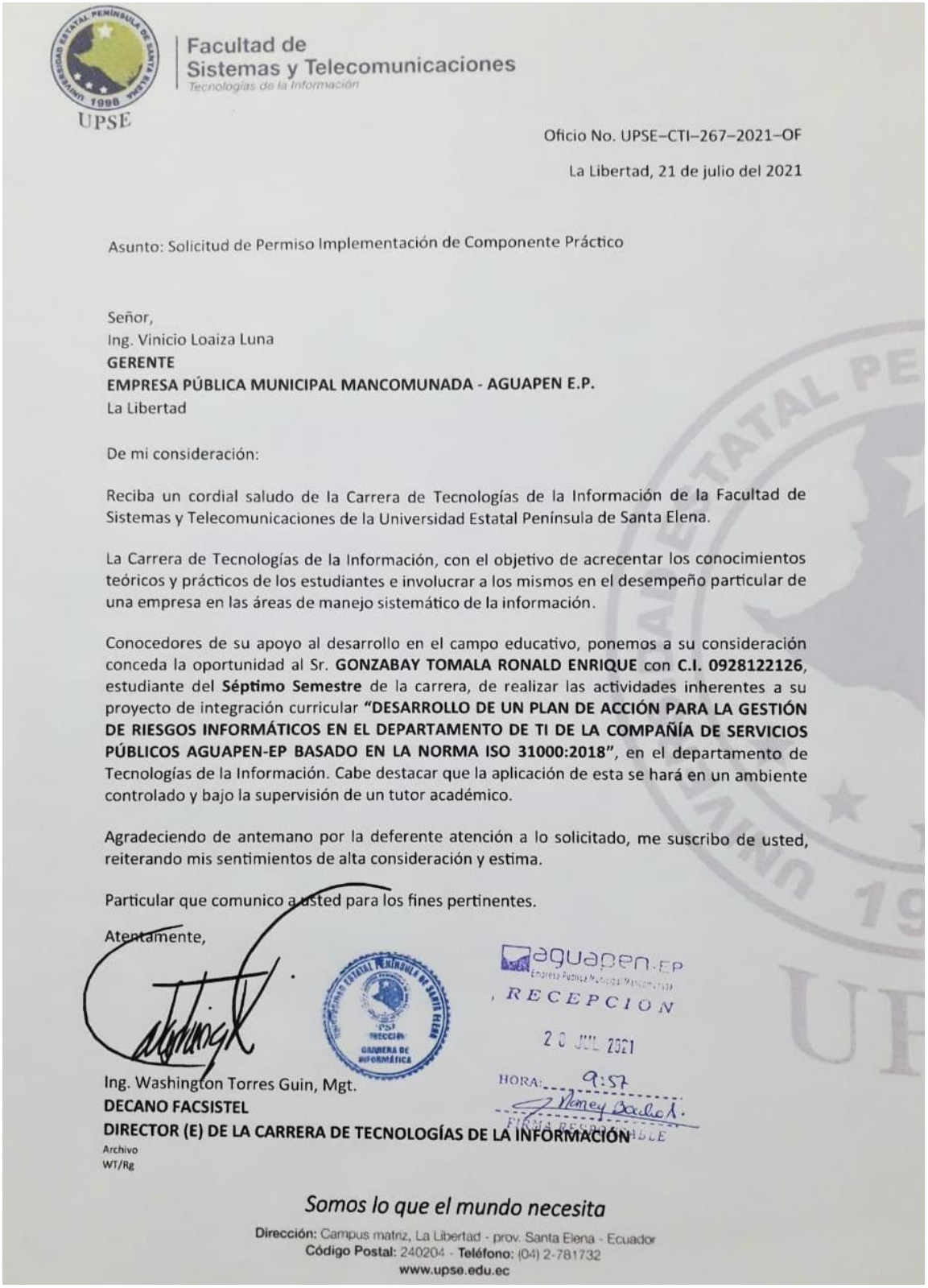
- ¿Considera oportuno identificar las posibles fuentes de riesgos informáticos que pudiesen afectar los activos informáticos que impedirían la correcta ejecución de los procesos de la compañía?

- ¿Consideraría necesario generar un plan de acción para minimizar el nivel de criticidad de los riesgos informáticos que existen en el departamento de TI?



Gracias por su colaboración.

Anexo 3: Evidencia de solicitud para el desarrollo del proyecto en la empresa Aguapen Ep.



Facultad de
Sistemas y Telecomunicaciones
Tecnologías de la Información

UPSE

Oficio No. UPSE–CTI–267–2021–OF

La Libertad, 21 de julio del 2021

Asunto: Solicitud de Permiso Implementación de Componente Práctico

Señor,
Ing. Vinicio Loaiza Luna
GERENTE
EMPRESA PÚBLICA MUNICIPAL MANCOMUNADA - AGUAPEN E.P.
La Libertad

De mi consideración:

Reciba un cordial saludo de la Carrera de Tecnologías de la Información de la Facultad de Sistemas y Telecomunicaciones de la Universidad Estatal Península de Santa Elena.

La Carrera de Tecnologías de la Información, con el objetivo de acrecentar los conocimientos teóricos y prácticos de los estudiantes e involucrar a los mismos en el desempeño particular de una empresa en las áreas de manejo sistemático de la información.

Conocedores de su apoyo al desarrollo en el campo educativo, ponemos a su consideración conceda la oportunidad al Sr. **GONZABAY TOMALA RONALD ENRIQUE** con **C.I. 0928122126**, estudiante del **Séptimo Semestre** de la carrera, de realizar las actividades inherentes a su proyecto de integración curricular **"DESARROLLO DE UN PLAN DE ACCIÓN PARA LA GESTIÓN DE RIESGOS INFORMÁTICOS EN EL DEPARTAMENTO DE TI DE LA COMPAÑÍA DE SERVICIOS PÚBLICOS AGUAPEN-EP BASADO EN LA NORMA ISO 31000:2018"**, en el departamento de Tecnologías de la Información. Cabe destacar que la aplicación de esta se hará en un ambiente controlado y bajo la supervisión de un tutor académico.

Agradeciendo de antemano por la deferente atención a lo solicitado, me suscribo de usted, reiterando mis sentimientos de alta consideración y estima.

Particular que comunico a usted para los fines pertinentes.

Atentamente,

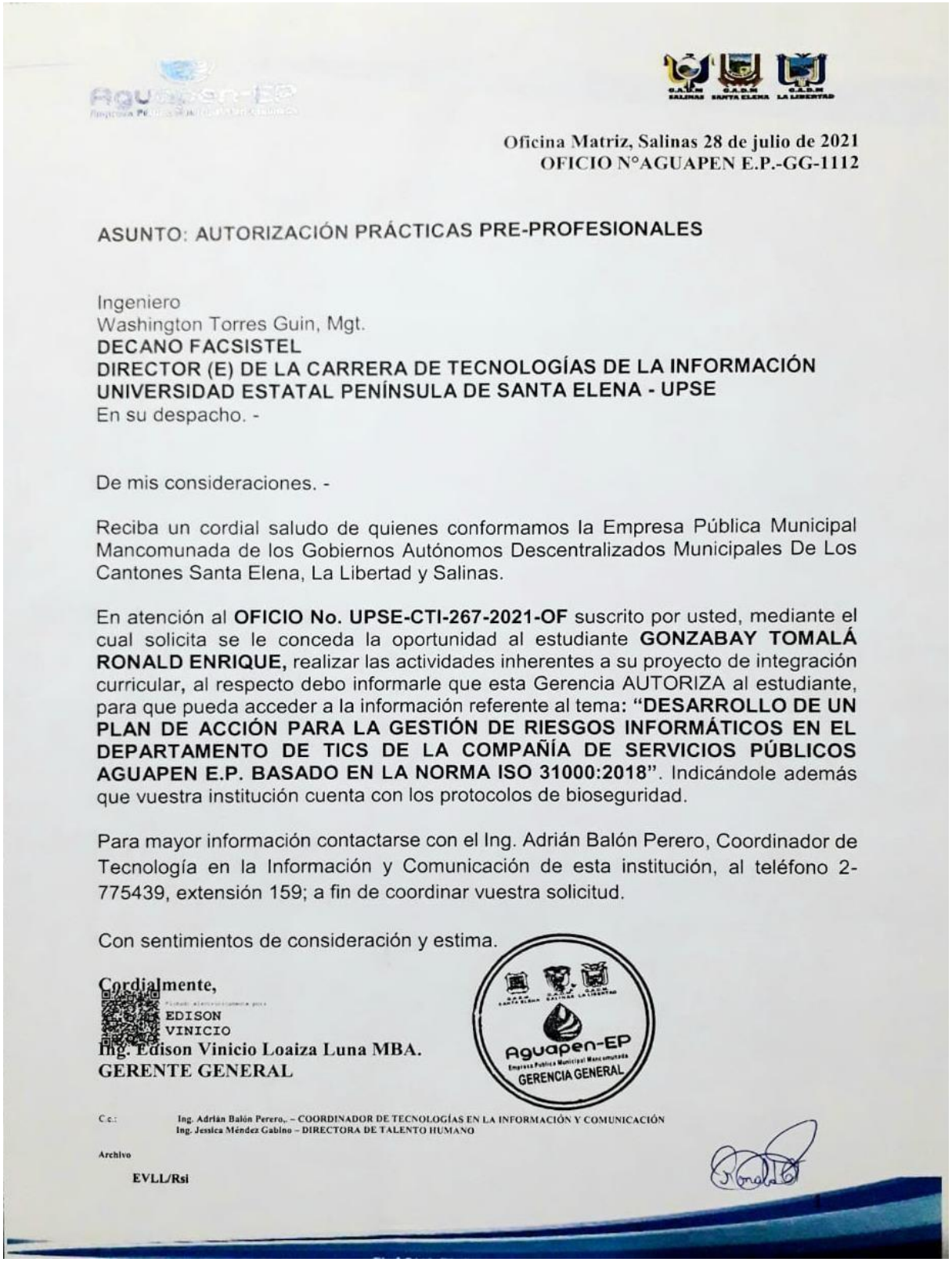
aguapen.EP
RECEPCION
20 JUL 2021
HORA: 9:57
FIRMA RESPONSABLE

Ing. Washington Torres Guin, Mgt.
DECANO FACSISTEL
DIRECTOR (E) DE LA CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN
Archivo
WT/Rg

Somos lo que el mundo necesita

Dirección: Campus matriz, La Libertad - prov. Santa Elena - Ecuador
Código Postal: 240204 - **Teléfono:** (04) 2-781732
www.upse.edu.ec

Anexo 4: Evidencia de autorización para ejecución del proyecto en la empresa.



Oficina Matriz, Salinas 28 de julio de 2021
OFICIO N°AGUAPEN E.P.-GG-1112

ASUNTO: AUTORIZACIÓN PRÁCTICAS PRE-PROFESIONALES

Ingeniero
Washington Torres Guin, Mgt.
DECANO FACSISTEL
DIRECTOR (E) DE LA CARRERA DE TECNOLOGÍAS DE LA INFORMACIÓN
UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA - UPSE
En su despacho. -

De mis consideraciones. -

Reciba un cordial saludo de quienes conformamos la Empresa Pública Municipal Mancomunada de los Gobiernos Autónomos Descentralizados Municipales De Los Cantones Santa Elena, La Libertad y Salinas.

En atención al **OFICIO No. UPSE-CTI-267-2021-OF** suscrito por usted, mediante el cual solicita se le conceda la oportunidad al estudiante **GONZABAY TOMALÁ RONALD ENRIQUE,** realizar las actividades inherentes a su proyecto de integración curricular, al respecto debo informarle que esta Gerencia AUTORIZA al estudiante, para que pueda acceder a la información referente al tema: **"DESARROLLO DE UN PLAN DE ACCIÓN PARA LA GESTIÓN DE RIESGOS INFORMÁTICOS EN EL DEPARTAMENTO DE TICS DE LA COMPAÑÍA DE SERVICIOS PÚBLICOS AGUAPEN E.P. BASADO EN LA NORMA ISO 31000:2018"**. Indicándole además que vuestra institución cuenta con los protocolos de bioseguridad.

Para mayor información contactarse con el Ing. Adrián Balón Perero, Coordinador de Tecnología en la Información y Comunicación de esta institución, al teléfono 2-775439, extensión 159; a fin de coordinar vuestra solicitud.

Con sentimientos de consideración y estima.

Cordialmente,

EDISON VINICIO
Ing. Edison Vinicio Loaiza Luna MBA.
GERENTE GENERAL

Aguapen-EP
Empresa Pública Municipal Mancomunada
GERENCIA GENERAL

C.c.: Ing. Adrián Balón Perero, – COORDINADOR DE TECNOLOGÍAS EN LA INFORMACIÓN Y COMUNICACIÓN
Ing. Jessica Méndez Gabino – DIRECTORA DE TALENTO HUMANO

Archivo

EVLL/Rsi

Anexo 5: Matriz de evaluación de riesgos medido por la probabilidad vs impacto.

TIPO DE ACTIVO	ID	ACTIVO	CODIGO AMENAZA	AMENAZA	AGENTE DE AMENAZA	VULNERABILIDAD	EVALUACIÓN DE RIESGOS				
							IMPACTO	PROBABILIDAD		CÁLCULO DEL NIVEL DE RIESGO	NIVEL DE RIESGO
							PROM CID	NIVEL DE AMENAZA	NIVEL DE VULNERABILIDAD		
INFRAESTRUCTURA	ACT001	SERVIDOR HP PROLIANT DL380 GEN 9	A-008	Acceso de terceros al servidor.	Hacker / Cracker	Puertos abiertos en el servidor	3,00	3	3	27	ALTO
			A-009	Denegación de Servicio DDOS	Hacker / Cracker	Infecciones en la red	3,00	3	2	18	ALTO
			A-029	Sobrecargas y cortes de energía eléctrica	Suministrador de energía electrica / falla	Partes del hardware del servidor con falencias	2,67	3	3	24	ALTO
			A-004	Inundación	Natural	Carencia de medidas preventivas	2,67	2	3	16	MEDIO
			A-027	Acceso no autorizado	Personal Descontento	Data Center sin adecuada protección de acceso	2,67	2	3	16	MEDIO
			A-002	Incendio	Natural	falta de extintores en el centro de datos	3,00	2	3	18	ALTO
	ACT002	SERV_SISTEMA_FINANCIERO	A-034	Infección de sistema	Scriptkiddie	Fallo en el sistema	3,00	3	3	27	ALTO
			A-030	Variaciones de voltaje	Material (falla)	Indisponibilidad del sistema por periodo de inactividad	2,67	3	3	24	ALTO
	ACT003	SERV_BD_SISTEMA_FINANCIERO	A-011	Inyección por SQL	Hacker / Cracker	Carencia de un saneamiento de entrada adecuado.	3,00	2	3	18	ALTO

	ACT004	SERV_SISTEMA_COMERCIAL	A-012	Infección de sistema	Scriptkiddie	Fallo en el sistema	3,00	2	3	18	ALTO
			A-013	Format string bugs	Desarrollador	Errores de cadena de formato / ejecución de código arbitrario	3,00	2	3	18	ALTO
	ACT007	SERV_BD_ SISTEMA_COMERCIAL	A-011	Inyección por SQL	Hacker / Cracker	Carencia de un saneamiento de entrada adecuado.	3,00	2	3	18	ALTO
			A-015	Sabotaje	Personal Descontento	Personal de confianza que quiera acceder a la base de datos	3,00	2	2	12	MEDIO
	ACT008	SERV_CORREO_ELECTRONICO	A-016	Fuga de datos	Hacker / Cracker	Falta de cifrado de protocolos SMTP, POP3 e IMAP	3,00	3	2	18	ALTO
			A-009	Denegación de Servicio DDOS	Hacker / Cracker	Carencia de la limitación de conexiones al servidor SMTP	3,00	3	2	18	ALTO
	ACT009	SER_PAGINA_WEB	A-017	Ataque Cross-Site Scripting	Hacker / Cracker	Datos sin validar	2,67	3	3	24	ALTO
			A-011	Inyección por SQL	Hacker / Cracker	Carencia de un saneamiento de entrada adecuado.	2,33	3	3	21	ALTO
	ACT009	SERV_DOMINIO	A-018	Ataques DNS basados en botnets	Hacker / Cracker	Ordenadores conectados posiblemente infectados	3,00	3	2	18	ALTO
			A-019	Password Spaying/	Hacker / Cracker	Contraseñas de acceso al servicio de Active Directory comúnes entre los usuarios	3,00	3	2	18	ALTO
	ACT010	SERV_FTP	A-020	Manipulación de archivos compartidos	Hacker / Cracker	Carece de encriptación y autenticación	2,33	3	2	14	MEDIO
			A-021	Malware	Hacker / Cracker	Desactualización de parches de seguridad	3,00	3	2	18	ALTO

	ACT011	SERV_ DIGITALIZACION	A-004	Inundación	Natural	Carencia de medidas preventivas	2,00	2	3	12	MEDIO
	ACT012	SERV_ KERIO	A-021	Malware	Hacker / Cracker	Uso de VPN por funcionarios desde sus hogares con máquinas vulnerables a malware	3,00	3	2	18	ALTO
	ACT013	SERV_BIOMETRICO	A-033	Filtración de componentes en estado liquido	Material (falla)	Equipo descontinuado (averias)	1,67	2	3	10	MEDIO
COMUNICACIONES, REDES.	ACT014	SWITCH CORE HP 5500AF48G-POE	A-022	Ataque Man in the middle	Hacker / Cracker	Desactualización de firmware / parches de seguridad	2,33	3	2	14	MEDIO
			A-003	Polvo	Natural	carencia de fechas fijas para mantenimiento preventivo	2,33	3	1	7	BAJO
	ACT015	SWITCH ACCESS HP 5120AF48G-POE	A-022	Ataque Man in the middle	Hacker / Cracker	Desactualización de firmware / parches de seguridad	2,67	3	2	16	MEDIO
			A-004	Inundación	Natural	Carencia de medidas preventivas	2,67	2	2	11	MEDIO
	ACT016	SWITCH CISCO CATALYST 2960	A-022	Ataque Man in the middle	Scriptkiddie	Desactualización de firmware / parches de seguridad	2,67	3	2	16	MEDIO
			A-004	Inundación	Material (falla)	Carencia de medidas preventivas	2,67	2	2	11	MEDIO
	ACT017	ROUTER CNT ISP	A-035	Fallos operativos	Proveedor	Desactualización de firmware / parches de seguridad	2,00	3	3	18	ALTO
			A-004	Inundación	Material (falla)	Carencia de medidas preventivas	2,00	3	2	12	MEDIO
	ACT018	ROUTER TELCONET ISP	A-035	Fallos operativos	Proveedor	Desactualización de firmware /parches de seguridad	2,00	3	3	18	ALTO

	ACT019	WIRELESS ROUTER HUAWEI	A-036	Intrusos en la red wifi	Scriptkiddie	Protocolos de cifrado descontinuados	3,00	3	3	27	ALTO
HARDWARE Y APLICACIONES.	ACT020	CPU DELL CORE I5 OCTAVA GENERACION	A-032	Virus en pc del Coordinador de TIC	Hacker / Cracker	Presencia de virus informático	2,33	1	2	5	BAJO
			A-003	Polvo	Natural	carencia de fechas fijas para mantenimiento preventivo	2,33	2	1	5	BAJO
	ACT021	CPU HP CORE I7 SEPTIMA GENERACION	A-032	Virus en pc del Administrador de base de datos	Hacker / Cracker	Presencia de virus informático	2,33	1	2	5	BAJO
	ACT022	CPU DELL CORE I7 SEPTIMA GENERACION	A-032	Virus en pc del jefe de Infraestructura	Hacker / Cracker	Presencia de virus informático	2,33	1	2	5	BAJO
			A-003	Polvo	Natural	Carencia de fechas fijas para mantenimiento preventivo	2,33	2	1	5	BAJO
	ACT023	CPU DELL CORE I7 SEPTIMA GENERACION	A-032	Virus en pc del Desarrollador	Hacker / Cracker	Presencia de virus informático	2,33	1	2	5	BAJO
			A-003	Polvo	Natural	carencia de fechas fijas para mantenimiento preventivo	2,33	2	1	5	BAJO
	ACT024	CPU DELL CORE I5 SEPTIMA GENERACION	A-032	Virus en pc del Desarrollador Junior	Falta de financiamiento	Discos defectuosos	2,33	1	2	5	BAJO
			A-003	Polvo	Natural	carencia de fechas fijas para mantenimiento preventivo	2,33	2	1	5	BAJO
	ACT025	CENTRAL TELEFONICA IP PANASONIC HIBRIDA KX-NS500	A-004	Inundación	Material (falla)	Carencia de medidas preventivas	2,33	2	3	14	MEDIO
			A-003	Polvo	Natural	carencia de fechas fijas para mantenimiento preventivo	2,33	2	1	5	BAJO
	ACT026	IMPRESORA HP PAGEWIDE PRO 477	A-004	Inundación	Natural	Carencia de medidas preventivas	2,33	2	3	14	MEDIO

EQUIPAMIENTO AUXILIAR	ACT027	UPS COMPUTER PONER 3KVA	A-030	Periféricos o Componentes defectuosos	Material (falla)	UPS descontinuado	2,67	3	2	16	MEDIO
	ACT028	NVR HIKVISION	A-037	Carencia de equipos de videovigilancia	Falta de financiamiento	Puntos Ciegos (sin monitoreo)	2,67	3	3	24	ALTO
			A-038	Fallos en cámaras de videovigilancia	Falta de financiamiento	Indisponibilidad del sistema por periodo de inactividad	2,67	3	3	24	ALTO
	ACT029	Cableado	A-028	Errores en la organización	Empleado sin experiencia	Interrupciones constantes / ruido	2,33	3	2	14	MEDIO
			A-014	Acceso no autorizado	Personal sin experiencia	Deficiente o nulo etiquetado del cable	2,67	2	2	11	MEDIO
	ACT030	Aire Acondicionado	A-003	Polvo	Natural	Carencia de fechas fijas para mantenimiento preventivo	2,00	2	1	5	BAJO
			A-004	Inundación	Natural	Carencia de medidas preventivas	2,00	2	3	12	MEDIO
Soportes de Información	ACT031	Discos Duros Externos.	A-024	Sabotaje	Personal Descontento	Carencia de fechas fijas para mantenimiento preventivo	2,33	2	3	14	MEDIO
			A-015	Hurto	Personal Descontento	Libre acceso a discos duros en el área de soporte	2,33	2	3	14	MEDIO
	ACT032	Blu-ray Disk	A-024	Sabotaje	Personal Descontento	Carencia de fechas fijas para mantenimiento preventivo	2,33	2	3	14	MEDIO
			A-015	Hurto	Personal Descontento	Libre acceso a discos blu-ray en el área de soporte	2,33	2	3	14	MEDIO
	ACT033	Memorias USB	A-039	Periféricos o Componentes defectuosos	Material (falla)	Dispositivos con averias físicas	2,67	2	2	11	MEDIO
			A-024	Hurto	Personal Descontento	Libre acceso a dispositivos USB en el área de soporte	2,33	2	3	14	MEDIO

	ACT034	Resmas de papel impresas.	A-005	Incendio	Personal / falla	Documentación sin respaldo en la nube	2,00	2	3	12	MEDIO
			A-024	Hurto	Personal Descontento	Falta de organización de documentos en folders	2,00	2	3	12	MEDIO
PERSONAL	ACT035	TALENTO HUMANO	A-007	Epidemias	Personal	Contagios COVID-19	2,33	3	2	14	MEDIO
			A-025	Phishing	Hacker / Cracker	Falta de capacitación sobre ciberseguridad	2,33	3	3	21	ALTO
			A-026	Ingeniería social	Hacker / Cracker	Falta de capacitación sobre ciberseguridad	2,33	3	3	21	ALTO

Anexo 6: Entrevista realizada al jefe de Coordinación de TI

Anexo 7: Matriz de registro de cumplimiento de salvaguardas preventivas.

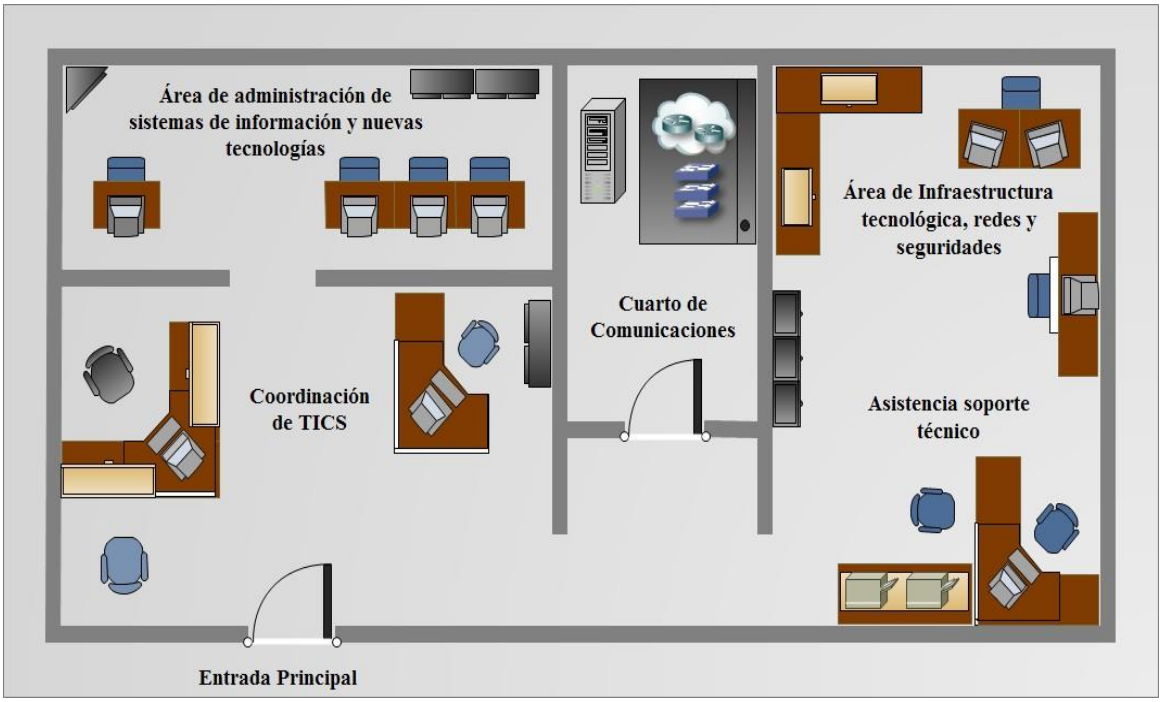
Aguapen-EP Empresa Pública Municipal Mancomunada	EMPRESA PÚBLICA MUNICIPAL MANCOMUNADA AGUAPEN EP MATRIZ DE REGISTRO DE CUMPLIMIENTO DE SALVAGUARDAS PREVENTIVAS ANTE CONTINGENCIAS A CARGO DEL DEPARTAMENTO DE TI						
No.	**ACTIVIDAD PREVENTIVA**	**CUMPLIMIENTO**		**FECHA**	**HORA**	**FIRMA DEL ENCARGADO DE REVISIÓN**	**OBSERVACIÓN**
		SI	**NO**				

Anexo 8: Bitácora de registro de contingencias en el departamento de TI.

Aguapen-EP Empresa Pública Municipal Mancomunada	**EMPRESA PÚBLICA MUNICIPAL MANCOMUNADA AGUAPEN EP** BITÁCORA DE REGISTRO DE CONTINGENCIAS EN EL DEPARTAMENTO DE TI	TICS

FECHA DE REPORTE	CONTINGENCIA	HORA	FIRMA DEL ENCARGADO DE REGISTRO	OBSERVACIÓN

Anexo 9: Diseño Físico del área de coordinación de Tecnologías de la Información de la empresa AGUAPEN-EP



Anexo 10: Controles ISO/IEC 27002:2013.

ISO/IEC 27002:2013. 14 DOMINIOS, 35 OBJETIVOS DE CONTROL Y 114 CONTROLES

5. POLÍTICAS DE SEGURIDAD.
- 5.1 Directrices de la Dirección en seguridad de la información.
  - 5.1.1 Conjunto de políticas para la seguridad de la información.
  - 5.1.2 Revisión de las políticas para la seguridad de la información.

6. ASPECTOS ORGANIZATIVOS DE LA SEGURIDAD DE LA INFORMAC.
- 6.1 Organización interna.
  - 6.1.1 Asignación de responsabilidades para la segur. de la información.
  - 6.1.2 Segregación de tareas.
  - 6.1.3 Contacto con las autoridades.
  - 6.1.4 Contacto con grupos de interés especial.
  - 6.1.5 Seguridad de la información en la gestión de proyectos.
- 6.2 Dispositivos para movilidad y teletrabajo.
  - 6.2.1 Política de uso de dispositivos para movilidad.
  - 6.2.2 Teletrabajo.

7. SEGURIDAD LIGADA A LOS RECURSOS HUMANOS.
- 7.1 Antes de la contratación.
  - 7.1.1 Investigación de antecedentes.
  - 7.1.2 Términos y condiciones de contratación.
- 7.2 Durante la contratación.
  - 7.2.1 Responsabilidades de gestión.
  - 7.2.2 Concienciación, educación y capacitación en segur. de la informac.
  - 7.2.3 Proceso disciplinario.
- 7.3 Cese o cambio de puesto de trabajo.
  - 7.3.1 Cese o cambio de puesto de trabajo.

8. GESTIÓN DE ACTIVOS.
- 8.1 Responsabilidad sobre los activos.
  - 8.1.1 Inventario de activos.
  - 8.1.2 Propiedad de los activos.
  - 8.1.3 Uso aceptable de los activos.
  - 8.1.4 Devolución de activos.
- 8.2 Clasificación de la información.
  - 8.2.1 Directrices de clasificación.
  - 8.2.2 Etiquetado y manipulado de la información.
  - 8.2.3 Manipulación de activos.
- 8.3 Manejo de los soportes de almacenamiento.
  - 8.3.1 Gestión de soportes extraíbles.
  - 8.3.2 Eliminación de soportes.
  - 8.3.3 Soportes físicos en tránsito.

9. CONTROL DE ACCESOS.
- 9.1 Requisitos de negocio para el control de accesos.
  - 9.1.1 Política de control de accesos.
  - 9.1.2 Control de acceso a las redes y servicios asociados.
- 9.2 Gestión de acceso de usuario.
  - 9.2.1 Gestión de altas/bajas en el registro de usuarios.
  - 9.2.2 Gestión de los derechos de acceso asignados a usuarios.
  - 9.2.3 Gestión de los derechos de acceso con privilegios especiales.
  - 9.2.4 Gestión de información confidencial de autenticación de usuarios.
  - 9.2.5 Revisión de los derechos de acceso de los usuarios.
  - 9.2.6 Retirada o adaptación de los derechos de acceso
- 9.3 Responsabilidades del usuario.
  - 9.3.1 Uso de información confidencial para la autenticación.
- 9.4 Control de acceso a sistemas y aplicaciones.
  - 9.4.1 Restricción del acceso a la información.
  - 9.4.2 Procedimientos seguros de inicio de sesión.
  - 9.4.3 Gestión de contraseñas de usuario.
  - 9.4.4 Uso de herramientas de administración de sistemas.
  - 9.4.5 Control de acceso al código fuente de los programas.

10. CIFRADO.
- 10.1 Controles criptográficos.
  - 10.1.1 Política de uso de los controles criptográficos.
  - 10.1.2 Gestión de claves.

11. SEGURIDAD FÍSICA Y AMBIENTAL.
- 11.1 Áreas seguras.
  - 11.1.1 Perímetro de seguridad física.
  - 11.1.2 Controles físicos de entrada.
  - 11.1.3 Seguridad de oficinas, despachos y recursos.
  - 11.1.4 Protección contra las amenazas externas y ambientales.
  - 11.1.5 El trabajo en áreas seguras.
  - 11.1.6 Áreas de acceso público, carga y descarga.
- 11.2 Seguridad de los equipos.
  - 11.2.1 Emplazamiento y protección de equipos.
  - 11.2.2 Instalaciones de suministro.
  - 11.2.3 Seguridad del cableado.
  - 11.2.4 Mantenimiento de los equipos.
  - 11.2.5 Salida de activos fuera de las dependencias de la empresa.
  - 11.2.6 Seguridad de los equipos y activos fuera de las instalaciones.
  - 11.2.7 Reutilización o retirada segura de dispositivos de almacenamiento.
  - 11.2.8 Equipo informático de usuario desatendido.
  - 11.2.9 Política de puesto de trabajo despejado y bloqueo de pantalla.

12. SEGURIDAD EN LA OPERATIVA.
- 12.1 Responsabilidades y procedimientos de operación.
  - 12.1.1 Documentación de procedimientos de operación.
  - 12.1.2 Gestión de cambios.
  - 12.1.3 Gestión de capacidades.
  - 12.1.4 Separación de entornos de desarrollo, prueba y producción.
- 12.2 Protección contra código malicioso.
  - 12.2.1 Controles contra el código malicioso.
- 12.3 Copias de seguridad.
  - 12.3.1 Copias de seguridad de la información.
- 12.4 Registro de actividad y supervisión.
  - 12.4.1 Registro y gestión de eventos de actividad.
  - 12.4.2 Protección de los registros de información.
  - 12.4.3 Registros de actividad del administrador y operador del sistema.
  - 12.4.4 Sincronización de relojes.
- 12.5 Control del software en explotación.
  - 12.5.1 Instalación del software en sistemas en producción.
- 12.6 Gestión de la vulnerabilidad técnica.
  - 12.6.1 Gestión de las vulnerabilidades técnicas.
  - 12.6.2 Restricciones en la instalación de software.
- 12.7 Consideraciones de las auditorías de los sistemas de información.
  - 12.7.1 Controles de auditoría de los sistemas de información.

13. SEGURIDAD EN LAS TELECOMUNICACIONES.
- 13.1 Gestión de la seguridad en las redes.
  - 13.1.1 Controles de red.
  - 13.1.2 Mecanismos de seguridad asociados a servicios en red.
  - 13.1.3 Segregación de redes.
- 13.2 Intercambio de información con partes externas.
  - 13.2.1 Políticas y procedimientos de intercambio de información.
  - 13.2.2 Acuerdos de intercambio.
  - 13.2.3 Mensajería electrónica.
  - 13.2.4 Acuerdos de confidencialidad y secreto.

14. ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE LOS SISTEMAS DE INFORMACIÓN.
- 14.1 Requisitos de seguridad de los sistemas de información.
  - 14.1.1 Análisis y especificación de los requisitos de seguridad.
  - 14.1.2 Seguridad de las comunicaciones en servicios accesibles por redes públicas.
  - 14.1.3 Protección de las transacciones por redes telemáticas.
- 14.2 Seguridad en los procesos de desarrollo y soporte.
  - 14.2.1 Política de desarrollo seguro de software.
  - 14.2.2 Procedimientos de control de cambios en los sistemas.
  - 14.2.3 Revisión técnica de las aplicaciones tras efectuar cambios en el sistema operativo.
  - 14.2.4 Restricciones a los cambios en los paquetes de software.
  - 14.2.5 Uso de principios de ingeniería en protección de sistemas.
  - 14.2.6 Seguridad en entornos de desarrollo.
  - 14.2.7 Externalización del desarrollo de software.
  - 14.2.8 Pruebas de funcionalidad durante el desarrollo de los sistemas.
  - 14.2.9 Pruebas de aceptación.
- 14.3 Datos de prueba.
  - 14.3.1 Protección de los datos utilizados en pruebas.

15. RELACIONES CON SUMINISTRADORES.
- 15.1 Seguridad de la información en las relaciones con suministradores.
  - 15.1.1 Política de seguridad de la información para suministradores.
  - 15.1.2 Tratamiento del riesgo dentro de acuerdos de suministradores.
  - 15.1.3 Cadena de suministro en tecnologías de la información y comunicaciones.
- 15.2 Gestión de la prestación del servicio por suministradores.
  - 15.2.1 Supervisión y revisión de los servicios prestados por terceros.
  - 15.2.2 Gestión de cambios en los servicios prestados por terceros.

16. GESTIÓN DE INCIDENTES EN LA SEGURIDAD DE LA INFORMACIÓN.
- 16.1 Gestión de incidentes de seguridad de la información y mejoras.
  - 16.1.1 Responsabilidades y procedimientos.
  - 16.1.2 Notificación de los eventos de seguridad de la información.
  - 16.1.3 Notificación de puntos débiles de la seguridad.
  - 16.1.4 Valoración de eventos de seguridad de la información y toma de decisiones.
  - 16.1.5 Respuesta a los incidentes de seguridad.
  - 16.1.6 Aprendizaje de los incidentes de seguridad de la información.
  - 16.1.7 Recopilación de evidencias.

17. ASPECTOS DE SEGURIDAD DE LA INFORMACION EN LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO.
- 17.1 Continuidad de la seguridad de la información.
  - 17.1.1 Planificación de la continuidad de la seguridad de la información.
  - 17.1.2 Implantación de la continuidad de la seguridad de la información.
  - 17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información.
- 17.2 Redundancias.
  - 17.2.1 Disponibilidad de instalaciones para el procesamiento de la información.

18. CUMPLIMIENTO.
- 18.1 Cumplimiento de los requisitos legales y contractuales.
  - 18.1.1 Identificación de la legislación aplicable.
  - 18.1.2 Derechos de propiedad intelectual (DPI).
  - 18.1.3 Protección de los registros de la organización.
  - 18.1.4 Protección de datos y privacidad de la información personal.
  - 18.1.5 Regulación de los controles criptográficos.
- 18.2 Revisiones de la seguridad de la información.
  - 18.2.1 Revisión independiente de la seguridad de la información.
  - 18.2.2 Cumplimiento de las políticas y normas de seguridad.
  - 18.2.3 Comprobación del cumplimiento.

 Octubre-2013