UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA

FACULTAD DE SISTEMAS Y TELECOMUNICACIONES

CARRERA DE INFORMÁTICA

TRABAJO DE TITULACIÓN

Propuesta tecnológica, previo a la obtención del Título de**:**

INGENIERA EN SISTEMAS

"Evaluación de riesgos y Desarrollo de un plan de recuperación ante desastres informáticos aplicado al Centro de Datos y Comunicaciones de la UPSE"

AUTOR

ANDREA ELIZABETH PALTÁN ORELLANA

PROFESOR TUTOR

LSI. DANIEL IVÁN QUIRUMBAY YAGUAL, MSIA.

LA LIBERTAD – ECUADOR

2017

AGRADECIMIENTO

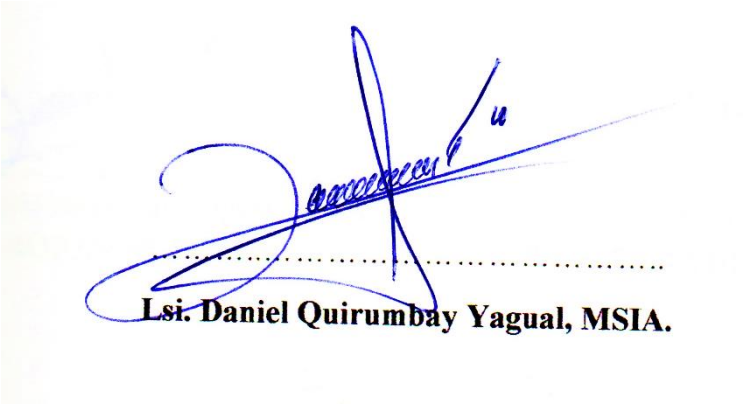
Agradezco a Dios por concederme salud y bienestar para poder finalizar favorablemente este trabajo y alcanzar cada uno de mis logros, a mis padres quienes me han enseñado día a día valores y principios indispensables para ser una persona de bien, a mis hermanos y amigos quienes siempre fueron incondicionales conmigo. A mis profesores por el conocimiento académico impartido; a mi Director de Tesis Licenciado Daniel Quirumbay, quien ha demostrado su experiencia en ser un excelente guía profesional. A todo el personal del departamento de Dirección de Tecnologías de Información y Comunicación de la UPSE, quienes han contribuido a proporcionar la información necesaria y colaboración brindada durante este proceso y mi profundo agradecimiento a las autoridades principales; Decano y Director de la carrera de informática, respetables profesionales por darme un gran sustento dentro de mi prestigiosa Universidad Estatal Península de Santa Elena.

Andrea Elizabeth Paltán Orellana

APROBACIÓN DEL TUTOR

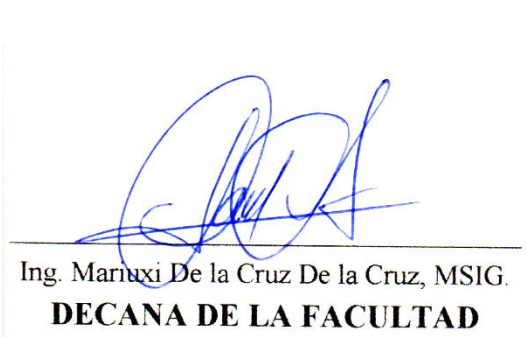
En mi calidad de tutor del trabajo de titulación denominado: "**Evaluación de riesgos y desarrollo de un plan de recuperación ante desastres informáticos aplicado al Centro de Datos y Comunicaciones de la UPSE**", elaborado por la egresada **Paltán Orellana Andrea Elizabeth**, de la carrera de Informática 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, 14 de agosto del 2017

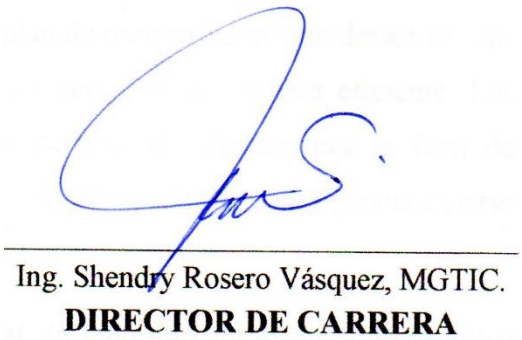


Lsi. Daniel Quirumbay Yagual, MSIA.

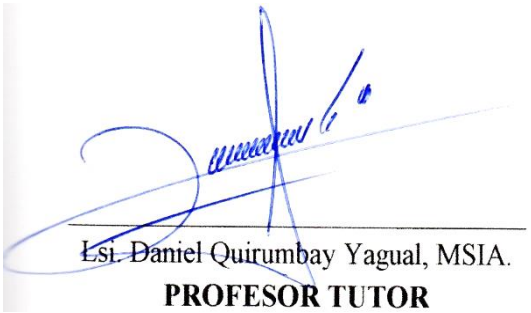
TRIBUNAL DE GRADO



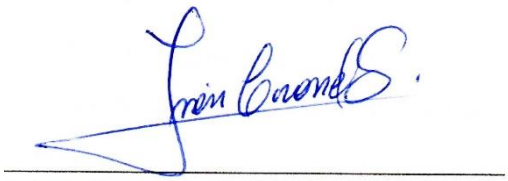
Ing. Mariuxi De la Cruz De la Cruz, MSIG.
DECANA DE LA FACULTAD



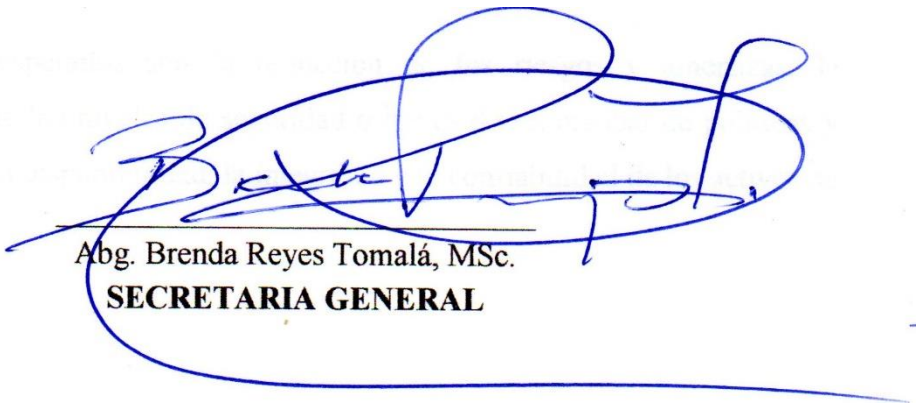
Ing. Shendry Rosero Vásquez, MGTIC.
DIRECTOR DE CARRERA



Lsi. Daniel Quirumbay Yagual, MSIA.
PROFESOR TUTOR



Ing. Iván Coronel Suárez, MSIA.
PROFESOR DE ÁREA



Abg. Brenda Reyes Tomalá, MSc.
SECRETARIA GENERAL

RESUMEN

El presente trabajo de titulación fue desarrollado para el centro de datos de la UPSE, área informática, el cual no dispone de un plan de recuperación ante desastres, que permita la reanudación de las operaciones y servicios de manera eficiente. Los mecanismos de seguridad física y lógica carecen de eficacia por la falta de documentos e informes escritos que garanticen actividades de contingencia en caso de desastres físicos y naturales.

Por tal motivo resulta esencial implementar un plan de contingencia informático que contenga un conjunto de medidas técnicas, humanas y administrativas indispensables para la continuidad de las operaciones, tomando como base principal la implantación de dominios y controles de seguridad basados en estándares internacionales como: ISO/IEC 27002, ISO/IEC 27001, SANS Security Policy, Estándar BS 7799-2 (Physical Security Policy), Metodología MAGERIT V.3**,** que proporcionen un análisis efectivo de impactos sobre la organización y faciliten estrategias de recuperación para afrontar de manera oportuna eventualidades de emergencia.

El objetivo general que persigue el proyecto es la elaboración de un plan de contingencias de TI mediante el uso de dominios de control y metodologías de análisis de riesgos basado en normas internacionales.

Los resultados esperados son la reducción de los riesgos y amenazas, la incrementación de los niveles de seguridad a través de un manual de políticas y procedimientos, la disponibilidad, la integridad y la confiabilidad de los activos de la información.

ABSTRACT

The present titling work was developed for the data center of UPSE, a computer area that does not have a disaster recovery plan, which allows the resumption of operations and services in an efficient manner. The mechanisms of physical and logical security are ineffective due to the lack of documents and written reports that guarantee contingency activities in case of physical and natural disasters.

For this reason it is essential to implement a computer contingency plan containing a set of technical, human and administrative measures essential for the continuity of operations, based on the implementation of domains and security controls based on international standards such as ISO / IEC 27001, ISO / IEC 27002, SANS Security Policy, Standard BS 7799-2 (Physical Security Policy), MAGERIT V3 Methodology, which provide an effective analysis of impacts on the organization and facilitate recovery strategies to deal with emergency contingencies in a timely manner .

The overall objective of the project is the development of an IT contingency plan through the use of control domains and risk analysis methodologies based on international standards.

The expected results are the reduction of risks and threats, the increase of security levels through a manual of policies and procedures, the availability, integrity and reliability of information assets.

DECLARACIÓN

El contenido del presente Trabajo de Graduación es de mi responsabilidad; el patrimonio intelectual del mismo pertenece a la Universidad Estatal Península de Santa Elena.

Andrea Elizabeth Paltán Orellana

TABLA DE CONTENIDOS

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

LISTA DE ANEXOS

INTRODUCCIÓN

En la actualidad los sistemas han evolucionado de manera vertiginosa, a través de las tecnologías de la información y comunicación (TIC); facilitando el procesamiento, transmisión y almacenamiento de enormes cantidades de datos. Sin embargo, esto ha provocado el surgimiento continuo de nuevas amenazas originando que los sistemas de información no sean totalmente seguros. En el departamento de Tic's, en el área del centro de datos ubicado en la Universidad Estatal Península de Santa Elena, se requiere la existencia de un plan de contingencias que admita o especifique medidas de seguridad óptimas, necesarias y apropiadas para una excelente calidad en la gestión administrativa de la institución favoreciendo la protección de recursos informáticos al reducir altos índices de amenazas tanto físicas como humanas. Por tal razón, las normas o estándares internacionales referentes a la seguridad de la información y las metodologías relacionadas con el análisis y gestión de riesgos informáticos contribuyen a la implementación de un plan de contingencias efectivo que enfrente casos críticos de emergencia derivados principalmente por la presencia de desastres naturales, y problemas informáticos.

La finalidad del proyecto conlleva principalmente a la realización de un análisis y gestión de riesgos informáticos utilizando exclusivamente la metodología Magerit version 3 para determinar los posibles inconvenientes que pueden sufrir los sistemas de información, eligiendo de esta forma los riesgos más significativos dentro de la institución con la intención de solucionarlos. Además, el análisis y uso eficiente de estándares, normas o leyes internacionales de seguridad que fueron creadas para lograr la prevención de amenazas beneficiando a las organizaciones públicas a: reducir sus pérdidas económicas, alcanzar la maximización de oportunidades y recuperar la continuidad del negocio en todo momento ante incidentes negativos, se convierten en un recurso necesario para el desarrollo del proyecto. Es importante recordar que los riesgos cambian con frecuencia produciendo vulnerabilidades, debido a eso será necesario inspeccionar regularmente el plan de seguridad informático y actualizar periódicamente todos los lineamientos implementados.

CAPÍTULO I

FUNDAMENTACIÓN DEL PROYECTO

1.1. Antecedentes

En la actualidad, la información es considerada parte primordial que toda empresa debe cautelar frente a situaciones de riesgo, esto implica que sea necesario el desarrollo de un plan de contingencias que permita restaurar el funcionamiento de los equipos de forma rápida, eficiente y con el menor costo posible. El centro de datos de la UPSE dispone de varios activos que pueden estar expuestos a constantes riesgos y amenazas que desencadenarían en posibles pérdidas ocasionando graves perjuicios a la institución.

Cabe mencionar que el departamento de TI carece de documentación escrita, precisa y optima sobre políticas y procedimientos de seguridad que faciliten la recuperación oportuna de las operaciones informáticas. La Universidad Estatal Península de Santa Elena está encaminada a ser un establecimiento de educación superior de excelencia, esto implica que sea beneficioso contar con un plan de recuperación ante desastres informáticos que establezcan precauciones para reducir el impacto producido por calamidades y mantener protegidos de manera adecuada los sistemas de información.

Adicionalmente un reciente análisis sobre el uso de políticas de seguridad de la información basadas en estándares internacionales ISO, específicamente la última versión ISO/IEC 27002:2013 presentada en 14 secciones y contempladas en 114 controles a diferencia de la versión anterior publicada en el año 2005, así como también el uso de ciertos estándares exclusivos para la seguridad física y para el análisis y gestión de riesgos como ISO 27001:2013 han resultado notablemente eficaces en la excelente calidad de protección sobre los activos informáticos. Con este documento se pretende disminuir los riesgos, de modo que las probabilidades de ser afectados por daño, por robo o por pérdidas económicas no se presenten, para aquello es necesario un análisis de guías más eficaces y controles que permitan

reaccionar ante incidentes que afecten al hardware, software y elementos complementarios o datos críticos dentro de la infraestructura de las Tecnologías de la Información.

1.2. Descripción del Proyecto

Este proyecto consiste en evaluar riesgos y plantear un plan de recuperación ante desastres informáticos basado en metodologías establecidas y normas internacionales, con el objetivo de brindar procedimientos detallados a seguir, logrando recuperar los sistemas que estuvieran afectados. El personal que labora en el departamento de TIC's, en el área de redes e infraestructura, donde se encuentra el centro de datos de la UPSE, serán los principales actores responsables que participarán directamente en la realización del proyecto.

Durante el desarrollo del plan se pretende utilizar metodologías y estándares precisos para consolidar el objetivo propuesto considerando los dominios de control correspondientes a la serie ISO/IEC 27002:2013 orientados a satisfacer necesidades puntualizadas en los sistemas de información que determinen una evaluación formal de riesgos y una aplicación formal de códigos de prácticas relacionados con técnicas específicas de seguridad.

La seguridad dentro de este estándar se define en tres aspectos: la confidencialidad, la integridad y la disponibilidad que deben asumir los sistemas computacionales en caso de que sea necesario. La aplicación de la metodología Magerit versión 3.0 facilitará la identificación de los activos de la institución al dividirlos en diferentes grupos con el fin de valorizar de forma amplia las amenazas y elaborar contramedidas específicas evitando la presencia de incidentes.

Dentro de este ámbito también es importante mencionar las Normas de Control Interno para el Sector Público del Ecuador, las normas del esquema nacional de seguridad y al instituto tecnológico Sans, porque contribuyen con guías generales agrupadas en áreas, sub-áreas y títulos, para la elaboración de procedimientos de seguridad relacionados a distintos fines, entre ellos al área de las tecnologías de la información, tratando de mantener siempre claro las necesidades del proyecto y la

importancia del uso de las mismas en el desarrollo de la solución propuesta. Para llevar a cabo el proyecto se debe tener presente el estudio de campo que se realizará mediante encuestas, entrevistas y visitas técnicas específicas para obtener resultados reales y significativos, y al mismo tiempo poder brindar soluciones con respecto al análisis y evaluación de los riegos mediante el uso de formularios precisos de los estándares escogidos.

1.3. Objetivos

1.3.1. Objetivo General

Elaborar un plan de contingencias orientado a las tecnologías de información mediante el uso de dominios de control y metodologías de análisis de riesgos basado en normas internacionales ISO.

1.3.2. Objetivos Específicos

Los objetivos específicos del proyecto se detallan a continuación:

- Identificar los riesgos que causen mayor impacto mediante la metodología Magerit que facilite la evaluación y la reducción de los mismos.
- Proponer procedimientos, guías o estrategias bajo normas para mantener la continuidad de las operaciones en el departamento de dirección de tecnologías de información y comunicación de la UPSE.
- Diseñar un plan emergente para la recuperación oportuna de incidentes que puedan suceder en el Centro de Datos de Tics de la UPSE.

1.4. Justificación

Hoy en día la Universidad Estatal Península de Santa Elena desea iniciar soluciones tecnológicas que permitan asegurar la integridad de la infraestructura de TI y sus operaciones, esto implica la existencia de factores de riesgo que afectan a los activos

debido a la forma de reaccionar frente a diversas amenazas a los que están expuestos a diario.

El objetivo de la solución tecnológica facilitará a la institución universitaria una documentación actualizada y efectiva como respuesta optima en caso de incidentes, catalogándolo como un instrumento de gestión para la administración de las TI, y servirá como herramienta fundamental para futuras auditorías informáticas, acciones legales y certificaciones internacionales que esté dispuesta a cumplir.

El proyecto ayudará a determinar acciones preventivas con la finalidad de recuperar y proteger la infraestructura tecnológica del centro de datos y comunicaciones de la UPSE. La base del plan de contingencia y su posterior recuperación, trata de establecer prioridades claras sobre qué tipo de procesos son los más esenciales. Los fallos técnicos y humanos permiten reconsiderar a las organizaciones que existe la necesidad de auxiliarse con herramientas que garanticen un eficaz giro a la regularidad ante la apariencia de un incidente, por tal razón, el diseñar un plan de contingencias no envuelve una afirmación en consideración a la ineficiencia en la gestión de la institución, sino al contrario, las medidas de seguridad protegen a la información y presume un importante progreso a la hora de superar todas aquellas adversidades que pueden provocar importantes pérdidas, no solo materiales sino también en la suspensión del centro de cómputo durante un período más o menos prolongado.

1.5. Resultados Esperados

Los resultados esperados dentro de este proyecto son los siguientes:

- Satisfacción en los usuarios por la eficiencia y eficacia al momento de reanudar las operaciones informáticas permitiendo la continuidad de la organización.

- Mitigación de posible materialización de amenazas y su impacto a las que pueda estar sometida la infraestructura del centro de datos y comunicaciones.

- Disponibilidad de documentación sobre un plan de contingencias como solución tecnológica al momento de incidencias presentadas.

- Mayor protección y fiabilidad de los activos de la información.

- Conocimientos sobre controles y salvaguardas para la recuperación de la infraestructura tecnológica aplicados tanto a los activos como al personal de la institución previniendo vulnerabilidades naturales y humanas.

- Mejor gestión de riesgos ayudando a mantener la información confiable y segura.

CAPÍTULO II

MARCO TEÓRICO

2.1. Marco Teórico

En este capítulo, se mencionan las diferentes definiciones, conceptos y elementos principales que constituyen la fundamentación teórica del proyecto tecnológico.

2.2. Fundamentación Teórica

2.2.1. Información (Datos)

La información es considerada un bien valioso o un activo muy importante dependiendo de su uso y propósito, debido a que está catalogada como un conjunto de datos procesados y organizados referente a algo en específico dentro de una institución, implicando la necesidad de estar protegida en todo momento de forma segura e impidiendo su mala manipulación. La información debe ser siempre gestionada correctamente para lograr obtener un nivel eficiente de confianza que aporte al crecimiento de la organización.

2.2.2. Seguridad de la Información

Consiste en la preservación de su confidencialidad, integridad y disponibilidad, así como de los sistemas implicados en su tratamiento, dentro de una organización [1].

De acuerdo con el marco de gestión global de las Tecnologías de Información de la organización **COBIT** (Objetivos de Control para Información y Tecnologías Relacionadas) [2], el conjunto de elementos importantes orientados específicamente a proveer condiciones seguras y confiables para que la seguridad de la información sea gestionada y certificada de forma adecuada en las instalaciones del centro de datos es:

- **EFECTIVIDAD:** se trata de lograr que la información sea en realidad la necesaria para desarrollar cualquiera de las tareas que se implanten en la organización y sea adecuada para realizar los procesos del negocio, proporcionándola de manera oportuna, correcta, consistente y accesible.
- **EFICIENCIA:** significa que la información sea procesada y generada utilizando de manera óptima los recursos que tiene la organización para este fin.
- **CONFIDENCIALIDAD:** se refiere a que, en todas las etapas del procesamiento de la información, ésta se encuentre protegida manteniéndose oculta o secreta contra accesos no autorizados, los cuales pueden derivar en la alteración o robo de información confidencial y no sea divulgada a personas, y tampoco a entidades no autorizadas.
- **INTEGRIDAD:** hace referencia a la preservación de tener la información intacta, exacta y completa, para no ocasionar la manipulación de la misma tanto de procesos y personas que no tienen autorización.
- **DISPONIBILIDAD**: característica relacionada con la disposición de quienes tienen acceso a la información, siendo estos todos los elementos autorizados en el momento en que así lo requieren.

Según el estándar ISO/IEC 27001, Las organizaciones y sus sistemas de información están expuestos a un número cada vez más elevado de amenazas que, aprovechando cualquiera de las vulnerabilidades existentes, pueden someter a activos críticos de información a diversas formas de fraude, espionaje, sabotaje o vandalismo [1].

La confidencialidad, integridad y disponibilidad de la información son elementos relevantes para proporcionar niveles elevados de competitividad y rentabilidad que determinen un excelente perfil profesional indispensable para alcanzar de forma segura los objetivos planteados, obteniendo beneficios económicos necesarios para la institución. Los elementos principales que constituyen un análisis de riesgos están relacionados con la magnitud de impactos y vulnerabilidades que pueden producirse en los activos de la información causando daños o pérdidas

significativas, y a la vez determinan la solución indicada a través de controles apropiados de seguridad que ayudarían a disminuir o evitar la ocurrencia masiva del riesgo. Debido a esto se considera a las amenazas como un impacto totalmente negativo y que conlleva a las autoridades competentes de las organizaciones a ejercer evaluaciones mediante la toma de decisiones definitivas para que los riesgos disminuyan a un nivel aceptable.

Figura 1 muestra las fases y los aspectos vitales en la gestión del riesgo. Sin embargo, un Sistema de Gestión de la Seguridad de la Información (SGSI) facilita la protección de activos implantando medidas, políticas y procedimientos de seguridad basados en minimizar riesgos en la organización.

Figura 1. Relación entre componentes de la gestión de riesgos y seguridad.
Fuente: www.iso27000.es.

2.2.3. Sistemas de información

Un sistema de información (SI) es un conjunto de elementos organizados, relacionados y coordinados entre sí, encargados de facilitar el funcionamiento global de una empresa o de cualquier otra actividad humana para conseguir sus objetivos [3].

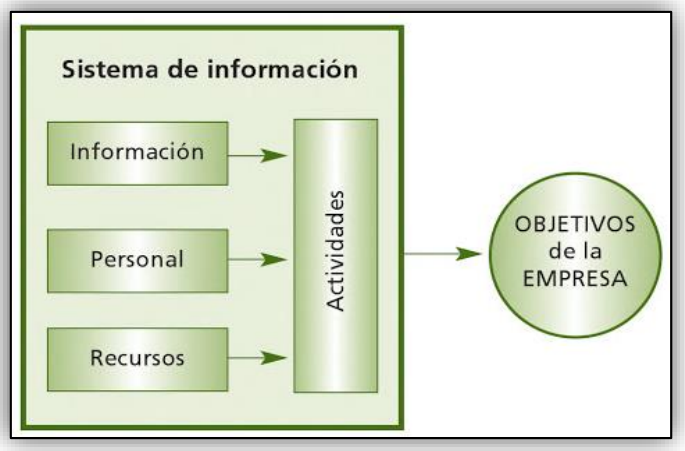


Figura 2. Elementos de un sistema de información.
Fuente: P. A. López, Seguridad informática.

2.2.4. Activos

Un activo es un componente o una parte de un sistema global al que la organización asigna un valor y, por tanto, que requiere protección [4].

Durante años y hoy en día, la información se ha convertido en el activo más importante que posee una organización. Dentro de los activos de la información pueden considerarse: las bases de datos, los manuales de usuarios y documentación de los sistemas, el software, el hardware y los servicios que estén involucrados con la administración de la información. En general un activo comprende a toda la información crítica o de alta validez que la institución posee dentro de un servidor informático.

2.2.5. Vulnerabilidad informática

Son aspectos que influyen negativamente en un activo y que posibilita la materialización de una amenaza [5].

Entendemos por vulnerabilidad, a la capacidad o a las condiciones que posee la entidad o sistema, de ser susceptible o débil de reaccionar ante cualquier amenaza siendo capaz de poder restablecerse y tolerar daños presentados.

Las vulnerabilidades se encuentran ligadas directamente a las amenazas, debido a que, si no existiera una amenaza, tampoco tendría lugar la vulnerabilidad, y no se producirían daños.

2.2.6. Amenazas

Una amenaza comprende una fuente efectiva de incidentes donde alguien o algo puede explotar una vulnerabilidad para obtener, modificar o impedir el acceso a un activo provocando reacciones graves que comprometan la información de la empresa [6].

Se las puede distinguir adecuadamente en dos grupos importantes que son: amenazas humanas y amenazas físicas o desastres naturales existentes en un centro de datos y comunicaciones. Una vez determinado que una amenaza podría perjudicar a un activo, es necesario estimar cuan vulnerable es dicho activo tomando en cuenta dos sentidos: Primero la degradación, que hace referencia a cuan perjudicado resultaría el activo, segundo la frecuencia, que significa cada cuanto se materializa la amenaza [7].

Para mejor entendimiento del tema se detallan a continuación la clasificación general de las amenazas.

2.2.6.1. Amenazas Humanas

- **Amenazas Internas**: suelen ser más complejas, porque son creadas por usuarios que saben del funcionamiento de la red y la ubicación de la información. Además, los usuarios mantienen un alto nivel de acceso por motivos de trabajo para la operación de datos de interés. En este caso, los sistemas de prevención de intrusos y firewalls no resultan eficaces por no estar orientados al tráfico interno.

- **Amenazas Externas:** son amenazas generadas fuera de la red. El usuario responsable de la amenaza realiza ataques externos con el fin de conocer la

información de la misma, sin embargo, esto puede ser solucionado por el administrador de la red encargándose de prevenirlas en gran medida.

Estas amenazas son también conocidas como amenazas deliberadas o intencionadas porque son ejecutadas siempre por la acción humana, entre estas tenemos:

- ✓ Robo o hurtos.
- ✓ Fraude, introducción de software malicioso (malware, virus), hacking, atentado, divulgación de información, sabotaje o alteración de datos).

2.2.6.2. Amenazas Físicas (Desastres Naturales)

Son amenazas o coacciones producidas por sucesos naturales o debido a fallos técnicos, y por incidentes que indirectamente suelen ocasionarse por la intervención humana.

Estas amenazas son también conocidas como amenazas accidentales y dentro de los ejemplos de estas amenazas tenemos los siguientes:

- ✓ Inundaciones, sismos, incendios.
- ✓ Sobrecargas de energía eléctrica, falta de corriente, presencia de polvo, mal funcionamiento de un equipo eléctrico, de red, o informático o funcionamiento incorrecto de un software (sistemas operativos).

2.2.7. Riesgo informático

Se denomina riesgo a la posibilidad de que se materialice o no una amenaza aprovechando una vulnerabilidad [8].

Los activos de la información si no son adecuadamente protegidos están sujetos a una alta probabilidad de amenazas que daría como resultado el desencadenamiento de fatales consecuencias en un centro de cómputo. Consideramos riesgos informáticos a fraudes internos y externos realizados por medio de los sistemas de información. Dentro de los riesgos relacionados con la informática, existen áreas

principales que deben ser protegidas en los centros de datos, tales como: la seguridad física y del entorno, la seguridad en controles de accesos, la protección de datos y la seguridad en la Red y seguridad lógica.

Existen factores agravantes de riesgo relacionados con el negocio de la empresa como las infraestructuras, servicios y aplicaciones mal protegidas o un plan de contingencia o de recuperación inexistente o no implementado [6].

2.2.8. Análisis de riesgos informáticos

El análisis de riesgo informático hace referencia al proceso y a las metodologías utilizadas para poder estimar de manera eficiente la magnitud de los riesgos a los que se expone una organización [9].

Este análisis conlleva a la identificación de amenazas a los que se encuentran expuestos los activos tecnológicos, también a la probabilidad de ocurrencia, al efecto e impacto potencial o residual de los riesgos con el objetivo de proponer controles necesarios para disminuirlos, gestionarlos, evitar su descontrolada y pronta aparición.

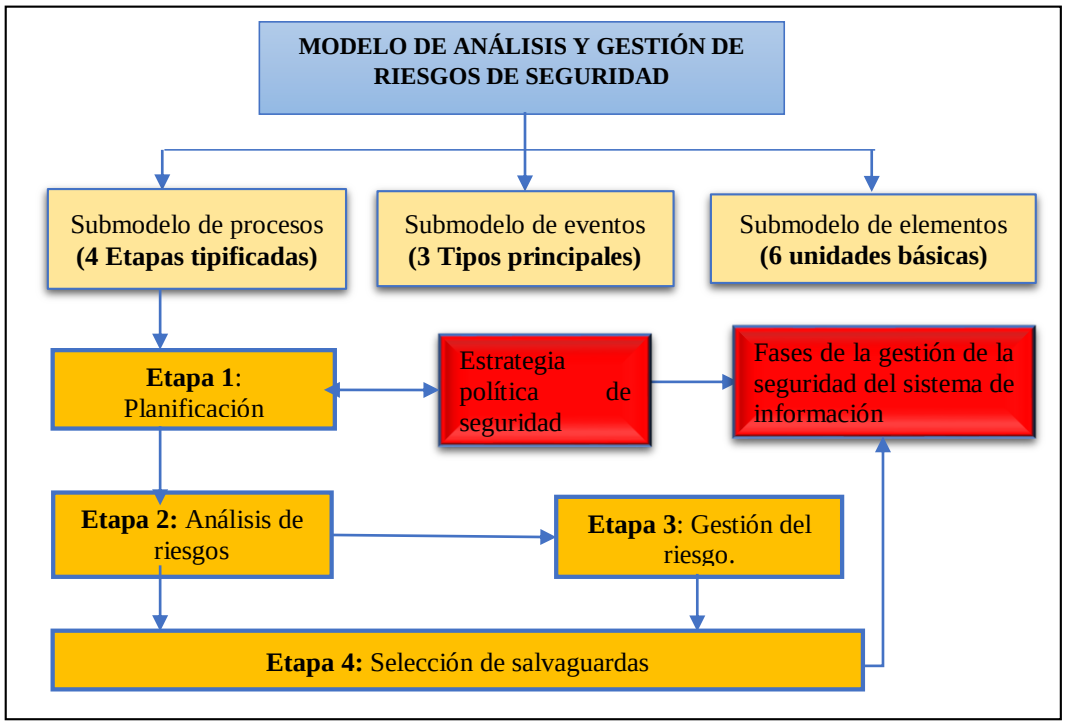


Figura 3. Proceso de evaluación de riesgos de la seguridad de la informacion.
Fuente: J y Bertolìn, Seguridad de la informacion.

Durante este proceso se desarrollan técnicas específicas para su implementación proporcionando habitualmente un documento denominado matriz de riesgos, según la metodología Magerit v3 [10], menciona algunos aspectos a seguir para la gestión de riesgos de los sistemas de información:

- Segmentación de los activos de información a identificar en grupos.
- Determinación los tipos de activos de la institución mediante fichas o matrices específicas.
- Elaboración de dimensiones y criterios adecuados para la valoración correspondiente de los activos.
- Diseño de matrices para identificar amenazas sobre los sistemas de información.
- Desarrollo de controles, estrategias o salvaguardas de seguridad para la mitigación de riesgos.

2.2.9. Impacto

Son la consecuencia de la materialización de una o más amenazas sobre uno o varios activos aprovechando la vulnerabilidad del sistema o, dicho de otra manera, el daño causado [8].

Según la gravedad y la magnitud los impactos pueden ser desastrosos, independientemente del tipo de incidente o vulnerabilidad, es necesario evaluar el impacto en los activos informáticos para conocer el nivel de daño causado por un riesgo. Por ende, las amenazas, incidentes e impactos, se catalogan en términos claves a considerar al momento de priorizar medidas de seguridad para la corrección de activos.

2.2.10. Gestión de Riesgos informáticos

El proceso de gestión del riesgo informático está basado en el uso de políticas, códigos de buenas prácticas y normas para garantizar la corrección de eventos que

hacen vulnerables a los activos, reduciendo las amenazas y el impacto que podrían causar con la finalidad de proporcionar un correcto funcionamiento y administración del centro de datos y comunicaciones de la UPSE. Durante este proceso de desarrollo se considerarán las fases ideales y correspondientes que permitirán el adecuado control de los riesgos informáticos y amenazas tanto naturales y como humanas, las mismas que se atribuyen como razón principal del proyecto. La idea primordial es elaborar un documento completo que establezca una matriz de riesgos indispensable para la adecuada gestión de los recursos de la institución relacionada con los niveles de impacto o gravedad y los niveles de probabilidad de ocurrencia de eventualidades peligrosas.

2.3. Metodología MAGERIT versión 3

La metodología Magerit será la herramienta indicada que se utilizará en el desarrollo del proyecto, su uso es específicamente para el análisis y gestión de los riesgos que podrían presentarse en los sistemas de información dentro del centro de datos de la Universidad Estatal Península de Santa Elena. Esta metodología se basa estrictamente en minimizar la aparición de riesgos, incidentes o amenazas y obtener un buen uso de las tecnologías de la Información.

El modelo normativo de magerit se apoya en algunos Submodelo: el Submodelo de procesos será la descripción funcional del proyecto de seguridad a construir; mientras que el Submodelo de elementos proporciona los componentes y atributos relacionados entre sí: activos, amenazas, impactos, riesgos, salvaguardas (Funciones, Servicios y mecanismos) [11].

2.3.1. Introducción

Hoy en día las organizaciones manejan grandes volúmenes de información totalmente relevante a través de equipos necesarios para su transmisión, causando que exista la presencia de riesgos muy peligrosos que provocarían grandes pérdidas económicas en cualquier momento. La seguridad informática es la encargada de

resguardar, proteger o salvaguardar los recursos computacionales en base a los objetivos de la institución, de manera que es fundamental la aplicación de políticas, que ayuden en construir entornos o sistemas más seguros. Existen diferentes metodologías que pueden ser aplicadas en el análisis de riesgos informáticos. Las más utilizadas son las siguientes:

- Metodología Magerit V3
- Metodología Octave
- Normativa ISO 27001
- Risk IT de ISACA
- Metodología NIST SP 800-30
- Metodología CORAS

Magerit es un método formal destinado exclusivamente a cualquier administración de carácter público que requiera realizar una investigación de riesgos a los sistemas de información, además de la elaboración de controles de seguridad apropiados que controlen aquellos riesgos. Es elemental la evaluación del riesgo porque permite elaborar planes de seguridad y de contingencia dentro de la institución y gestionar los posibles ataques a la información.

2.3.2. Magerit versión 3

MAGERIT es un instrumento para facilitar la implantación y aplicación del esquema nacional de seguridad proporcionando los principios básicos y requisitos mínimos para la protección adecuada de la información [12].

Esta metodología es elaborada por el Consejo Superior de Administración Electrónica (CSAE), se basa generalmente en estudiar el impacto que pueden generar las amenazas en una organización, obteniendo una visión mejorada sobre las estrategias preventivas y correctivas apropiadas para el correcto funcionamiento de las tecnologías de Información. Magerit busca dividir los activos informáticos en distintos grupos para llevar a cabo la identificación eficiente de los riesgos y dar lugar a un tratamiento o mitigación de los mismos en base a contramedidas.

El proceso de evaluación es importante para generar los posibles planes de contingencias con la finalidad de documentar, gestionar, proteger los datos, la información, los equipos y los servicios prestados de ataques intencionados. La metodología ayuda a crear un proceso de gestión y establece un marco de trabajo competente para facilitar la toma de decisiones considerando los riesgos en las TI.

La metodología Magerit ofrece las siguientes ventajas:

- Brinda un método sistemático adecuado para formalizar el análisis de riesgos que surge de la utilización de las tecnologías de información y comunicación Tic's.
- Planifica el tratamiento de mitigación adecuado para llevar el control de los riesgos, evitando, disminuyendo y aceptando las amenazas ocasionadas.
- Puede ser aplicada para organismos gubernamentales, compañías grandes y pequeñas, medianas empresas, comerciales y no comerciales, de forma manual o por medio de una herramienta de información lógica para el análisis y gestión de riesgos "PILAR".
- Favorece a la preparación de riesgos del proceso de apreciación en cuanto a auditorias, certificaciones o acreditaciones según sea el caso en cada organización.

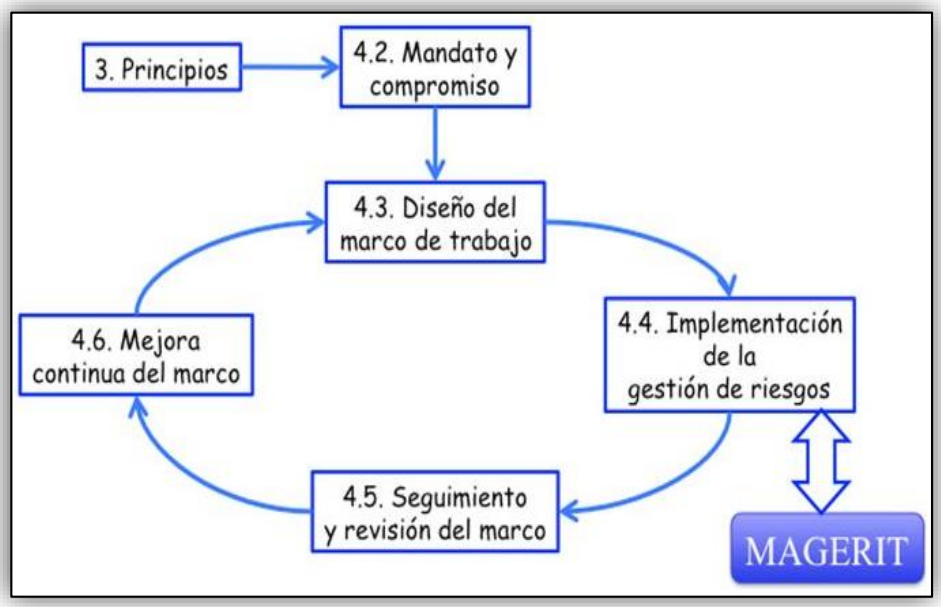


Figura 4. Diseño de análisis y gestión de riesgos.
Fuente. (Amutio Gómez & Candau) MAGERIT V3 Libro I: Método.

2.3.3. Objetivos de Magerit

La magerit v3 es una de las metodologías más utilizadas porque propone cumplir los objetivos directos e indirectos importantes que toda organización debe conocer. Los objetivos mencionados a continuación son extraídos del libro magerit versión 3 volumen 1 [10].

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

2.3.4. Volúmenes o manuales de Magerit

Magerit presenta una guía completa de métodos donde se especifica la forma de cómo llevar a cabo el análisis de riesgos. Se encuentra divida en tres libros o volúmenes con una información completa y precisa.

- **Libro I:** Método
- **Libro II:** Catálogo de Elementos
- **Libro III:** Guía de Técnicas

2.3.4.1. Libro I: Método

El primero de ellos hace referencia al Método, donde se describe la estructura que debe tener el modelo de gestión de riesgos [13].

En este volumen se mencionan los métodos, procesos y proyectos correspondientes al análisis de riesgos para el desarrollo de los sistemas de información, relacionándose específicamente a lo que propone ISO para la gestión de riesgos.

2.3.4.2. Libro II: Catálogo de Elementos

Según la metodología Magerit v3, el catálogo de elementos es una especie de inventario que puede utilizar la empresa para enfocar el análisis de riesgo [13].

Los inventarios que este catálogo incluye están relacionados con: tipos de activos, dimensiones y criterios de valoración, clasificación de las amenazas, salvaguardas e interpretación de informes sobre riesgos obtenidos. Los objetivos a sugerirse son extraídos del libro de magerit versión 3 volumen 2 [14].

- Facilitar la labor de las personas que acometen el proyecto, en el sentido de ofrecerles ítem estándar a los que puedan adscribirse rápidamente, centrándose en lo específico del sistema objeto del análisis.
- Homogeneizar los resultados de los análisis, promoviendo una terminología y unos criterios que permitan comparar e incluso integrar análisis realizados por diferentes equipos.

2.3.4.3. Libro III: Guía de Técnicas

El tercer libro manifiesta una extensa guía de técnicas a utilizar en las diferentes etapas del análisis marcando la diferencia entre otras metodologías, debido a su buen contenido en la elaboración de proyectos.

Dentro de las técnicas específicas de análisis se mencionan: Manejo de tablas para la recopilación adecuada de resultados, aplicación de algoritmos cualitativos y cuantitativos para determinar los tipos de amenazas producidas en un sistema de información, técnicas gráficas y buenas prácticas para llevar adelante las sesiones de trabajo para el análisis de los mismos.

2.3.5. Técnicas para análisis de riesgos

El análisis de riesgos es una aproximación metódica para implementar políticas de seguridad en un sistema, por eso es preciso la determinación de pasos lógicos pautados en el libro I de Magerit [10].

- Fijar los activos relevantes, su interrelación y su valor, en el sentido de qué perjuicio supondría su degradación.

- Establecer a qué amenazas están expuestos aquellos activos.

- Determinar qué salvaguardas hay dispuestas y cuán eficaces son frente al riesgo.

- Estimar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza.

- Valorar el riesgo, definido como el impacto ponderado con la tasa de ocurrencia (o expectativa de materialización) de la amenaza.

La importancia de seguir un método de análisis resulta favorable porque provee las técnicas de gestión necesarias para mantener protegidos todos los activos informáticos y propone la continuidad de la organización libre de amenazas durante el transcurso de operatividad del mismo. Las técnicas utilizadas durante el proceso están sujetas a los objetivos de la institución, favoreciendo las decisiones indicadas para sobrellevar un mejor funcionamiento de los servicios tecnológicos.

2.3.6. Documentación del Proceso (Informes)

Esta documentación es indispensable para el proceso de adquisición de la información y realización del proyecto de análisis, determinando el desarrollo de informes puntualizados que reflejen mejor la información obtenida y los resultados esperados.

2.3.6.1. Documentación Intermedia

La documentación intermedia a realizarse en el proceso está relacionada con:

- Realizar documentación auxiliar que contenga el análisis funcional, manuales, organigramas y especificaciones de datos según las necesidades de la organización.

- Desarrollar informes de las entrevistas realizadas a las autoridades indicadas para la recolección de información detallando los resultados obtenidos.

- Extraer documentación de otras fuentes: como información estadística, observaciones de expertos y observaciones de los analistas.

- Utilizar la información existente para el proyecto tecnológico considerando asuntos importantes como: inventario de activos.

2.3.6.2. Documentación Final

Los informes a presentarse en la evaluación de riesgos son los siguientes:

- **Modelo de Valor:** Informe para detallar de forma adecuada el proceso de definición e identificación de todos los activos informáticos encontrados en el centro de datos del departamento de tecnologías de información.

- **Mapa de riesgos:** Informe para detallar las amenazas a las que están expuestos los activos, evaluando significativamente los riesgos encontrados para obtener resultados óptimos.

- **Evaluación de salvaguardas:** Informe que despliegue de acuerdo al riesgo existente o resultados obtenidos por el proceso, la evaluación eficaz de las salvaguardas o medidas de seguridad a tomarse para el tratamiento del riesgo, considerando aspectos relevantes como: protección de salvaguardas y eficacia de las mismas.

- **Estado de riesgo:** Informe de caracterización de los activos por su riesgo residual; asumiendo lo que podría proporcionarse al considerar las salvaguardas o medidas desarrolladas para la seguridad.

2.3.7. Proyectos de análisis de riesgos

Los proyectos relacionados con este análisis serán elaborados por primera vez y serán iniciados bajo un estudio de recursos y una planificación de actividades teniendo en consideración todo lo necesario en formalizar algunas tareas para que el proyecto llegue a buen término.

Las actividades que son organizadas para el funcionamiento del proceso de gestión de riesgos son analizadas de forma periódica debido a lo importante que significa mantenerlas al día. Los aspectos a seguir para la finalización exitosa de este proyecto son:

- **Parte 1:** Acciones previas o preliminares.
- **Parte 2:** Preparación y elaboración completa de análisis de riesgos.
- **Parte 3:** Notificación de resultados conseguidos.

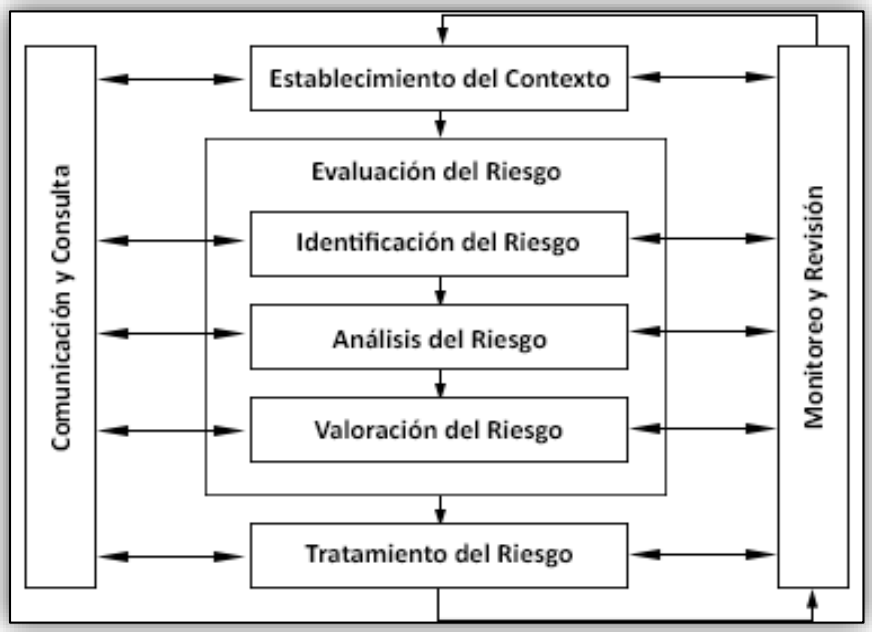


Figura 5. Enfoque general del proceso de gestión de riesgos. Fuente: ISO 31000.

2.3.7.1. Plan de seguridad

En esta etapa se manifiesta la forma de cómo llevar a cabo planes de seguridad adecuados por medio de decisiones acogidas para el tratamiento de los riesgos. Dichos planes están conformados por actividades para la elaboración de programas, diseños y cronogramas que permitan ejecutar los proyectos de seguridad. Se identifican 3 fases para este proceso:

- **PS.1 Identificación de proyectos de seguridad**: se detalla acciones sobre la elaboración de conjuntos de programas de seguridad, servicios y resultados de actividades.

- **PS.2 Plan de ejecución:** se establece el tiempo determinado de los programas de seguridad, diseñando cronogramas de ejecución.

- **PS.3 Ejecución**: se obtiene o consigue los resultados de los objetivos pronosticados que se elaboran para cada proyecto de seguridad.

2.4. Generalidades para plan de contingencias

La determinación de un modelo de desarrollo para un plan de contingencias dependerá en gran medida de la infraestructura y de los servicios de la organización, en realidad no existe un modelo único para todos, sin embargo, lo ideal es procurar construir ciertos puntos más significativos para la creación del plan.

2.4.1. Plan de Contingencia

Se denomina plan de contingencia o también conocido como plan de recuperación de desastres o de continuación de negocios, a la definición de acciones a realizar, recursos a utilizar y personal a emplear en caso de producirse un acontecimiento intencionado o accidental que degrade los recursos informáticos o de transmisión de datos de una organización [15].

El plan de contingencias permite ejecutar un conjunto de procedimientos, y acciones básicas como respuestas para enfrentar antes, durante o después de la presencia de incidentes o eventos de emergencia causados por fenómenos naturales o por el hombre.

Una organización institucional debe contar con un plan de contingencias actualizado y basado en un análisis de riesgos oportuno que permita contar con la transferencia, eliminación, aceptación o mitigación de los riesgos dependiendo de la frecuencia y el nivel de impacto generado. Este plan de seguridad debe mantenerse actualizado de forma periódica para detectar y eliminar futuros problemas.

2.4.2. Contenido o Subplanes

Un plan de contingencias está conformado especialmente por tres Subplanes y que comprenden medidas, acciones o actividades necesarias que enfrenten la materialización de amenazas en cada tiempo, debido a esto el documento de contingencia que será desarrollado deberá contener algunos planes que manifiesten las actividades diferentes apropiadas para cada evento de riesgo. Los planes a implementarse son:

- **Plan de respaldo:** comprende contramedidas preventivas para evitar que la amenaza llegue a materializarse.

- **Plan de emergencia:** comprende contramedidas importantes durante la presencia de amenazas, o después de estas, tratando de mitigar los efectos producidos por la materialización.

- **Plan de recuperación:** comprende medidas indispensables después de materializada y reconocida la amenaza, la finalidad es restaurar el estado de las cosas como se encontraban antes de que se diera la amenaza.

Las contramedidas sugeridas para la creación del plan de contingencias pueden ser de las siguientes:

- Medidas Técnicas.
- Medidas Organizativas.
- Medidas Humanas.

2.4.3. Tipos de contingencias

Las contingencias o eventualidades negativas se presentan principalmente dependiendo de los prejuicios y de acuerdo al tiempo producido. Los tipos de contingencias se pueden clasificar en:

- **Menor:** son contingencias que poseen repercusiones solo en las operaciones diarias y pueden ser recuperadas en un tiempo menor a 8 horas.

- **Grave:** son contingencias que afectan a las instalaciones con daños, pero pueden regresar a la funcionalidad de sus operaciones en un tiempo menor a 24 horas.

- **Crítica:** son contingencias que afectan a las operaciones y a las instalaciones, no son recuperables en corto tiempo, y pueden suceder por la falta de normas preventivas o bien porque estas no son suficientes. Dentro de las eventualidades categorizadas como críticas se encuentran exclusivamente: los terremotos, incendios, inundaciones, son especialmente los desastres naturales.

2.5. Políticas de Seguridad de la Información

En general, una política de seguridad define las directrices que deben ser permitidas y prohibidas en un sistema de información [16].

El propósito principal de una política de seguridad es informar a los usuarios y al personal de la organización en general sobre los requisitos obligatorios a cumplir por cada uno de ellos para proteger los valores tecnológicos y la información de la organización [17].

Para obtener un adecuado y correcto manejo de la información para el centro de datos y comunicaciones de la UPSE es necesario la disposición y el uso de políticas bien elaboradas que generen información concreta y precisa a nivel de seguridad.

Es realmente importante conocer y considerar normativas internacionales reconocidas como: estándares ISO o las normas de control interno para instituciones públicas del Ecuador que brindan aspectos, requisitos y técnicas para la implantación de un correcto sistema de gestión de seguridad de la información facilitando un nivel de certificación en la institución.

Las Políticas de Seguridad Informática (PSI), surgen como una herramienta organizacional para concientizar a cada uno de los miembros de una organización sobre la importancia y sensibilidad de la información y servicios críticos [18].

2.5.1. Descripción de la norma 27001

Es la norma principal de la serie y contiene los requisitos del sistema de gestión de seguridad de la información [19].

Esta normativa fue elegida por que ofrece la oportunidad de adquirir certificaciones en el ámbito de la seguridad de la información, motivo por el cual sus requerimientos pueden ser implementados en el centro de datos de la universidad. La principal función de esta normativa se centra en indagar los problemas que puedan afectar a la información para brindar un tratamiento sistemático mediante políticas o procedimientos tanto a organizaciones públicas como privadas consiguiendo que los usuarios confíen en la protección de los datos.

Para la protección de la información se requiere de la mejora e implementación de las medidas de seguridad como impulso a que la institución logre sus objetivos y garantice el cumplimiento de la norma a un nivel superior, consiguiendo legalizar la información y permitir el crecimiento favorable del centro de datos de la UPSE en relación con el ámbito profesional de calidad.

La nueva estructura ISO/IEC 27001:2013 está alineada a un ciclo de mejora continua, al modificarse el contenido que conforman los controles del “Anexo A”,

aumentando el número total de dominios de 11 a 14 y reduciendo el número de controles de 133 a 113 debido a un proceso de incorporación, fusión y sustracción de nuevos controles de seguridad.

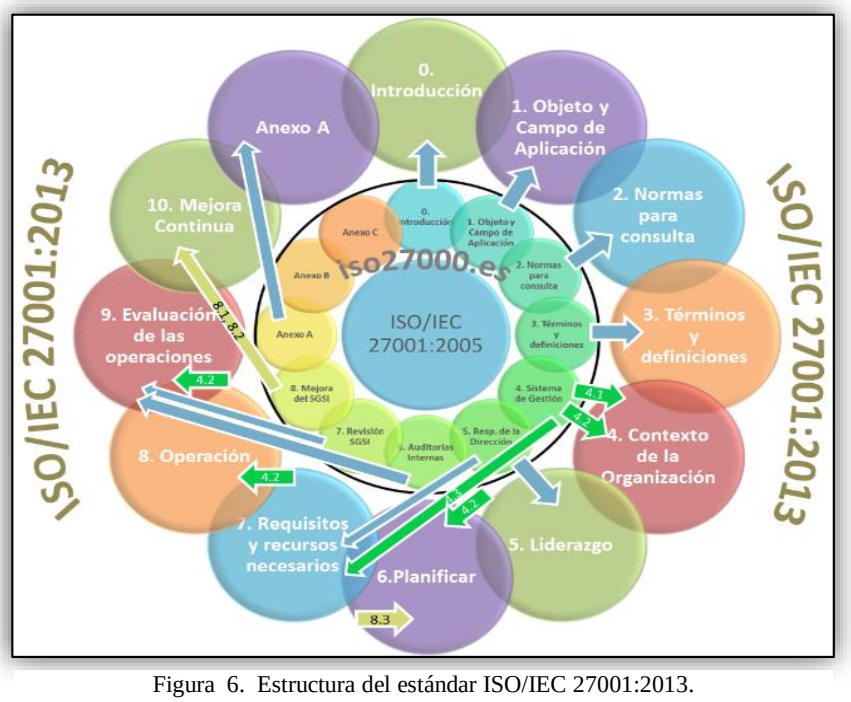


Figura 6. Estructura del estándar ISO/IEC 27001:2013.
Fuente: http://www.iso27000.es/iso27000.html.

2.5.2. Descripción de la norma 27002

La implementación de este estándar para el departamento de Tic's servirá para lograr la aplicación de controles, objetivos y directrices en especial guías de buenas prácticas que gestionen y reduzcan los niveles de probabilidad de incidentes otorgando verdadera protección en la seguridad física y lógica de la institución con la intención de alcanzar una gestión administrativa de calidad. El contenido de la norma está desarrollado bajo dos organizaciones: (ISO) "International Organization for Standardization." y (IEC) "International Electrotécnicas Commission.", encargados de áreas con respecto a la tecnología de la información logrando reducir las amenazas y adoptando un nivel de seguridad aceptable.

La selección de los controles depende de decisiones de la organización sobre la base de los criterios de aceptación del riesgo, las opciones de tratamiento del riesgo y el enfoque general de gestión de riesgos aplicado a la organización, y también debe

estar sujeta a todas las leyes y regulaciones nacionales e internacionales relevantes [20].

La Figura 7 especifica la última edición del año 2013 de este estándar, actualizado a un total 14 Dominios, 35 Objetivos de control y 114 Controles de seguridad, certificando un conjunto de categorías de seguridad principales para la protección de los servicios informáticos.

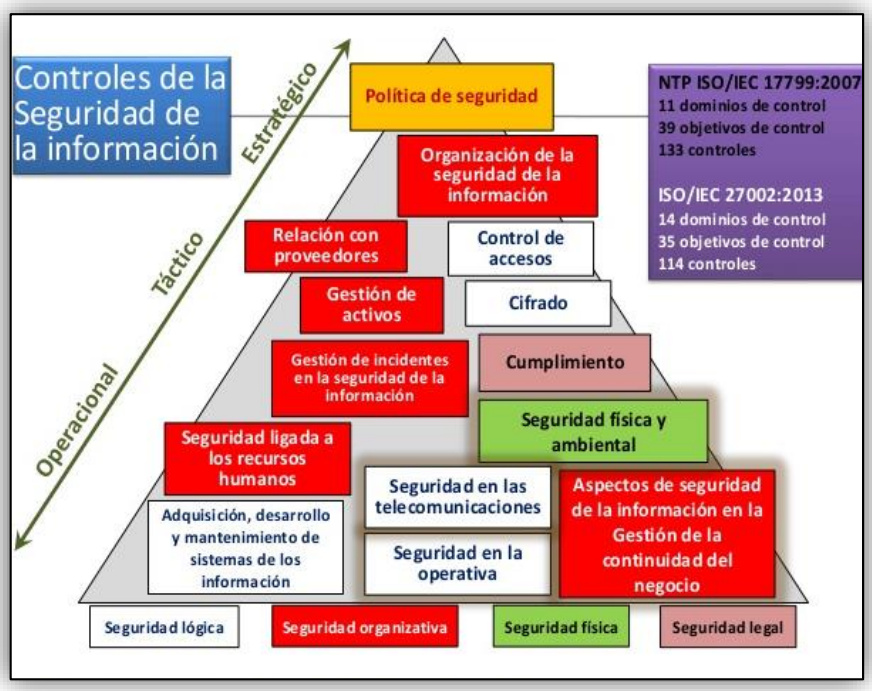


Figura 7. Estructura del Estándar ISO/IEC 27002:2013.
Fuente: www.iso27001security.com.

2.5.3. Normas de Control Interno - República del Ecuador

Las normas de control interno están dirigidas al Sector Público de la República del Ecuador y establecen guías generales emitidos por la contraloría general del estado. Esta norma tiene el objetivo de mantener un buen control de los recursos públicos y se enfoca en obtener una seguridad razonable haciendo que las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos puedan lograr los objetivos propuestos bajo un marco legal y normativa técnica pertinente.

El uso de estos controles internos para el proyecto se centra en la responsabilidad máxima de la institución, por eso es indispensable la posibilidad de crear condiciones aptas para ejercer dicho control.

Las normas internas de la contraloría general del estado consideradas para el desarrollo de planes de contingencias informáticos están manifestadas necesariamente mediante artículos relacionados con la normativa **COBIT** que se ajusten a las tecnologías de la Información mantenida por la Asociación Internacional de Auditoria y Control de Sistemas de Información (**ISACA**):

- **Normativa 410-11 Plan de Contingencias**: Corresponde a la unidad de tecnología de información la definición, aprobación e implementación de un plan de contingencias que describa las acciones a tomar en caso de una emergencia o suspensión en el procesamiento de la información por problemas en los equipos, programas o personal relacionado [21].

2.5.4. Instituto de seguridad de la información (SANS)

Es la fuente más grande y confiable en proveer una buena certificación de seguridad de la información en el mundo. Este instituto brinda diferentes temas, políticas o controles disponibles en las tecnologías avanzadas, redactadas por excelentes especialistas en el ámbito de Sistemas, Auditoria, Redes y Seguridad. Cabe mencionar que Sans está encargado indispensablemente en desarrollar, mantener, actualizar y poner a disposición la mayor serie de documentos de investigación sin costo alguno.

Esta institución orientada a la seguridad de la información ofrece además una certificación a través de GIAC, filial del Instituto SANS, que es un organismo de certificación que brinda más de 20 aspectos tecnológicos e incluye certificaciones técnicas en seguridad de la información, y programas de grado opcional a través del Instituto de Tecnología SANS, así como numerosos recursos de seguridad gratuitos, incluyendo boletines de noticias, documentos técnicos y transmisiones por Internet [22].

Figura 8. Instituto de Auditoria, Redes y Seguridad.
Fuente: https://www.sans.org/.

Los recursos de SANS Security Policy tienen como objetivo principal conceder plantillas y herramientas necesarias aproximadamente para 27 aspectos relacionados con el desarrollo e implementación de políticas de seguridad informática.

Según SANS, Una política es típicamente un documento que describe los requisitos o reglas específicas que se deben cumplir [23].

Los recursos de esta organización fueron escogidos principalmente para la elaboración del plan de contingencia informático dirigido a la dirección de TI de la universidad. Esta documentación presentará un conjunto de estrategias reformadas y renovadas acorde a las necesidades reflejadas en los resultados del obtenidos del análisis de riesgos. Entre las herramientas Sans más comunes que fueron utilizadas para la creación de políticas se distinguen las plantillas de directivas:

- Directivas General de seguridad de la información.
- Directivas de seguridad de la red.
- Directivas para Gestión de la continuidad del negocio.

Para la utilización y aplicación de estos recursos no existe ningún costo debido a que los miembros del consenso están reunidos en ayudar a personas que asisten a programas de formación SANS, debido a eso está información resulta ser de fácil acceso.

CAPÍTULO III

MARCO CONCEPTUAL

3.1. Problematización

En este capítulo se identifica la problemática del proyecto y se determina la metodología de investigación y técnicas para recopilación de la información.

La problematización dentro de este proyecto tecnológico consiste en realizar pensamientos, actitudes he indagaciones históricos - críticas sobre algún tema en particular con la finalidad de plantear dudas, haciendo inseguro lo dado por seguro y llegando a comprender el cómo y el por qué algo se convierte en indudable e incuestionable.

3.2. Identificación del problema

Debido al constante crecimiento tecnológico y de sus aplicaciones, a niveles de infraestructura física, a la cantidad de riesgos analizados tanto humanos y naturales, resulta importante gestionar los inconvenientes graves que amenazan los servicios tecnológicos del centro de datos. Esto origina que sea necesario contar con mejores prácticas que deben ser aplicadas para enfrentar incidentes que pongan en riesgo la información. La institución no posee medidas preventivas adecuadas, por tal motivo se plantea determinar las mejores comunidades que brinden soluciones óptimas para la reducción de riesgos informáticos encontrados, entre aquellas se destacan los recursos Sans, los mismos que recopilan información sobre todo lo referente a la seguridad informática gracias a profesionales como administradores de sistemas, universitarios, consultores y auditores, todos especializados en áreas críticas referentes a la tecnología. De la misma forma estándares como la norma ISO 27002, normas de control interno de la república del Ecuador ajustadas al área de las tecnologías de información han sido de gran ayuda para la gestión de la seguridad de la misma.

Este proyecto tecnológico también busca proteger la seguridad física del entorno y establecer un ambiente seguro de las áreas del centro cómputo en la institución, debido a eso es preciso analizar el estándar BS 7799 versión 2 que brinda mejores prácticas referentes a la seguridad de equipos y al área física para las tecnologías de información otorgando confiabilidad por estar incorporada y adoptada por la norma ISO 27001. Es importante mencionar que, para la realización del proyecto, el uso de varias metodologías permite mejorar la calidad de la evaluación, razón por la cual el uso de Magerit como metodología principal proporcionara un buen proceso general de análisis de las amenazas. Sin embargo, existen también otras metodologías apropias que favorecen la aplicación de técnicas para valoración, estimación y medición de matrices y estados de riesgos potenciales y residuales mediante métodos de evaluación y respuesta.

3.3. Actores del proyecto

Los actores principales que colaboraron para la obtención y recopilación de la información y los que forman parte del proyecto son directamente el personal encargado del centro de datos y comunicaciones, específicamente del Área de Redes e Infraestructura. En la tabla 1 se encuentra detallado todo el personal de TI.

INFORMANTES	CANTIDAD
Director de TIC	1
Jefe de Desarrollo de Software	1
Programadores	2
Jefe de Redes e Infraestructura	1
Coordinador de Mantenimiento de Hardware	1
Técnico en Hardware y Aplicaciones	1
Técnico en Electrónica	1
Técnico de Soporte al Usuario	1
TOTAL	**9**

Tabla 1. Población del proyecto tecnológico.

3.4. Metodología de la Investigación

La metodología de la investigación tiene como propósito exponer los elementos indispensables para la búsqueda, recopilación e interpretación de los datos, lo cual es de vital importancia para el desarrollo del proyecto.

3.4.1. Tipos de Investigación

Para el presente proyecto tecnológico "Evaluación de riesgos y desarrollo de un plan de recuperación ante desastres informáticos aplicada al centro de datos de la UPSE", la metodología utilizada está basada en una investigación diagnóstica, con la finalidad de definir y resolver problemas, generar respuestas o conocimientos científicos, estudiar las relaciones entre factores y acontecimientos mediante el conjunto de técnicas y procedimientos. Las principales características del diagnóstico, son la observación crítica, la descripción y la selección de sus prioridades. La observación es un aspecto clave para todo proyecto, con esto se puede obtener mayor cantidad de información y registrarla para su posterior análisis.

Para el análisis e interpretación de los resultados, serán de utilidad también los siguientes métodos:

- Investigación de campo.
- Investigación documental.

Mediante estos métodos fue posible obtener una recopilación adecuada de los datos permitiendo sugerir y orientar soluciones a los problemas encontrados.

3.4.2. Investigación de Campo

La investigación de campo es aquella que consiste en la recolección de datos directamente de los sujetos investigados, o de la realidad donde ocurren los hechos datos primarios, sin manipular o controlar variable alguna, es decir, el investigador obtiene la información, pero no altera las condiciones existentes [24, p. 13].

Las técnicas de investigación de campo establecidas para la recolección de información primaria están relacionadas con la observación, la entrevista y la encuesta.

3.4.3. Técnicas de recolección de datos

Las técnicas de recolección de información elegidas indican las instrucciones particulares para la generación de los datos mediante las cuales fue posible la obtención de informaciones confiables y válidas para ser utilizadas en el proceso de evaluación de los riesgos aproximando los resultados a la realidad.

La función más indicada y primordial de estas técnicas fue el uso de la observación y la exploración de anomalías para la generación de modelos cualitativos y cuantitativos que permitieron medir la situación actual de la universidad.

Entre los procedimientos realizados para la recolección de datos dentro del departamento de tecnologías de información se mencionan los siguientes:

- Preparación del material apropiado para la construcción de entrevistas exclusivas al Jefe de dirección de TIC's, al Jefe del Área de Redes e infraestructura, y al Jefe del Área de desarrollo de sistemas de la UPSE mediante investigaciones previas de los posibles riesgos informáticos.
- Realización de visitas técnicas para observar de forma concisa el estado de funcionamiento del hardware, software, servicios e infraestructura del centro de cómputo y de las oficinas de TI.
- Procesamiento y análisis de la información recolectada sobre amenazas y vulnerabilidades informáticas sin introducir distorsiones que afecten la interpretación de los datos.

3.4.3.1. Observación

Consiste en la percepción del hecho o fenómeno [25, p. 20]. La observación es una de las técnicas de investigación que se realiza por medio de los sentidos ya sean

por medio de datos visuales y auditivos, productos del tacto y el olfato; la cual favoreció en la recopilación de datos empíricos del proyecto tecnológico.

3.4.3.2. Entrevista

La entrevista es un intercambio verbal, que nos ayuda a reunir datos durante un encuentro, de carácter privado y cordial, donde una persona se dirige a otra y cuenta su historia, da su versión de los hechos y responde a preguntas relacionadas con un problema específico [26].

La entrevista abierta a profundidad ejercida al director de TI, Ing. Wellington Robys, MSIA, fue realizada mediante una plática entre el auditor informático y el informante, generalmente el auditor emplea la entrevista a todas las personas claves para colaborar con la obtención de mayor información para la investigación.

La observación y las entrevistas permitieron ampliar los conocimientos adquiridos de forma concreta y certera en cuanto al proyecto tecnológico, logrando plantear las conclusiones adecuadas mediante hechos estrictamente estudiados en el campo, descartando de esta forma opiniones subjetivas.

Finalmente, los resultados de las entrevistas correspondientes al análisis de riesgos dirigidas al director de TI, al Jefe de Redes e Infraestructura y al Jefe de Desarrollo de Software por motivos de verificación de riesgos en los sistemas de información pueden visualizarse en el **Anexo 1.**

3.4.4. Recursos para levantamiento de información

Los recursos o materiales utilizados para el levantamiento de información de acuerdo al análisis del proyecto fueron:

- Metodología Magerit version3 para la elaboración de análisis y gestión de los riesgos, considerando los siguientes aspectos: Formas de Metodología, tablas de categorización de activos, tablas de categorización de amenazas y la aplicación de procedimientos indicados para el tratamiento de riesgos.

- Guías técnicas para la medición y evaluación de riesgos.
- Fichas e informes de controles ISO 27002 / ISO 27001 actualizados aptos para la seguridad de la información.
- Documentos de investigación de la seguridad de la información facilitados por organizaciones como: Sans, Isaca, Centro Criptológico Nacional (CCN) del estado español, Contraloría general del estado, portales oficiales de organismos internacionales de normalización, entre otros.
- Computador personal, lápiz, carpetas, herramienta de Microsoft (Excel) para interpretación de información.
- Cámara fotográfica digital y servicio de internet.

3.4.5. Investigación Documental

La investigación documental es un proceso basado en la búsqueda, recuperación, análisis, crítica e interpretación de datos secundarios, es decir los obtenidos y registrados por otros investigadores en fuentes documentales: impresas, audiovisuales o electrónicas [24, p. 12].

Las técnicas de investigación documental para recopilar información, podrían ser las siguientes:

- Investigación Bibliográfica (libros, periódicos).
- Investigación hemerográfica (artículos y revistas).
- Investigación archivista (encuestas y conferencias escritas).
- Documentos Fílmicos (películas, diapositivas, fílmicas).
- Documentos grabados (discos, cintas).
- Documentos Electrónicos (páginas web).

Gracias a las técnicas de investigación documental fue posible la recolección de información relevante, obteniéndose resultados coherentes bajo el uso de procedimientos lógicos que facilitaron al proceso de desarrollo del proyecto mediante: el análisis y la síntesis de la información.

CAPÍTULO IV

DESARROLLO DEL ANÁLISIS DE RIESGOS PARA EL CENTRO DE DATOS "UPSE"

4.1. Situación Actual del departamento de Dirección de TIC's

Según la web documental: "Dirección de TIC's", el departamento de Dirección de Tecnologías de Información y Telecomunicación tiene bajo su responsabilidad la optimización informática institucional, la coordinación de las jefaturas que dependen de ella, la automatización de los diversos ámbitos del quehacer institucional, siempre con criterios de usabilidad, eficiencia y eficacia.

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

Está conformada por las siguientes áreas:

- **Área de Infraestructura:** Departamento encargado de promover, gestionar e implementar soluciones informáticas pertinentes sobre equipamiento tecnológico o hardware manteniendo la colaboración de la dirección de TIC's a nivel institucional.

- **Área de Desarrollo:** Departamento encargado de planificar, coordinar, controlar, desarrollar, diseñar y supervisar todas las tareas involucradas con el diseño, desarrollo y mantenimiento de software de los sistemas de información a nivel institucional, así como también las herramientas de programación utilizadas en el proceso.

- **Soporte al Usuario:** Departamento que se encarga de proveer la atención inmediata y eficiente a todos los usuarios de la plataforma informática institucional de la universidad con el fin de suministrar indispensables soluciones tecnológicas.

4.2. Organigrama Estructural de la dirección de TIC's

Según el documento: "Manual de Puestos", de la Dirección de tecnologías de la información y comunicación, a cargo del Director de TI el Ingeniero Wellington Robys MSIA, muestra en la figura 9, el organigrama estructural actualizado donde detalla cómo está distribuido el departamento en cuanto a niveles jerárquicos o cargos profesionales.

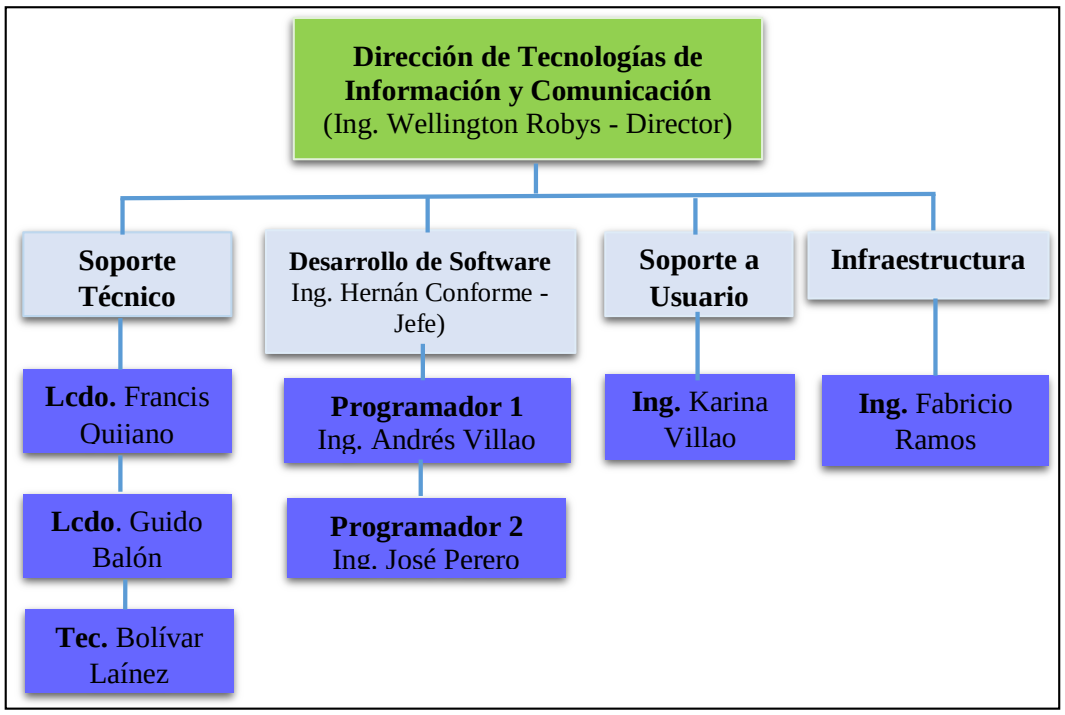


Figura 9. Organigrama estructural actual de la dirección de TI, actualizado al 2017.

4.3.Diagrama actual de red de datos

La Figura 10 muestra de manera general el diagrama de red de datos actual de la Universidad y adicional a eso el equipamiento Core conformado por dispositivos y equipos de comunicación, proveedores de internet y medios de transmisión (Fibra Óptica y Cable UTP) implementados en los diferentes sectores de institución para brindar el correcto funcionamiento de los servicios existentes para la comunidad universitaria. Es necesario mencionar que en los puntos de conexión de cada edificio están instalados Switches de 8, 12, 24, y 48 Puertos, así como también antenas y routers para red inalámbrica.

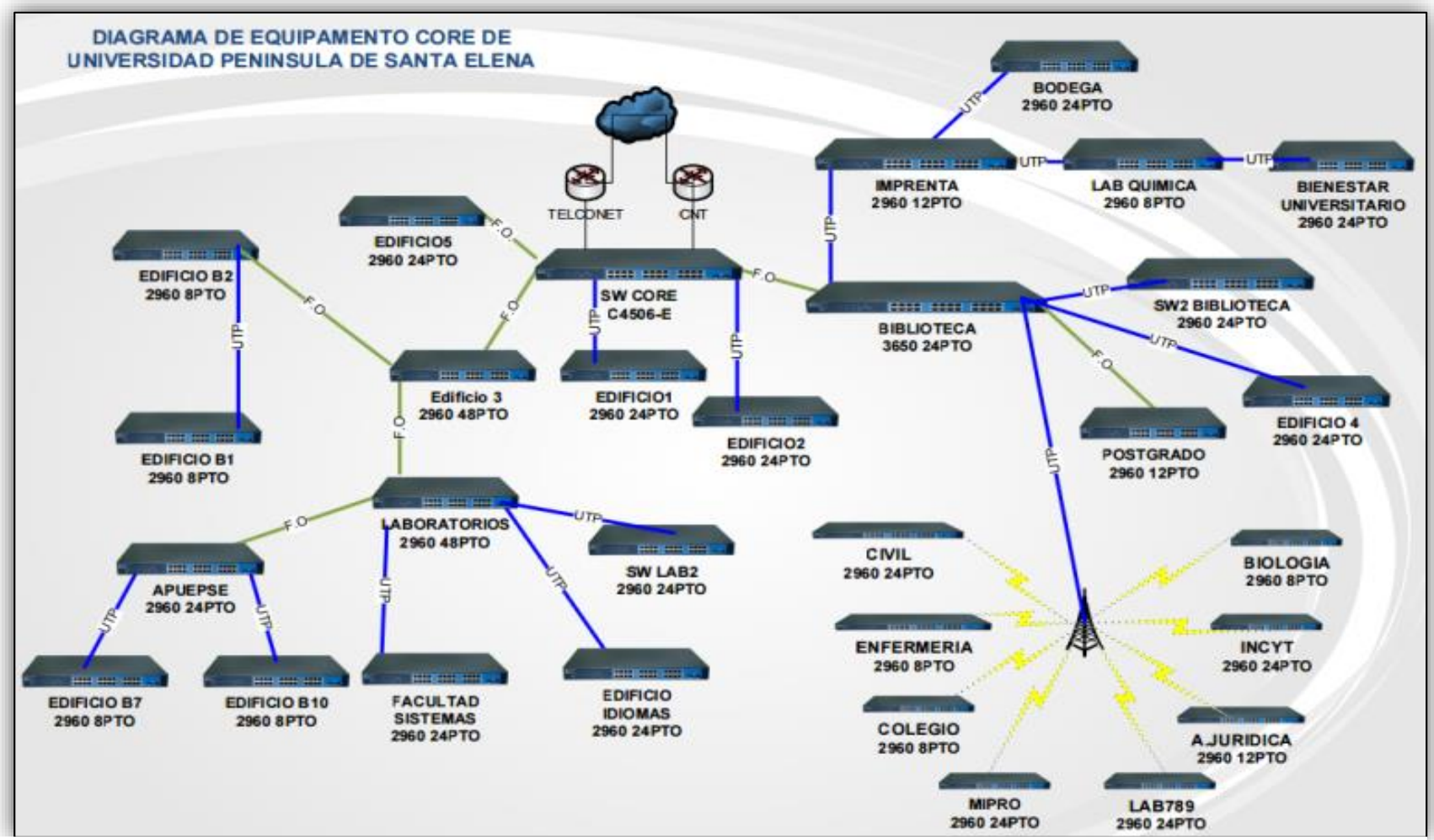


Figura 10. Diagrama actual de equipamiento Core de UPSE 2016.

4.4. Diagrama del Centro de Datos

Esquema actual de la comunicación del centro de datos a nivel lógico. Se puede ver en Figura 11.

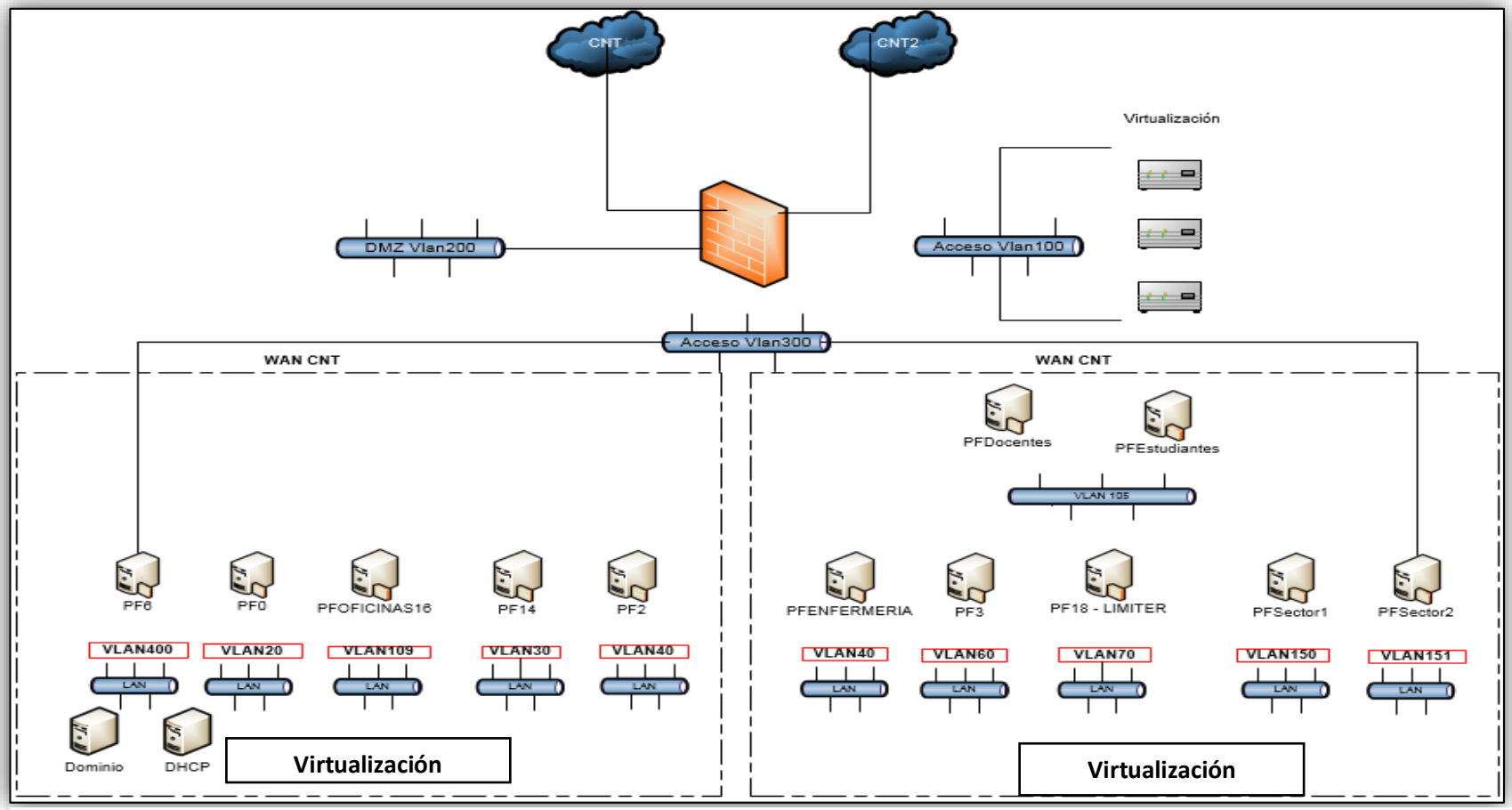


Figura 11. Esquema lógico de comunicación del centro de datos 2016.

4.5. Servicios Funcionales de la dirección de TIC's

Según la web documental: Dirección de TIC's, el departamento de Tecnologías de la Información y Comunicación proporciona los siguientes servicios:

- Correo Electrónico Institucional.
- Desarrollo de aplicaciones
- Asistencia a usuarios
- Servicios Web.
- Intranet
- Internet.
- Protección sobre accesos no autorizados mediante Firewall.
- Seguridad informática.
- Instalación y Mantenimiento del Cableado Estructurado.
- Redes Inalámbricas
- Mantenimiento Preventivo y Correctivo a los equipos de cómputo
- Instalación, configuración y mantenimiento de Software
- Asesorías a Estudiantes y Profesores

4.6. Análisis de riesgos

En esta etapa el punto principal es contribuir en la utilización de la metodología Magerit para evaluar los riesgos obteniendo una mayor validez y eficiencia en el desarrollo del proyecto.

En toda organización comúnmente los activos están sujetos a constantes riesgos producidos por diferentes factores que determinan un entorno totalmente inseguro, por lo tanto, los responsables de las TI deben estar atentos a estas situaciones emergentes evitando pérdidas en los activos y deben facilitar el correcto funcionamiento de los mismos. Para el cumplimiento de esta fase fueron realizadas entrevistas, encuestas y visitas técnicas a los usuarios importantes de los sistemas, herramientas tecnológicas y equipos que ayudaron en la recopilación de información del dentro del centro de datos de la UPSE.

4.6.1. Caracterización de los activos

Esta actividad tiene como objetivo identificar y clasificar los activos que conforman los sistemas de información dentro de la institución, definir su valoración mediante las dimensiones de seguridad establecidas y determinar las dependencias entre ellos.

4.6.1.1. Identificación de los Activos

El activo primordial es la información o datos que integran los sistemas, pero también existen otros activos que se identifican con los datos y MAGERIT diferencia los activos y los agrupa en varios tipos de acuerdo a la función que ejercen en el tratamiento de la información [27].

La tabla 2, especifica detalladamente los tipos de activos clasificados por magerit.

Tipos de activos	Descripción
Servicios	Son los que se necesitan para la gestión de los datos.
Software	Herramientas que permiten manejar los datos.
Hardware	Equipos informáticos que permiten alojar datos, servicios y aplicaciones.
Comunicaciones	Redes y dispositivos que permiten transmitir e intercambiar datos.
Soportes de Información	Son los encargados del almacenamiento de la Información.
Equipamiento Auxiliar	Son complementos necesarios para los elementos informáticos.
Instalaciones	Infraestructura donde se instalan los sistemas de información y comunicaciones.
Personal	Personas encargadas del manejo, administración y control de los sistemas de información.

Tabla 2. Listado de tipos de activos.

4.6.1.2. [S] Servicios

La institución ofrece o presta a los usuarios internos los siguientes servicios que se muestran en la tabla 3. Se pretende implementar para el siguiente año: Cámaras IP y Telefonía IP.

<table>
<tr><td colspan="3">Servicios Internos</td><td colspan="2">[ST_UPSE] Soporte Técnico</td></tr>
<tr><td colspan="3"></td><td colspan="2">[INTERNET_UPSE] Internet</td></tr>
<tr><td colspan="5">SOPORTE TÉCNICO</td></tr>
<tr><td colspan="3" rowspan="4">Asistencia a Usuarios</td><td colspan="2">Soporte Aplicativo</td></tr>
<tr><td colspan="2">Soporte de Hardware</td></tr>
<tr><td colspan="2">Soporte de Sistemas de Información</td></tr>
<tr><td colspan="2">Soporte de Redes de Comunicación</td></tr>
<tr><td colspan="5">SERVICIO DE INTERNET</td></tr>
<tr><td>ISP</td><td>Conexión</td><td>Ancho de Banda</td><td>Cant./ Usuarios</td><td>Servicios / ISP</td></tr>
<tr><td rowspan="2">CNT</td><td>Fibra Óptica</td><td>Servicio de 70 Megas (Laboratorios, y Red Inalámbrica), pero se pretende extender a 100 Megas.</td><td rowspan="2">Usuarios Internos 3000 U. aprox.</td><td rowspan="2">- Correo Electrónico (Nube Office 365).
- Sistemas Académicos y de Información. (Estudiantes, docentes, área académica).
- Aula Virtual.
- Red inalámbrica.
- Servicios de Páginas Web.
- Bibliotecas Virtuales.
- Soporte Informático.</td></tr>
<tr><td>Fibra Óptica</td><td>Servicio de 30 Megas (Oficinas “Usuarios Administrativos”) , pero se pretende extender a 45 Megas</td></tr>
</table>

Tabla 3. Servicios internos y soporte informático.

4.6.1.3. [SW] Software - Aplicaciones Informáticas

Los múltiples aplicativos, programas o desarrollos que maneja el centro de datos de la UPSE se detallan en la tabla 4.

Software	**[SI_UPSE]** Sistemas Informáticos
	[OFFICE_UPSE] Ofimática
	[AV_UPSE] Anti virus
	[SO_UPSE] Sistema Operativo
	[HYPERVISOR_UPSE] Gestor de máquinas virtuales
	[OTR_UPSE] Otros Software

Tabla 4. Software y aplicaciones informáticas.

Listado de Sistemas Informáticos Vigentes

Los sistemas informáticos se consideran en dos ámbitos dentro de la Dirección de TIC's:

- **Académicos y Administrativos. -** los cuales se clasifican en Sistemas Web y Sistemas de Escritorio.
- **Los sistemas web. -** están desarrollados en lenguaje de programación PHP, con framework JQuery, Javascript, Ajax.
- **Los sistemas de escritorio. -** están desarrollados en lenguaje Visual Basic y Visual .Net.

Los sistemas informáticos producidos por el área de desarrollo del departamento en la tabla 5.

Sistemas Informáticos Vigentes	**Descripción**
SISTEMAS WEB	
• Registro de Calificaciones	Sistema para docentes donde se ingresan las calificaciones
• Control de Planes de Clase	Sistema para docentes donde registran el plan analítico y los planes de clases.
• Actividades de Personal Académico	Sistema administrativo, donde los docentes registran sus actividades complementarías

• Seguimiento a Graduados	Sistema administrativo, donde se visualizan información de seguimiento a graduados
• Gestión y Control Planificación Institucional	Sistema administrativo de Planificación institucional
• Recursos Humanos	Sistema administrativo de la unidad de Talento Humano
• Secretaria General	Sistema administrativo de actas de secretaria general
• Relaciones Externas	Sistema administrativo, de la unidad de Relaciones externas, Relex.
• Servicios Académicos	Aplicación de matriculación en línea, consultas de notas para estudiantes
• Sistema de Encuestas	Aplicación administrativo para la realización de fichas de encuestas
• Evaluación a Docentes	Aplicación para estudiantes donde realizan la evaluación a los docentes
• Intranet	Sistema administrativo, para consultas de la academia.
• Accesos a Bibliotecas Virtuales	Aplicación de accesos a Bibliotecas Virtuales
SISTEMAS DE ESCRITORIO	**Descripción**
• Sistema Académico de secretarias	Sistema académico, para matriculación de estudiantes, módulos autofinanciados, etc.
• Sistema de Egresados y Graduados	Sistema administrativo para el registro de egresados y graduados
• Sistema de recaudaciones	Sistema administrativo, para el registro de las recaudaciones de tesorería
• Sistema de Planificación docente	Sistema académico, para el registro del distributivo docente
• Sistema de Biblioteca	Sistema administrativo para la gestión de Biblioteca Upse.

Tabla 5. Listado de los sistemas informáticos vigentes.

- **Ofimática:** La institución cuenta con las siguientes herramientas de ofimática:
    - Herramientas de Microsoft (Paquetes completos).
    - Versiones desde Office 2010 hasta Office 365.
    - Microsoft Office 365 para correo electrónico institucional en teléfonos y PC.
    - Todos los programas de ofimática tienen buena compatibilidad.

- **Antivirus:** Para protección de estaciones de trabajo o equipos informáticos utilizan:
    - Deep Freeze Versión 7. como herramienta de análisis y protección de archivos.
    - Plan de mantenimiento cada 6 meses

- **Sistemas Operativos:** Los sistemas operativos y las licencias de software con los que cuenta la institución se especifican en la siguiente tabla 6 y tabla 7 respectivamente.

LICENCIAS DE SOFTWARE		
Nombre	**Licencia**	**Descripción**
Windows, Office	Licencia Microsoft	Convenio con "Campus Agreement"
Centos, Fedora, FreeBSD, PFSense, VMWare.	GNU Software Libre	Open Source, VMWare (Virtualización.)
Visual Basic 6.0	Licencia Microsoft	Herramientas de Programación
Visual Net 2005	Licencia Microsoft	Herramientas de Programación
Aptana y Eclipse	Software Libre	Herramientas de Programación
SQL Server	Licencia Microsoft	Herramientas de Motor de BD.

Tabla 6. Licencias de software de sistemas operativos y herramientas.

SISTEMAS OPERATIVOS				
PC / (Oficinas)				
Nombre	**S.O.**	**Bits**	**Versión**	**Licencia**
Windows	Windows	64 bits	Versión 7 en adelante.	Licencia Microsoft
SERVIDORES				
Nombre	**S.O.**	**Bits**	**Versión**	**Licencia**
Centos	Linux	64 bits	Versión 7	Open Source
Fedora	Linux	64 bits	Versión 12	Open Source
Free BSD. PFSense	Linux	64 bits	Versión 2.3	Open Source
Windows Server	Microsoft	64 bits	Versión 2012	Licencia Microsoft
VMWare (Virtualización)	Linux	64 bits	Versión 6	VMWare

Tabla 7. Sistemas operativos existentes para servidores.

4.6.1.4. [HW] Equipamiento Informático (hardware)

El Data center del departamento de TIC's contiene servidores con respectivas características que están especificados en la tabla 9:

Hardware	**[SERV_UPSE]** Servidores
	[VHOST_UPSE] Equipo Virtual
	[BACKUP_UPSE] Equipamiento de Respaldo
	[MID_UPSE] Equipos medios / computadores
	[PERIPHERAL_UPSE] Periféricos **[PRINT_UPSE]** Medios de Impresión **[SCAN_UPSE]** Escáneres
	[NETWORK_UPSE] Soporte de la red
	[MODEM_UPSE] Módems **[SWITCH_UPSE]** Switches **[ROUTER_UPSE]** Routers **[BRIDGE_UPSE]** Antenas **[FIREWALL_UPSE]** Firewalls

Tabla 8. Equipamiento informático o hardware.

SERVIDORES				
Servidor	**RAM**	**Disco Duro**	**Marca /Modelo**	**Descripción**
Principal	2,3,4,5,8	100 GB 5 TB	HP Blade c3000	Nodos de Virtualización
Principal	2,3,4,5,8	100 GB 5 TB	HP Proliant DL380	Nodos de Virtualización
Servidor BD	8	15 TB	HP DL380	En torre, conexión con arreglo de discos de 15 Tb.

Tabla 9. Lista de servidores y especificaciones técnicas.

- **Equipo de Respaldo:** Las características del servidor de respaldo del centro de datos y el funcionamiento en copias de seguridad son:
    - Equipo de respaldo clonado con capacidad de 2TB y 4 GB.
    - No se hacen respaldos completos, sola se respalda la "Data" de cada máquina virtual.
    - Las copias de seguridad se realizan de forma automática y la periodicidad es dependiendo de los sistemas.
    - Respaldos Diarios: BD de Sistemas Académicos, Aulas Virtuales, Sistemas Críticos.
    - Respaldos mensuales: Páginas Web, etc. (semanales).
    - La información es respaldada en discos duros con una capacidad de almacenamiento de 2 TB.

- **Equipos Informáticos:** La institución cuenta con equipos informáticos para oficinas.
    - PC oficinas: Marca HP, Disco duro 500 GB a 1 TB, Core 2 Duo, Windows 7 y 8.
    - Laptops: Marcas HP, Dell, Toshiba y Mac, 500 GB a 1 TB, Core i3 hasta Core i7, Windows 7 y 8.

- **Equipos de Red:** Los dispositivos de comunicación con los que cuenta el centro de datos se refieren específicamente a encaminadores, conmutadores y antenas, los mismos que se definen a continuación:

SWITCH CISCO CATALYST 4500 – Switch Principal (DATASHET)	
 Figura 12. Dispositivo de conmutación Catalyst 4500. Fuente: www.cisco.com	
Producto	**Descripción**
Sistema	
Sistema de Base	El flujo de aire de adelante hacia atrás
Módulo de expansión	8x10 + GE SFP / SFP - C4KX-NM-8SFP +
Puerto de gestión	10/100/1000 Base-T
Puerto USB	Tipo A (almacenamiento y arranque) hasta a 4 GB
Fuente de alimentación dual	Sí
Escalabilidad	
Rendimiento del sistema	Hasta 800 Gbps
Enrutamiento IPv4 en hardware	Hasta 250 Mpps
Enrutamiento IPv6 en el hardware	Hasta 125 Mpps
L2 puente en el hardware	Hasta 250 Mpps
Media Access Control (MAC)	55K
VLAN totales	4094
Alta Disponibilidad y Flexibilidad	
VSS Throughput	Hasta 1,6 Tbps
Virtual Switch Link	1GE o 10GE
Número máximo de interruptor de enlaces virtuales	8
CPU y Memoria	
Memoria (SRAM DDR-II)	4GB
Los tampones de puerto	32 MB
UPC	Dual Core 1.5 GHz
NVRAM	2 GB
Memoria externa opcional.	2 GB
Seguridad	
Seguridad portuaria	Sí
Extensiones y 802.1x IEEE 802.1x	Sí
VLAN, router, y el puerto de ACL	Sí

Virtualización	
Escalabilidad VRF-Lite	64
Fácil de Red Virtual (EVN)	32
Multidifusión, soporte	Sí
Administración basada en web	Sí

Tabla 10. Especificaciones técnicas de switch cisco 4500. Fuente: Ficha Técnica creado por Icecat.

SWITCH
CISCO CATALYST 3650 – (DATASHET)

Figura 13. Dispositivo de conmutación Catalyst 3650.
Fuente: www.cisco.com

Producto	**Descripción**
Puertos e Interfaces	
Puertos RJ-45 Ethernet	Gigabit Ethernet (10/100/1000)
Cantidad de puertos RJ-45 Ethernet	24
SFP module slots quantity	4
Peso y dimensiones	
Altura y Ancho	4,4 cm y 44,5 cm
Control de energía	
Consumo energético	64,18 W
Número de fuentes de alimentación	1
Frecuencia de entrada AC	50/60 Hz
Voltaje de entrada AC	100-240 V
Condiciones ambientales	
Intervalo de humedad relativa	5 - 96%
Intervalo de temperatura operativa	-5 - 50 °C
Red	
Bidireccional completo (Full dúplex)	Sí
Estándares de red	IEEE 802.1D, 802.1p, 802.1Q, 802.1s, 802.1w, 802.1x, 802.3, 802.3ab, 802.3ad, 802.3af, 802.3at, 802.3u, 802.3x, 802.3z
DHCP, servidor	Sí
Ruteo de IP y IGMP	Sí
Soporte VLAN	Sí

Transmisión de datos	
Tabla de direcciones MAC	32000 entradas
Capacidad de conmutación	88 Gbit/s
Número de VLANs	4094
Seguridad	
Lista de Control de Acceso (ACL)	Sí
Otras características	
Ancho de banda	160 Gbit/s
Montaje en rack	Sí
Alimentación a través de Ethernet (PoE)	
Energía sobre Ethernet (PoE), soporte	Sí
Alimentación mediante Ethernet Plus (PoE +) Cantidad de puertos	24
Desempeño	
Memoria interna	4096 MB
Memoria Flash	2000 MB
Tipo de memoria	DRAM
Apilable	Sí

Tabla 11. Especificaciones técnicas de switch cisco 3650. Fuente: Ficha Técnica creada por Icecat.

SWITCH **CISCO CATALYST 2960 – (DATASHET)**	
	
Figura 14. Dispositivo de conmutación Catalyst 2960. Fuente: www.cisco.com.	
Puertos e Interfaces	
Tecnología de cableado ethernet	100BASE-T, 10BASE-T
Cantidad de puertos Fast Ethernet	24
Cantidad de puertos SFP	2
Puertos tipo básico de conmutación RJ-45 Ethernet	Fast Ethernet (10/100)
Cantidad de puertos de conmutación RJ-45 Ethernet	24

Control de energía	
Consumo energético	22 W
Frecuencia de entrada AC	50/60 Hz
Voltaje de entrada AC	100-240 V
Condiciones ambientales	
Intervalo de humedad relativa	10 - 85%
Intervalo de temperatura operativa	-5 - 45 °C
Red	
Estándares de red	IEEE 802.1D, 802.1Q, 802.1p, 802.1s, 802.1w, 802.1x, 802.3, 802.3ab, 802.3ad, 802.3af, 802.3u, 802.3x, 802.3z
Control de transmisión de tormentas	Sí
DHCP, servidor, Ruteo de IP, IGMP	Sí
Auto MDI / MDI-X y Soporte VLAN	Sí
Transmisión de datos	
Tabla de direcciones MAC	8000 entradas
Jumbo Frames, soporte	Sí
Número de VLANs	255
Rendimiento	6,5 Mpps
Seguridad	
MAC, filtro de direcciones	Sí
Soporte SSH/SSL	Sí
Características de administración	
Calidad de servicio (QoS) soporte, multidifusión.	Sí
Diseño	
Montaje en rack	Sí
Desempeño	
Memoria interna	64 MB
Tiempo medio entre fallos	403745 h
Memoria Flash	32 MB
Nivel de ruido	40 Db

Tabla 12. Especificaciones técnicas de switch cisco 2960. Fuente: Ficha Técnica creada por Icecat.

ROUTER
CISCO ROUTER 1900 – "Se encargan de proveer el internet"

Figura 15. Dispositivo enrutador modelo 1900.
Fuente: www.cisco.com.

CARACTERÍSTICAS

- 2 y 1 unidades RU con un máximo de 2 puertos GE integrados WAN
- Hasta 1 Módulo de Servicios Integrados (ISM)
- Hasta 11 puertos de switch LAN, dos ranuras para tarjetas de interfaz WAN de alta velocidad mejoradas acelerada por hardware DES, 3DES y AES de IPSec y SSL VPN
- 802.11a/g/n punto de acceso integrado con 802.11i, WPA y WPA2 para la seguridad
- 16 VLANs inalámbricas y 15 SSIDs
- Optimización WAN a través WAAS exprés
- Acceso a la nube segura con prevención de intrusiones integrado, filtrado de contenidos y seguridad web cloud.
- Soportan 120 Gbit/s de transmisión.

Tabla 13. Especificaciones técnicas de router cisco 1900.

ANTENAS	
UNIFI - WIFI- AP OUTDOOR – (DATASHET)	

Figura 16. Antena UniFi AP-Outdoor.
Fuente: www.ubnt.com.

Frecuencia	5GHz

Rendimiento de 2,4 GHz	N/A
5GHz Throughput	300Mbps
Distancia	183m
UNIFI - WIFI- LR – (DATASHET)	

Figura 17. Antena UniFi LR.
Fuente: www.ubnt.com.

Frecuencia	Frecuencia
Rendimiento de 2,4 GHz	Rendimiento de 2,4 GHz
5GHz Throughput	5GHz Throughput
Distancia	Distancia
UNIFI - WIFI- AP PRO – (DATASHET)	

Figura 18. Antena UniFi AP-PRO.
Fuente: www.ubnt.com.

Frecuencia	2.4 GHz,5 GHz
Rendimiento de 2,4 GHz	450Mpbs
5GHz Throughput	300Mbps
Distancia	122m
UBIQUITI - RE-ENLACE- NanoStation – (DATASHET)	

Figura 19. Antena UniFi NanoStation.
Fuente: www.ubnt.com.

Marca	UBIQUITI Networks
Series	NanoStation M5
Peso del producto	399 g
Dimensiones del producto	3 x 29,2 x 8,1 cm
Capacidad de la memoria RAM	32 MB
Tipo de conexión inalámbrica	5.8 GHz Radio Frequency
Número de puertos ethernet	2
Voltaje	24 voltios
Potencia eléctrica	8 vatios
5 GHz	Sí
Distancia de Funcionamiento Máximo	15000 m
Energía sobre Ethernet (PoE	Si
Estándares de red	IEEE 802.3u
Ethernet LAN (RJ-45) cantidad de puertos	2
Ethernet LAN, velocidad de transferencia/datos	10,100 Mbit/s
Frecuencia de banda	4.9 - 5.9
Ganancia de la antena (Max)	16 dBi

Tabla 14. Especificaciones técnicas de antenas wifi-re-enlace.

4.6.1.5. [COM] Redes de Comunicaciones

A partir de los medios de transporte de información tenemos los tipos de redes. Las mencionamos a continuación:

Comunicaciones	**[LAN_UPSE]** Red Local
	[WIFI_UPSE] Red Inalámbrica
	[RADIO_UPSE] Comunicaciones radio
	[INTERNET_UPSE] Internet

Tabla 15. Tipo de redes de comunicación de datos.

- **Redes de comunicación de datos:** Las características principales sobre las redes de datos existentes en la institución se mencionan en los diversos aspectos:
    - **Segmentación de red LAN:** Red Wireless, Red de Laboratorios, Red de Docentes, Red de Rectorado, Red de Oficinas Administrativas, Red de Servidores.

- **Topología de Red:** Estrella.
- **Capacidad de transmisión:** En base a los equipos de comunicación (1 Gbit/s).
- **Medio de transmisión**: Fibra Óptica, Cable UTP, Radio Enlace.

Además, para seguridad en las redes poseen: Firewall Perimetral, con la utilización de Software Libre "PFSENSE", equipo Virtualizado frente al servicio de internet para control especializado.

4.6.1.6. [Media] Soportes de Información

El centro de datos cuenta con dispositivos de almacenamiento y soportes de información que son mencionados en la tabla 16. Poseen además bitácoras de soporte de mantenimiento de hardware y software, así como el diagrama lógico del centro de datos que se visualiza al principio de este capítulo.

Soportes de Información	**[ELECTRONIC_UPSE]** Electrónicos **[DISK_UPSE]** Discos Duros Externos **[BLU-RAY_UPSE]** Blu-ray Disk **[CD_UPSE]** CD-ROM **[USB_UPSE]** Memorias USB **[MC_UPSE]** Tarjetas de memoria **[IC_UPSE]** Tarjetas de inteligentes (Wireless)
	[NON_ELECTRONIC_UPSE] No electrónicos **[PRINTED_UPSE]** Material Impreso **[TAPE_UPSE]** Cinta de Papel **[RESMAS_UPSE]** Resmas

Tabla 16: Soportes de dispositivos de información.

4.6.1.7. [AUX] Equipamiento Auxiliar

Los equipos auxiliares que posee el data center y sirven para soporte a los sistemas de información sin estar relacionados con datos se muestran:

Equipos Auxiliares	**[UPS_UPSE]** Sistemas de alimentación ininterrumpida
	[AC_UPSE] Equipos de climatización
	[AC_UPSE] Cableado
	[AUXOTR_UPSE] Otros equipos auxiliares (equipos de detección y extinción)

Tabla 17. Equipamiento auxiliar.

	Equipo	**Capacidad**	**Características**
Características	1 UPS LG	10 KVA	Utilizados para los Servidores. Cuenta con: • Banco de Baterías Independientes • Tiempo de duración al usarse es de 5 horas. • Mantenimiento al equipo cada 3 meses.
	1 Aire Acondicionado	7000 BTU	Utilizado para Servidores, encendido las 24 horas
	1 Aire Acondicionado	32000 BTU	Utilizado Para oficina
	• 1 Extintor para centro de datos • 1 Extintor para oficina • No hay alarmas.		• Para Equipos Electrónicos • De “Bióxido de Carbono” • Usados para líquidos inflamables.

Tabla 18. Especificaciones técnicas de los equipos auxiliares.

4.6.1.8. [L] Instalaciones

La infraestructura tecnológica donde se alojan los sistemas de información y comunicaciones, está ubicada en el Departamento de Dirección de Tecnologías de la Información y Comunicación de la UPSE, específicamente en el centro de datos y comunicaciones, área de redes e infraestructura (Edificio).

4.6.1.9. [P] Personal

El personal encargado del centro de datos de la UPSE se especifica en la tabla 21, está conformado por:

Personal encargado de la Dirección de TIC	**[DT_UPSE]** Director de TIC
	[JF_UPSE] Jefe de Desarrollo de Software
	[AS_UPSE] Analista de Sistemas
	[DES_UPSE] Desarrolladores / Programadores
	[JR_UPSE] Jefe de Redes e Infraestructura
	[CHW_UPSE] Coordinador de Mantenimiento de Hardware
	[THW_UPSE] Técnico en Hardware y Aplicaciones
	[TE_UPSE] Técnico en Electrónica
	[TS_UPSE] Técnico de Soporte al usuario

Tabla 19. Personal informático capacitado de la dirección de TI.

4.7. Caracterización de amenazas

Esta fase fue desarrollada mediante un enfoque del libro II de la metodología Magerit "Catálogo de elementos", indispensable para seleccionar las amenazas adecuadas a las que está expuesto el centro de datos y poder categorizar los riesgos existentes. Las amenazas se clasificaron en los siguientes grupos:

- De origen natural (Desastres naturales)
- Del entorno (de origen industrial).
- Errores y fallos no intencionados.
- Ataques intencionados.

El objetivo de esta fase es dividir en grupos las amenazas posibles que pueden darse sobre los activos de un sistema, teniendo en consideración que no todas las amenazas afectan a todos los activos debido a que primero debe existir una relación entre ambos.

4.8. Identificación de riesgos

Teniendo identificados todos los activos correspondientes, es necesaria la caracterización de los posibles riesgos existentes que pueden afectar a la información. Los riesgos fueron obtenidos mediante las encuestas, entrevistas y visitas técnicas formales a los usuarios responsables de los sistemas de información, teniendo la aprobación y consentimiento inmediato del Director de TIC, para la ejecución de un análisis de riesgos óptimo y oportuno. Las posibles eventualidades consideradas dentro del proyecto describiendo todos los riesgos a tratar en el Data Center del Departamento de Tecnologías de Información y Comunicación pueden verse en la tabla 20.

No.	RIESGO
1	Fuego
2	Daños por Agua (Lluvias + Rotura de Tuberías +Llaves Abiertas)
3	Desastres Naturales (Terremoto)
4	Desastres Naturales (Tsunami)
5	Contaminación en los equipos (Polvo , suciedad)
6	Fallas en los Sistemas (S.O, Aplicaciones Desarrolladas, BD, SB)
7	Fallas en los Servidores (Físicos + Virtualizados)
8	Fallas en las Comunicaciones de Datos (Equipos +Medios Transmisión)
9	Cortes de Suministro Eléctrico
10	Fallas en la Climatización (Condiciones inadecuadas de temperatura o humedad)
11	Fallas en la protección de archivos
12	Equivocaciones, daño de archivos
13	Errores de configuración
14	Virus, daño de Información
15	Acceso no autorizado, filtrado de información
16	Robo Común
17	Robo de Información
18	Vandalismo
19	Indisponibilidad del Personal
20	Uso No Previsto (Mal uso de Recursos)
21	Delitos Informáticos (Fraude, alteración de Información, piratería informática)
22	fallas en Ups (respaldo de información)

Tabla 20. Listado de posibles riesgos existentes en la dirección de TI.

4.8.1. Criterios de valoración de riesgos

Para la evaluación y valoración de los riesgos, fue indispensable realizar una matriz donde se toman a consideración dos puntos importantes:

- **APARICIÓN** (Probabilidad de ocurrencia).
- **GRAVEDAD** (Impacto).

La probabilidad de que se materialice una amenaza, así como la magnitud o gravedad del daño pueden tomar los valores o condiciones escogidos respectivamente según la frecuencia y daño.

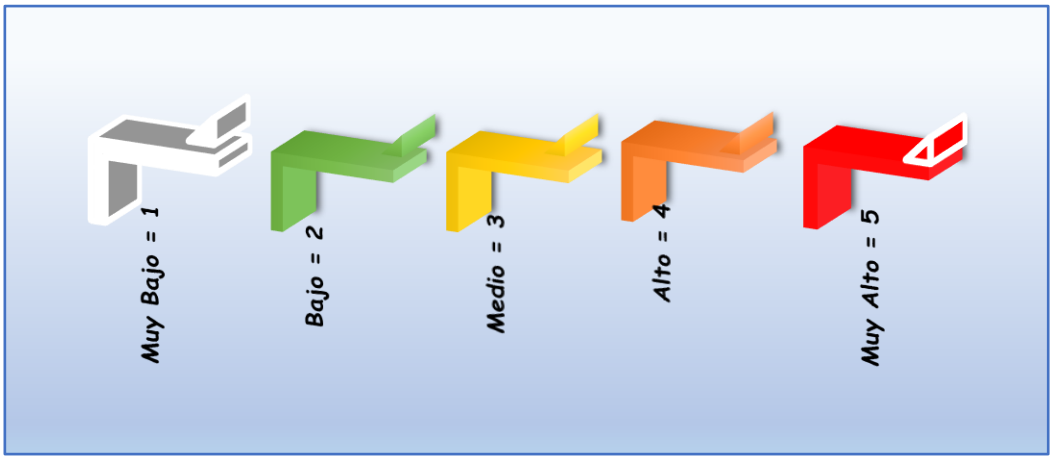


Figura 20. Escala de valoración de probabilidad e impacto.

Para obtener resultados más aproximados en cuanto a la probabilidad y al impacto en consideración con las amenazas encontradas en el Data Center es necesario utilizar la escala de valoración mencionada anteriormente.

4.8.2. Matriz de Riesgos aplicada a las TI

La matriz de probabilidad – impacto elaborada para el proyecto sirve de ayuda como un instrumento de análisis cualitativo de riesgos, que permite categorizar los riesgos en varios niveles de importancia en función a la evaluación de la

probabilidad de que ocurra el riesgo y a la medida del daño que cae sobre cada activo derivado de la materialización de una amenaza.

Los valores obtenidos de la matriz se utilizaron para categorizar los riesgos en cuanto a niveles:

- Los valores entre **15 – 25** se consideran los riesgos muy graves o críticos y están marcados de color rojo.
- Los valores entre **9 - 12** se consideran riesgos importantes y están marcados de color naranja.
- Los valores entre **3 - 8** se consideran riesgos apreciables y están marcados de color amarillo.
- Los valores entre **1 – 2** se consideran los riesgos menos relevantes o marginales y están marcados de color blanco.

Los niveles de riesgos considerados en el proyecto están clasificados por varios colores:

	Riesgo muy grave. Requiere medidas preventivas urgentes. No se debe iniciar el proyecto sin la aplicación de medidas preventivas urgentes y sin acotar sólidamente el riesgo.
	Riesgo importante. Medidas preventivas obligatorias. Se deben controlar fuertemente las variables de riesgo durante el proyecto.
	Riesgo apreciable. Estudiar económicamente si es posible introducir medidas preventivas para reducir el nivel de riesgo. Si no fuera posible, mantener las variables controladas.
	Riesgo marginal. Se vigilará, aunque no requiere medidas preventivas de partida.

Tabla 21. Niveles de riesgos a considerar en el Data Center.

La matriz de riesgos compone 2 partes: las columnas horizontales equivalentes a los valores promedio de probabilidad (entre 1 a 5) y las filas verticales en donde se reflejan los valores promedio de impacto del riesgo (entre 1 a 5).

			APARICIÓN (probabilidad)				
			MUY BAJO **1**	BAJO **2**	MEDIO **3**	ALTO **4**	MUY ALTO **5**
GRAVEDAD (IMPACTO)	MUY ALTA	**5**	5	10	15	20	25
	ALTA	**4**	4	8	12	16	20
	MEDIA	**3**	3	6	9	12	15
	BAJA	**2**	2	4	6	8	12
	MUY BAJA	**1**	1	2	3	4	5

Tabla 22. Matriz de evaluación y respuesta de probabilidad e Impacto.

El resultado del riesgo equivale al producto de la multiplicación de la probabilidad de ocurrencia de una amenaza por la gravedad o magnitud de daño y está expresada mediante la siguiente fórmula:

- $\boldsymbol{NP} = Nivel\ de\ Probabilidad$
- $\boldsymbol{NI} = Nivel\ de\ Impacto$
- $\boldsymbol{NR} = Nivel\ de\ Riesgo$

$$\boldsymbol{Nivel\ de\ riesgo} = (NP * NI)$$

Figura 21. Fórmula general del nivel del riesgo.

En dependencia del color de cada celda es posible obtener conclusiones sobre el nivel del riesgo que ocurre en cada activo de la institución, permitiendo determinar incidentes significativos y especificar también las posibles medidas de protección necesarias adecuadas al problema.

4.8.3. Probabilidad de ocurrencia

La probabilidad de ocurrencia hace referencia a la periodicidad o repetición en que pueda ocurrir o materializarse una amenaza, para este análisis fue considerado como modelo una tasa anual de ocurrencia para determinar la frecuencia de aparición de la misma.

PROBABILIDAD	VALOR	DESCRIPCIÓN
MUY BAJA	**1**	Amenaza materializada 1 vez cada varios años
BAJA	**2**	Amenaza materializada 1 vez cada año
MEDIA	**3**	Amenaza materializada 1 vez cada mes
ALTA	**4**	Amenaza materializada 1 vez cada semana
MUY ALTA	**5**	Amenaza materializada a diario

Tabla 23. Criterios para estimar la probabilidad de ocurrencia.

4.8.4. Impacto

El impacto se refiere al daño causado por una eventualidad en caso de que ocurra. Los criterios para estimar el impacto destacan una escala desde muy baja representada con 1 hasta muy alta tomando el valor de 5, cada una describiendo las consecuencias que podrían causar sobre los activos informáticos. La escala de valores está considerada:

IMPACTO	VALOR	DESCRIPCIÓN
MUY BAJO	**1**	El daño derivado de la materialización de la amenaza, no tiene consecuencias relevantes para la organización
BAJO	**2**	El daño derivado de la materialización de la amenaza, tiene consecuencias leves para la organización

MEDIO	**3**	El daño derivado de la materialización de la amenaza, tiene consecuencias destacables para la organización
ALTO	**4**	El daño derivado de la materialización de la amenaza, tiene consecuencias graves para la organización
MUY ALTO	**5**	El daño derivado de la materialización de la amenaza, tiene consecuencias muy graves para la organización

Tabla 24. Criterios para estimar el impacto o gravedad.

4.9. Riesgos existentes en la dirección de TIC's

En la tabla 25, se observa detalladamente el valor y el nivel de los riesgos encontrados en el departamento de TIC's (Data Center), los mismos que a través de entrevistas realizadas correctamente a los Jefes de las áreas responsables como: Área de redes y telecomunicaciones, Área de sistemas y al director de TI sobre cada uno de los posibles riesgos clasificados según el valor del mismo llegando a determinarlos como: graves, importantes, apreciables y marginales.

En la matriz están reflejados los niveles de prioridad, fueron seleccionados 3 riesgos más relevantes de cada nivel, los riesgos distinguidos en niveles graves e importantes están obligados a sujetarse a un plan de mitigación con el objetivo de brindar medidas preventivas apropiadas para establecer la continuidad de la función de las operaciones en caso de impactos graves en el departamento.

Para la estimación de la probabilidad de amenaza fue necesario trabajar con valores generalizados utilizados para todos los elementos de riesgo, considerando el tiempo de la presencia de amenazas y evaluándolas de forma diaria, semanal, mensual y anual en dependencia de la magnitud del daño por las consecuencias producidas en la organización. En relación a estos dos factores la matriz es calculada por el producto de ambas variables obteniendo como resultado el grado de riesgo.

Dependiendo de los colores de cada celda es fácil concluir y decidir sobre el plan de seguridad y de mitigación a usar para los riesgos analizados. Las medidas de protección necesarias fueron elaboradas para niveles de riesgo graves e importantes:

- **Riesgos muy graves**
    - Fuego.
    - Desastres naturales (terremoto).
- **Riesgos Importantes**
    - Daños por Agua (Lluvias+Rotura de Tuberias+Llaves Abiertas).
    - Fallas en las comunicaciones de datos (Equipos y Medios de transmisión).
    - Cortes de Suministro Eléctrico.
    - Fallas en la Climatización (Condiciones inadecuadas de temperatura o humedad).
    - Fallas en la protección de archivos.
    - Virus, daño de Información.
    - Acceso no autorizado, filtrado de información.
    - Robo Común.
    - Robo de Información.
    - Fallas en UPS, respaldo de información.

Las dos categorías de riesgos mencionadas anteriormente contaran con un adecuado plan de mitigación y contingencias que especificará simplificadamente actividades de respaldo, emergencia y recuperación implementadas a través de acciones o controles urgentes y obligatorios para la protección del riesgo con el objetivo de reaccionar de forma efectiva ante eventos de contingencia a darse en la dirección de TI.

La evaluación de la matriz de riesgo previamente elaborada contiene la relación entre amenazas y magnitudes de daños, además proporciona una apreciación del promedio total de riesgos y su nivel, para constatar aquello es necesario visualizar la tabla 25.

MATRIZ DE RIESGOS	Aparición probabilidad	Gravedad (Impacto)	Valor del Riesgo	
RIESGO				
Fuego	4	4	16	Muy grave
Daños por Agua (Lluvias+Rotura de Tuberias+Llaves Abiertas)	3	3	9	Importante
Desastres Naturales (Terremoto)	4	4	16	Muy grave
Desastres Naturales (Tsunami)	1	4	4	Apreciable
Contaminación en los equipos (Polvo , suciedad)	3	2,4	7,2	Apreciable
Fallas en los Sistemas (S.O, Aplicaciones Desarrolladas, BD, SB)	3	2,5	7,5	Apreciable
Fallas en los Servidores (Fisicos+Virtualizados)	2	2,8	5,6	Apreciable
Fallas en las Comunicaciones de Datos (Equipos+Medios Transmisión)	4	2,7	10,8	Importante
Cortes de Suministro Eléctrico	3	3,5	10,5	Importante
Fallas en la Climatización (Condiciones inadecuadas de temperatura o humedad)	3	3	9	Importante
Fallas en la protección de archivos	4	2,6	10,4	Importante
Equivocaciones, daño de archivos	2	2	4	Apreciable
Errores de configuración	3	2,7	8,1	Apreciable
Virus, daño de Información	4	2,8	11,2	Importante
Acceso no autorizado, filtrado de información	3	3,6	10,8	Importante
Robo Común	4	3	12	Importante
Robo de Información	3	3	9	Importante
Vandalismo	2	3	6	Apreciable
Indisponibilidad del Personal	2	2	4	Apreciable
Uso No Previsto (Mal uso de Recursos)	1	2	2	Marginal
Delitos Informáticos (Fraude, alteración de Información, piratería informática)	2	2,8	5,6	Apreciable
fallas en UPS, respaldo de información	3	3	9	Importante
PROMEDIO =			**187,7**	Importante

Tabla 25. Matriz de riesgos evaluada en el departamento de TI.

4.9.1. Niveles del riesgo en la dirección de TIC's

Los niveles de riesgo obtenidos están especificados en valores porcentuales indicando el grado de criticidad entre ellos, ver en la Figura 22.

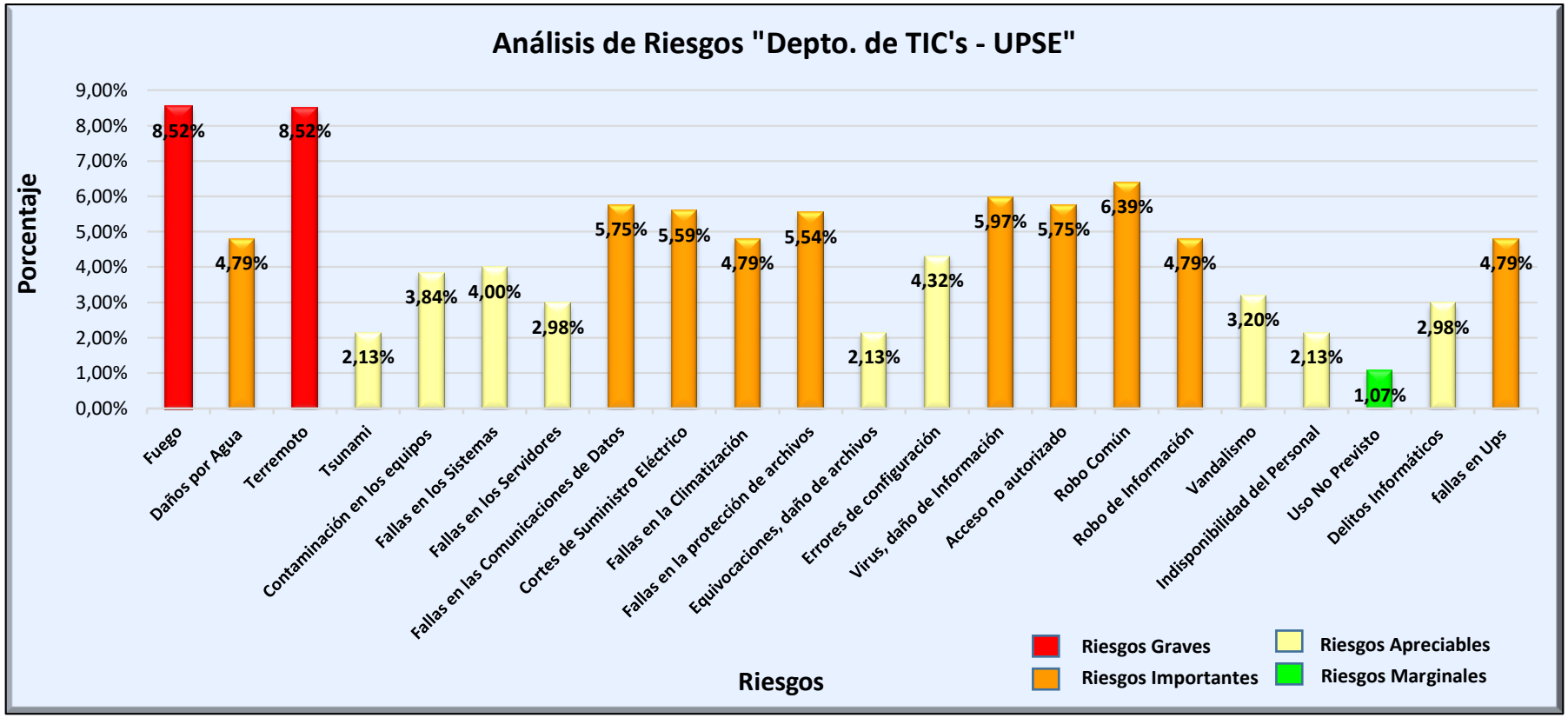


Figura 22. Gráfico de columnas agrupadas por categorías de riesgos.

4.10. Tratamiento del riesgo

El tratamiento del riesgo abarca un proceso de selección e implementación de medidas de seguridad para modificar y corregir el riesgo con el objetivo de brindar a la institución una forma óptima y eficiente de lograr una mayor reducción de los mismos con una menor inversión posible.

Cabe mencionar que la mitigación no está orientada a todos solo está aplicada a los riesgos no aceptables, es decir los que tienen un mayor nivel de gravedad y son considerados graves e importantes de lo contrario sería difícil financiar y priorizar la mitigación

4.10.1. Caracterización de las salvaguardas

Una vez analizados los posibles riesgos a presentarse con el mayor nivel de importancia, es necesario identificar las salvaguardas con cada medida efectiva que posee cada una de ellas para la mitigación adecuada del riesgo.

Es necesario tener en cuenta que existen amenazas que se conjuran simplemente organizándose adecuadamente, sin embargo hay otras que requieren de elementos técnicos, programas o equipos, seguridades físicas y, por último, de políticas de personal [10].

Las salvaguardas representan mayormente una defensa hacia las amenazas. Estas medidas específicamente las técnicas, varían de acuerdo al avance tecnológico. Por tal razón, aparecen tecnologías nuevas y van desapareciendo tecnologías antiguas, produciendo un cambio de los tipos de activos, una evolución en las posibilidades de los atacantes y un aumento de los catálogos de salvaguardas disponibles [14].

4.10.2. Efectos de las salvaguardas

Las salvaguardas o medidas entran en el cálculo del riesgo mediante dos formas:

- **Reduciendo la probabilidad de las amenazas:** corresponden a salvaguardas preventivas. Son actividades de planteamiento que impidan

que la amenaza se materialice, asegurando un proceso de recuperación con el menor costo posible a la institución.

- **Limitando el daño causado:** Hay salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance. Incluso algunas salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye [27].

4.10.3. Tipo de protección de salvaguardas

Existen diferentes tipos de protección proporcionados por las salvaguardas, mientras tanto para las necesidades de nuestro proyecto se seleccionaron los siguientes aspectos de protección que ofrece el libro 1 de la metodología Magerit v.3 [10].

Tipo de Protección	Descripción
[PR] prevención	Una salvaguarda es preventiva cuando reduce las oportunidades de que un incidente ocurra.
[DC] detección	Una salvaguarda funciona detectando un ataque cuando informa de que el ataque está ocurriendo. Aunque no impide el ataque, sí permite que entren en operación otras medidas que atajen la progresión del ataque, minimizando daños.
[CR] corrección	Una salvaguarda es correctiva cuando, habiéndose producido un daño, lo re-para. Son salvaguardas que actúan después de que el incidente se haya producido y por tanto reducen los daños.

Tabla 26. Tipo de protección de salvaguardas.

4.10.4. Eficacia de la protección

Las salvaguardas además de su existencia dentro del tratamiento del riesgo, se califican también por su nivel de eficacia ante los riesgos. Este nivel está representado en un rango de 0% a 100% eficaz dependiendo de un punto de vista técnico y operacional de la salvaguarda.

Las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos son factores reales y apropiados para la reducción del riesgo en la organización [3].

factor	nivel	significado
0%	L0	inexistente
	L1	inicial / ad hoc
	L2	reproducible, pero intuitivo
	L3	proceso definido
	L4	gestionado y medible
100%	L5	optimizado

Figura 23. Eficacia y madurez de las salvaguardas. Fuente: (Amutio Gómez & Candau) magerit v3.

En el nivel **L0** representan los procedimientos inexistentes que no han sido evaluados. En los niveles **L1** tiene el 10% de eficacia y **L2** tiene el 50% de eficacia, se consideran los procedimientos existentes (iniciales y parcialmente realizados) pero que aún falta mejorar su gestión. En los niveles **L3** tiene el 90% de eficacia y **L4** tiene el 95% de eficacia, se consideran aquellas salvaguardas que están implementadas de forma correcta, en funcionamiento y sujetas a optimizarse. El nivel **L5** representa procedimientos con mejora continua, 100% eficaces para el funcionamiento de la organización. Se tiene como objetivo los niveles **L4 y L5** en las salvaguardas de los riesgos a tratar, dependiendo de los casos, con la finalidad de aplicar y optimizar los procedimientos de protección.

La evaluación de las salvaguardas se llevará a cabo determinando su grado de importancia con respecto a la emisión de buenas prácticas previas que deberían de cumplirse con el fin de dar el debido tratamiento a los riesgos obtenidos.

En la valoración de las medidas de seguridad preventivas se determinará mediante dos columnas importantes: la columna "**Actual**" menciona la apreciación que se dará dependiendo de cómo se encuentra la institución en la actualidad mediante lo evaluado, y la columna "**Objetivo**" mostrará la apreciación de mejoras optimas como **L3, L4 y L5** según el argumento y proceso de la salvaguarda y el riesgo, esta columna en sí especifica una forma clara de cómo debería manejarse la dirección de TI con la aplicación de medidas de seguridad implantadas en una institución pública como la UPSE.

4.10.5. Evaluación de salvaguardas

Las medidas deberían ser evaluadas tomando en cuenta el alcance de la reducción del riesgo. Dentro de esta actividad las salvaguardas proyectadas se eligieron bajo consejos o buenas prácticas del estándar **ISO/IEC 27001, 27002**, lo que ayuda a reconocer las necesidades en la seguridad de la información. En las siguientes tablas, se identifican las alternativas a implementar en caso de que se requieran, y a continuación, se muestra las amenazas más relevantes que fueron seleccionadas para el debido tratamiento del riesgo.

4.10.5.1. Salvaguardas previas al riesgo

Riesgo	Salvaguardas	Actual	Objetivo
1. **Fuego**	**ÁREA FÍSICA**		
	• Identificar y señalar adecuadamente las rutas de evacuación (salidas de emergencia).	**L0**	**L3**
	• Implementación de señales normalizadas (No fumar, no comer, etc.) suficientes, en puntos específicos del departamento de Dirección de TIC's y áreas de trabajo, donde pudiera existir riesgos de incendio.	**L0**	**L3**
	• Instalación de sistemas de alarmas contra incendio.	**L0**	**L3**

	• Identificar la ubicación de las estaciones manuales de alarma contra incendio.	**L0**	**L3**
	• Adquirir cajas de seguridad para Cintotecas, sobre acero blindado inmune al fuego, para almacenar los respaldos para cintas magnéticas y documentos importantes del depto. de TIC's.	**L0**	**L3**
	• Instalación de extintores manuales (portátiles) y/o automáticos (rociadores) contra incendio en sitios estratégicos.	**L2**	**L3**
	• Contar con suficientes extintores debidamente cargados, en buen estado de funcionamiento, dentro del año que dura su carga y con presión correspondiente.	**L2**	**L5**
	• Uso correcto de los extintores, teniendo en cuenta aspectos generales, aparatos del sistema, lectura del manómetro, fecha de comprobación de recarga, etc.	**L0**	**L5**
	• Instalación y mantenimiento de los sistemas de detección y extinción de incendios (Agente limpio FM200).	**L0**	**L5**
	• Debe construirse un "Piso falso" instalado sobre el piso real, con materiales incombustibles y resistentes al fuego.	**L0**	**L3**
	• El piso y el techo del centro de cómputo y de almacenamiento de los medios magnéticos deben ser impermeables.	**L2**	**L4**
	• Aplicar procedimientos óptimos para recibir y almacenar abastecimientos de papel.	**L0**	**L3**
	• Adquirir un seguro contra incendios.	**L2**	**L4**
	SERVIDORES Y EQUIPOS DE CÓMPUTO		
	• Realizar respaldos internos y externos de información de los servidores.	**L3**	**L4**
	• Asignar un equipo a cada personal de la Dirección de TIC's, dependiendo de su cargo y prioridad.	**L3**	**L4**
	• Mantener correctamente apagados los equipos de cómputo no utilizados.	**L3**	**L4**
	INSTALACIONES ELÉCTRICAS		
	• Mantenimiento periódico de las instalaciones eléctricas, verificar que	**L3**	**L4**

	estén en perfecto estado de funcionamiento.		
	• Mantener las conexiones eléctricas seguras en el rango de vida útil.	**L2**	**L4**
	• Disponer de diagramas eléctricos actualizados en la institución y en el depto. de TIC's.	**L2**	**L3**
	• Mantener debidamente aterrizado los equipos informáticos y los racks sobre los que están montados los servidores.	**L0**	**L5**
	• Implementar normas internacionales sobre el tipo de cable utilizado paras las instalaciones eléctricas.	**L2**	**L3**
	• Evitar múltiples conexiones, y eludir sobre carga de circuitos eléctricos.	**L3**	**L3**
	• Verificar que los niveles de voltaje sean los adecuados para los equipos informáticos.	**L3**	**L3**
	• Implementación de sistema de tierra para protección de los equipos.	**L2**	**L3**
	• Evitar derramar fluidos líquidos, sobre las conexiones eléctricas.	**L4**	**L4**
	GENERALES		
	• Realizar simulacros contra incendios periódicamente (2 veces por año).	**L0**	**L3**
	• Capacitar al personal informático sobre el uso correcto de extinguidores por parte de personal especializado.	**L0**	**L3**
	• Ubicar/Localizar los contactos telefónicos de emergencia que incluya a: bomberos, ambulancias, y personal de la institución responsable de la ejecución de acciones de contingencia.	**L0**	**L3**
	• Mantener siempre el área de trabajo limpia y en orden.	**L3**	**L4**
	• Descartar el almacenamiento total de sustancias y productos inflamables.	**L3**	**L3**
	• Desarrollo de plan de emergencia ante desastres y normas precisas contra incendios por parte del personal informático.	**L0**	**L3**
	• Conocer el plan de evacuación por parte del personal informáticos.	**L2**	**L3**
2. Terremoto	**ÁREA FÍSICA**		
	• Mantener un inventario adecuado de materiales, herramientas y el equipo necesario para enfrentar una situación de emergencia.	**L0**	**L4**

	• Corregir inmediatamente rajaduras o cimientos en caso de que existan en el cuarto de servidores y oficinas.	**L2**	**L3**
	• Fijar adecuadamente al piso o paredes las estanterías y equipos de gran tamaño y peso.	**L2**	**L3**
	• Identificar las zonas de escape o emergencia, seguridad sobre terremotos y mantenerlas libres de obstáculos.	**L0**	**L3**
	• Asegurarse de que el techo de la dirección de TIC's estén realizados bajo normas de protección contra sismos y estén debidamente reforzados.	**L2**	**L3**
	• Contar con equipos de protección para el personal como: kit de primeros auxilios, cascos de seguridad, protectores faciales, respiradores, linternas, etc., manteniendo equipados los lugares de emergencias.	**L0**	**L3**
	GENERALES		
	• Realizar simulacros de terremoto periódicamente (2 veces al año) para mantener la efectividad de operación en caso de emergencia.	**L0**	**L3**
	• Localizar la lista de personal que trabajara en brigadas de emergencia.	**L0**	**L3**
	• Almacenar las cintas de respaldo en un lugar externo al de la institución.	**L0**	**L3**
	• Desarrollar un plan de evacuación y emergencia de las instalaciones del depto. de TIC's en caso de terremoto.	**L0**	**L3**
	• Capacitar al personal sobre medidas de prevención para enfrentar caso de terremotos y sobre primeros auxilios	**L0**	**L3**
3. Fallas en las comunicaciones de datos	**GENERALES**		
	• Controlar el tiempo de uso de los equipos de comunicación.	**L2**	**L3**
	• Supervisar siempre los segmentos de la red a fin de encontrar vulnerabilidades.	**L3**	**L4**
	• Mantener los diagramas de las redes de la institución actualizados.	**L3**	**L4**
	• Incrementar personal para el área de las comunicaciones.	**L0**	**L3**
	• Cumplir con normas internacionales para comunicaciones.	**L2**	**L3**

	• Adquirir equipos idóneos para comunicaciones de datos de marcas reconocidas.	**L3**	**L4**
	• Analizar el tipo de cable y su categoría para la implementación del cableado horizontal y vertical.	**L3**	**L4**
	• Establecer un plan de acción para actuar frente a problemas en las redes.	**L2**	**L3**
	• Determinar la ubicación más óptima antes de realizar una instalación inalámbrica.	**L2**	**L3**
	• Verificar el correcto funcionamiento de las tarjetas de red y dispositivos de comunicaciones como switch, router, Access point.	**L4**	**L4**
	• Diseñar procedimientos para instalación de red integral de datos y monitoreo de redes LAN y WAN.	**L2**	**L3**
	• Revisar el cableado total de la red, verificando que estén en buen estado.	**L2**	**L3**
	• Hacer actualizaciones periódicas de inventarios de los equipos de comunicaciones.	**L0**	**L3**
	• Realizar mantenimiento punto a punto de la red total, para evitar problemas de transmisión y corregirlos a tiempo.	**L3**	**L3**
	• Instalar correctamente los equipos de comunicación, las redes utilizando normas internacionales por medio de técnicos capacitados.	**L2**	**L3**
4. Daños por agua.	**INFRAESTRUCTURA**		
	• Implementar techo impermeable, para evitar daños de los equipos provocados por lluvias prolongadas.	**L2**	**L3**
	• Ofrecer mantenimiento preventivo una vez por año con impermeabilizantes a los techos y paredes donde exista el riesgo de inundación.	**L1**	**L3**
	• Implementar un sistema de drenaje adecuado para el depto. de TIC's.	**L4**	**L4**
	• Realizar mantenimiento preventivo a los sistemas de aguas servidas y agua potable.	**L4**	**L4**
	• Disponer en la institución de los planos de distribución de la institución.	**L3**	**L3**
	• Identificar lugares susceptibles a inundaciones y gestionar las medidas de seguridad necesarias.	**L2**	**L3**

	• Supervisar las instalaciones físicas del depto. de TIC's y los alrededores, ofreciendo reparaciones inmediatas para evitar inundaciones.	**L3**	**L4**
	SERVIDORES Y EQUIPOS		
	• Ubicar los equipos en lugares estratégicos, fuera de lugares propensos a roturas de tuberías de agua.	**L2**	**L3**
	• Apagar equipos de cómputo no prioritarios.	**L3**	**L3**
	• Contar con bolsas de plástico para cubrir servidores y documentos importantes que puedan mojarse.	**L0**	**L3**
	• Mantener en lugares seguros el hardware, software y documentos importantes.	**L2**	**L3**
	INSTALACIONES ELÉCTRICAS		
	• Supervisar que todo contacto o interruptor mantenga siempre su tapa aislada y estar a una altura correcta para prevenir cortocircuitos provocados por el agua.	**L2**	**L3**
	• Verificar periódicamente que las instalaciones eléctricas estén en perfecto estado de funcionamiento.	**L2**	**L4**
	GENERALES		
	• Realizar simulacros de inundaciones dos veces por año, para analizar los tiempos de evacuación	**L0**	**L3**
	• Fumigar las áreas de la institución una vez por año para evitar alergias provocadas por la humedad (moho, insectos).	**L0**	**L3**
	• Analizar los lugares alternos de trabajo en caso de inundaciones.	**L1**	**L3**
	• Eliminar escombros, basuras o materiales que podrían ser arrasados por el agua.	**L0**	**L3**
5. Cortes de suministro eléctrico	**PLANTA DE EMERGENCIA**		
	• Contar con una planta de emergencia que suministre energía regulada en cada sitio o centro de cableado eléctrico.	**L0**	**L3**
	• Supervisar semanalmente el nivel óptimo de combustible, agua, baterías, etc. Contar con un plan de mantenimiento semestral.	**L2**	**L5**

	• Contar con equipo de emergencia contra incendios en el local de la planta.	**L0**	**L3**
	• Contar con el mapa eléctrico del área en la planta y archivado, identificando los contactos respaldados y regulados.	**L2**	**L3**
	• Contar con tierras físicas independientes a los servicios de telecomunicaciones.	**L0**	**L4**
	BYPASS		
	• Implementar un Bypass en cada sitio que contenga equipos críticos conectados a la red o al segmento de red.	**L2**	**L5**
	• Supervisar mensualmente el óptimo estado del Bypass.	**L2**	**L4**
	• Contar con un diseño de mapa eléctrico del área ilustrando el Bypass	**L0**	**L3**
	• Realizar un plan de mantenimiento anual integral con supervisiones mensuales.	**L2**	**L4**
	• Contar con los elementos necesarios para activar y/o desactivar el Bypass	**L3**	**L3**
	UPS		
	• Adquirir un UPS con capacidades necesarias (40% superiores) en todos los sitios y centros de cableado.	**L2**	**L3**
	• Verificar que los equipos UPS cuenten con el mantenimiento adecuado y con suficiente energía para soportar una operación continua de 15 minutos como mínimo. El tiempo variará de acuerdo a la función que cumplan los equipos UPS.	**L2**	**L4**
	• Analizar los bancos de UPS (capacidad, tiempo, duración, respaldos de UPS, cargas de UPS, manuales de funcionamiento, mantenimientos).	**L3**	**L4**
	• Determinar semestralmente el tiempo efectivo y real de respaldo del UPS con respecto a las diferentes cargas.	**L2**	**L3**
	• Realizar pruebas periódicas de los equipos UPS para asegurar su correcto funcionamiento	**L2**	**L3**
	• Contar con UPS para proteger los equipos de vigilancia (cámaras, sistemas de grabación) y de control de acceso a las instalaciones de la	**L0**	**L3**

	dirección de TIC's (puertas, contactos magnéticos, etc.)		
	• Contar con el mapa eléctrico del área, identificando los contactos regulados y respaldados.	**L0**	**L3**
	GENERALES		
	• Poseer un directorio de los responsables del suministro eléctrico en cada nodo.	**L3**	**L3**
	• Contar con procedimientos para reportar el incidente a las áreas involucradas (Servicios Generales, Proveedores de Mantenimientos, etc.).	**L3**	**L4**
	• Contar con procedimientos de ejecución de respaldos de emergencia a la información del servidor Web, mail, DNS, configuraciones de Equipo Activo principales y centrales.	**L0**	**L5**
	• Contar con una tabla de claves de prioridades para dar aviso a los usuarios prioritarios con el fin de optimizar tiempo y recursos.	**L0**	**L3**
6. Fallas en la climatización la climatización	**GENERALES**		
	• Realizar controles de integridad de los equipos de climatización: (capacidad, temperaturas, circulación de aire dentro de los racks).	**L2**	**L4**
	• Implementar un régimen de mantenimiento del sistema de enfriamiento.	**L2**	**L5**
	• Instalación de sistema de calefacción, ventilación y aire acondicionado por separado dedicado a la data center y al área de máquinas de forma exclusiva.	**L2**	**L3**
	• Instalar paneles de obturación e implementar un régimen de organización del cableado.	**L0**	**L3**
	• La alimentación eléctrica debe ser independiente para estos equipos, por motivo del ruido eléctrico producido.	**L2**	**L3**
	• En caso de corte de energía, se debe contar con UPS o generador eléctrico, que respalde la función del aire acondicionado de precisión.	**L0**	**L3**
	• Contar con normas de instalación para los equipos de enfriamiento.	**L0**	**L4**
	• Retirar obstáculos bajo el piso elevado y sellar el piso elevado, si el centro de datos cuenta con uno.	**L0**	**L3**

	• Separar racks de alta densidad.	**L0**	**L3**
	• Mantener la temperatura idónea del equipo de enfriamiento: se recomienda de 20 – 25ºC (68-77ºF) y la permitida es de 15-32ºC (59-90ºF).	**L2**	**L3**
	• Implementar una configuración de pasillo caliente/frío.	**L2**	**L3**
	• El mantenimiento debe estar a cargo de personal capacitado o técnicos de una empresa proveedora de aires acondicionados, ellos se encargarán: determinar la capacidad del equipo, efectuar el balance térmico, etc.	**L3**	**L5**
	• Contar con indicadores y sensores de temperatura y humedad.	**L0**	**L3**
7. Fallas en protección de archivos.	**INFRAESTRUCTURA**		
	• Supervisar el Data Center mediante cámaras de seguridad.	**L0**	**L5**
	• Almacenar las copias de los respaldos en lugares seguros fuera de la institución.	**L0**	**L3**
	SOFTWARE		
	• Actualizar los sistemas antimalware, antispyware, firewalls para su detección eficiente.	**L2**	**L4**
	• Realizar escaneos de la red para detectar la intrusión de hackers.	**L3**	**L3**
	GENERALES		
	• Realizar respaldos diarios de la información más importante.	**L3**	**L4**
	• Almacenar las contraseñas en lugares seguros y fáciles de recordar para el encargado de ellas, pero difíciles de encontrar para el resto.	**L3**	**L4**
	• Cambiar las contraseñas periódicamente (1 vez por semana) y con una longitud de entre 14-18 caracteres incluidos letras, números y caracteres en minúscula.	**L2**	**L3**
	• Mantener discreción en el manejo de la información valiosa de la institución por parte del personal de la dirección de TIC’s.	**L4**	**L4**

8. Virus, daño de información	**SOFTWARE**		
	• Contar con sistemas de antivirus originales, evitando software no original o pre-instalado sin el soporte original.	**L0**	**L4**
	• Implementar un servidor firewall, antispyware, y antimalware actualizados al día.	**L2**	**L4**
	• Verificar que el antivirus muestre un detalle completo de su análisis; además de brindar las actualizaciones periódicas.	**L2**	**L4**
	• Actualizar los patrones de los antivirus cada uno o dos meses.	**L0**	**L4**
	• Implementar plataformas LINUX para los servidores.	**L4**	**L4**
	GENERALES		
	• Impedir el uso de Pendrive, CD a personal no autorizado por el Director de Sistemas.	**L3**	**L3**
	• Realizar respaldos de la información más importante de los equipos, al menos 1 vez al día.	**L3**	**L4**
	• Implementar políticas adecuadas para evitar descargas de información desde internet a personal no autorizado	**L3**	**L4**
	• Descargar programas de Internet desde los sitios oficiales	**L3**	**L3**
	• Analizar los nuevos discos en el sistema con un antivirus actualizado.	**L2**	**L4**
	• Analizar también archivos comprimidos y documentos.	**L3**	**L3**
	• Evitar ejecutar programas de origen desconocidos.	**L3**	**L3**
	• Efectuar periódicamente la depuración de archivos en los discos duros.	**L2**	**L3**
	• Tener un proveedor de software antivirus para las estaciones y otro diferente para el servidor, con el objetivo de reducir la probabilidad de que un virus se filtre en toda la red.	**L0**	**L4**
	• Establecer políticas de seguridad para prevenir el uso de aplicaciones no autorizadas en las estaciones de trabajo.	**L0**	**L4**
	• Restringir el acceso a Internet a las estaciones de trabajo que por su uso no lo requieran.	**L3**	**L3**

	• Deshabilitar los puertos de comunicación USB en las estaciones de trabajo que no los requieran habilitados.	**L3**	**L3**
	• Contar con equipos de respaldo ante posibles fallas de las estaciones, para su reemplazo provisional hasta su desinfección y habilitación.	**L3**	**L4**
9. Acceso no autorizado, filtrado de información.do de información.	**NIVEL FÍSICO**		
	• Verificar que el servidor de archivos no sea accesible físicamente a cualquier persona.	**L3**	**L4**
	• Mantener políticas de identificación para los visitantes de la dirección de tic y el Data Center	**L2**	**L4**
	• Mantener vigilancia exclusiva para el Data Center las 24 horas.	**L0**	**L3**
	• Dotar de armamento adecuado a los guardias de seguridad de la institución.	**L3**	**L3**
	• Mantener las tarjetas de identificación para el personal de trabajo y actualizarlas en caso de nuevo personal.	**L0**	**L3**
	• Implementar sistemas de alarmas para la detección de personal que ingresen con armas y objetivos peligrosos.	**L0**	**L3**
	• Tener información del personal con acceso a los diferentes sistemas informáticos, ya sean locales, en red o vía internet.	**L3**	**L3**
	NIVEL LÓGICO		
	• Instalar firewall que evite ingresos desde redes externas hacia la red de la institución.	**L4**	**L4**
	• Instalar un sistema de detección de intrusos para monitorear los accesos o tentativas de accesos a la red.	**L3**	**L4**
	• Deshabilitar los servicios que no sean necesarios y verificar los posibles puertos que se encuentren abiertos innecesariamente para proceder a cerrarlos.	**L3**	**L4**
	• Concienciar a los usuarios de la red acerca de una política mínima de seguridad, por ejemplo, evitar las claves fácilmente descifrables.	**L3**	**L4**
	• Implementar controles de seguridad para la dirección de TIC’s.	**L0**	**L3**

	• Verificar que las redes estén basadas en conmutadores evitando que los paquetes de información lleguen a todas las tarjetas de red.	**L3**	**L3**
10. Robo Común	**INFRAESTRUCTURA**		
	• Colocar letreros que impidan el acceso al personal no autorizado	**L2**	**L3**
	• Asignar al personal autorizado la identificación respectiva para el ingreso al departamento de TI.	**L3**	**L3**
	• Mantener un lugar físico externo adecuado para resguardar copias de los documentos, sistemas, respaldos de la institución.	**L0**	**L3**
	• Impedir el uso de cámaras fotográficas en el Data Center, sin permiso por escrito de la Dirección de Sistemas.	**L2**	**L3**
	• Implementar un sistema de alarmas.	**L0**	**L4**
	• Incrementar cámaras de vigilancia interiores y exteriores para la dirección de TIC's.	**L0**	**L4**
	• Reforzar las puertas y ventanas del departamento de TIC's a fin de evitar un fácil ingreso y posterior robo de equipos.	**L0**	**L3**
	SERVIDORES Y EQUIPOS		
	• Evitar el acceso de personal no autorizado al área de servidores.	**L3**	**L4**
	GUARDIAS DE SEGURIDAD		
	• Contratar guardia exclusivo para la dirección de TI, el mismo que deberá estar debidamente capacitado y contar con equipos de seguridad	**L0**	**L3**
	• Controlar la entrada y salida de las personas al departamento de TI, manteniendo un registro actualizado por parte del guardia de seguridad.	**L0**	**L3**
	• Ubicar los guardias de la institución en sitios estratégicos de tal manera que no sea fácil el ingreso de una persona extraña.	**L2**	**L3**
	• Incrementar guardias de seguridad en la institución, los mismos que deberán ser altamente confiables y no registrar antecedentes penales.	**L2**	**L3**
	GENERALES		
	• Contar con registros de salida de equipos, autorizado por el jefe del área	**L2**	**L3**
	• Contar con los números telefónicos de la Policía Nacional y Guardias de seguridad de la institución.	**L3**	**L3**

	• Contar con carné de identificación siempre en un lugar visible por parte del personal informático.	**L3**	**L3**
	• Mantener vigilancia del personal que labora en el área de archivos.	**L0**	**L3**
	• Establecer políticas de autorización de acceso físico a la dirección de TIC's y mantener revisiones periódicas de las mismas.	**L0**	**L5**
	• Contar con pólizas de seguros para los equipos de cómputo.	**L3**	**L4**
	• Asignar al Jefe de área la responsabilidad de la protección de los equipos en cada espacio de la institución.	**L3**	**L4**
	• Prohibir facilitar información del personal o información confidencial de la institución.	**L3**	**L4**
11. Robo de información	**INFRAESTRUCTURA**		
	• Colocar letreros que impidan el acceso al personal no autorizado.	**L2**	**L3**
	• Verificar que el personal autorizado cuente con tarjeta de identificación respectiva.	**L3**	**L3**
	• Implementar un sistema de alarmas contra robo.	**L0**	**L3**
	• Mantener un lugar físico externo adecuado para resguardar copias de los documentos, sistemas, respaldos de la institución	**L0**	**L3**
	• Incrementar cámaras de vigilancia interiores y exteriores para la UI.	**L0**	**L3**
	• Reforzar las puertas y ventanas de la dirección de TI a fin de evitar un fácil ingreso y posterior robo de información	**L0**	**L3**
	• Mantener la puerta de acceso principal y del Data Center siempre cerrada, asimismo las ventanas de la dirección de TI.	**L2**	**L3**
	• Adquirir caja de seguridad para Cintotecas sobre acero blindado, para almacenar los respaldos de las cintas magnéticas y documentos importantes.	**L0**	**L3**
	GUARDIAS DE SEGURIDAD		
	• Contratar guardia exclusivo para la dirección de TI, el mismo que deberá estar debidamente capacitado y contar con equipos de seguridad	**L0**	**L3**

	• Controlar la entrada y salida de las personas al departamento de TI, manteniendo un registro actualizado por parte del guardia de seguridad.	**L0**	**L3**
	• Ubicar los guardias de la institución en sitios estratégicos de tal manera que no sea fácil el ingreso de una persona extraña.	**L2**	**L3**
	• Incrementar guardias de seguridad en la institución, los mismos que deberán ser altamente confiables y no registrar antecedentes penales.	**L2**	**L3**
	SOTWARE Y APLICACIONES		
	• Incrementar la seguridad para los Sistemas Gestores de Base de datos.	**L3**	**L4**
	• Implementar sistemas de escaneo de redes a través de IP para determinar posibles intrusos.	**L3**	**L4**
	• Coordinar un análisis del tráfico de la red con el proveedor de internet.	**L3**	**L4**
	• Mantener actualizados los sistemas firewalls.	**L3**	**L4**
	• Incrementar políticas de acceso a los sistemas y aplicaciones, a los usuarios de la institución.	**L0**	**L5**
	GENERALES		
	• Contar con registros de salida de documentos, autorizado por el jefe del área.	**L2**	**L3**
	• Mantener vigilancia al personal que labora en el área de archivos	**L0**	**L3**
	• Almacenar las contraseñas de acceso a los sistemas, en lugares seguros y mantener respaldos de las mismas.	**L2**	**L4**
	• Establecer políticas para cambio de contraseña mínimo cada mes.	**L0**	**L4**
	• Establecer procedimientos de actualización de copias de seguridad de sistemas, bases de datos, archivos, etc.	**L2**	**L4**
	• Dar énfasis a las políticas de seguridad de la institución.	**L2**	**L3**
	• Mantener un ambiente de trabajo limpio y ordenado.	**L2**	**L3**
	• Realizar procedimientos de administración de base de datos: instalación y actualización, asignación de recursos, monitoreo e integridad de información de la base de datos.	**L2**	**L3**
	• Capacitar al personal de la institución para estar alerta ante posibles ladrones.	**L1**	**L3**

12. Fallas en UPS, respaldo de información	**GENERALES**		
	• Realizar el mantenimiento adecuado periódicamente, por parte del personal especializado en equipos auxiliares.	**L3**	**L4**
	• Contar con UPS de calidad para servidores, equipos, aires acondicionados, etc., acorde a la cantidad de equipos.	**L2**	**L4**
	• Establecer estándares de instalación para mantenimiento de un sistema de backup.	**L2**	**L4**
	• Verificar que no existan conexiones sueltas y fallas en las baterías.	**L3**	**L4**
	• Tener repuestos de baterías para poder realizar los respaldos diarios de información.	**L0**	**L4**
	• Establecer políticas y procedimientos de backups.	**L0**	**L5**
	• Realizar copias de seguridad completas cada semana.	**L3**	**L4**

Tabla 27. Actividades de seguridad previas al riesgo.

4.10.5.2. Salvaguardas durante el riesgo

Riesgo	Salvaguardas	Área responsable
1. Fuego	**INFRAESTRUCTURA**	• Departamento de dirección de TIC's. • Departamento de electricidad. • Departamento de análisis y prevención de riesgos.
	• Activar el sistemas de alarmas contra incendio si existe la presencia de humo o fuego.	
	• Desconectar inmediatamente los suministros de energía eléctrica.	
	• Respetar los señalamientos de las rutas de evacuación.	
	• Tratar de cerrar las ventanas de la dirección de TIC's, para evitar que el fuego se propague.	
	SERVIDORES Y EQUIPOS DE CÓMPUTO	
	• Apagar inmediatamente los servidores.	
	• Apagar inmediatamente los equipos de cómputo.	
	• Dependiendo de la magnitud del incendio, tratar de trasladar los servidores fuera del departamento.	

	• Ubicar el hardware, software y documentos importantes, de acuerdo a su responsable de equipo en lugares seguros.	
	EXTINTORES	
	• Si el incendio es pequeño, apagarlo, utilizando extintores. Si el fuego es de origen eléctrico no intentar apagarlo con agua.	
	• Utilizar los extintores por personal capacitado y responsable del rol.	
	• El personal de la dirección de TIC's deberá controlar los medios de extinción a su alcance.	
	GENERALES	
	• Evitar pánico generalizado, conservar la calma: No gritar, No correr, No empujar.	
	• Realizar evacuación del área si el fuego está fuera de control y comunicarse inmediatamente con el departamento de bomberos para controlar la emergencia.	
	• Evitar no interferir las labores del personal especializado en incendios, dejar actuar a los profesionales en extinguir el incendio.	
2. Terremoto	**INFRAESTRUCTURA**	• Departamento de dirección de TIC's. • Departamento de análisis y gestión de riesgos.
	• Tratar de desconectar el fluido eléctrico.	
	• Abrir las puertas y ventanas del depto. de TIC's.	
	• Evacuar el área de trabajo de acuerdo a las disposiciones de los directores responsables, mediante las rutas de emergencia establecidas durante los simulacros.	
	• Seguir de forma correcta la señalización de rutas, zonas de agrupamiento del personal, entre otros.	
	SERVIDORES Y EQUIPOS	
	• Apagar los servidores.	
	• Apagar los equipos de cómputo.	

	• Trasladar el hardware, software y documentos importantes, de acuerdo a su responsable de equipo a lugares seguros.	
	GENERALES	
	• Realizar la evacuación del lugar en orden, conservando la calma: NO gritar, NO correr, No empujar, y dirigirse a una zona segura previamente identificada.	
	• Manifestar los primeros auxilios al personal afectado si fuese necesario.	
	• En caso de que el desastre lo necesite, resguardarse debajo de un escritorio.	
3. Fallas en las comunicaciones de datos	**GENERALES**	
	• Revisar y probar la integridad de las comunicaciones de datos.	• Departamento de dirección de TIC'S, Área de infraestructura y comunicaciones.
	• Reemplazar equipos, si el fallo es derivado por mal funcionamiento o remitirse a póliza de mantenimiento.	
	• Reiniciar y reconfigurar el equipo inmediatamente, si resulta ser un problema de configuración.	
	• Realizar una evaluación de las fallas de comunicación de datos.	
	• Declarar en estado de contingencia hasta verificar aspectos importantes de la red y corregirlos.	
	• Realizar un registro de soporte al usuario, identificando el tipo de fallo y la solución brindada.	
4. Daños por agua	**INFRAESTRUCTURA**	• Departamento de mantenimiento. Departamento de dirección de TIC's.
	• Desconectar el fluido eléctrico.	
	• Trasladar los respaldos de datos, programas, manuales y claves, al centro de respaldo u oficinas alternas correspondientes con el propósito de reiniciar operaciones si es necesario.	
	• Abrir las puertas y cerrar las ventanas para impedir el ingreso del agua al depto. de TIC's.	
	SERVIDORES Y EQUIPOS	
	• Apagar los servidores.	

	• Apagar los equipos de cómputo.	
	• Cubrir con bolsas de plástico impermeables los servidores y documentos importantes que puedan mojarse.	
	GENERALES	
	• No tocar cables y tomacorrientes.	
	• Mantenerse en alerta y en sintonía con la radio y la televisión al comunicador de autoridades competentes.	
	• Atender las indicaciones de las autoridades, conservar la calma y prepararse para evacuar, si llega a ser necesario.	
5. Cortes de suministro eléctrico	**CORTE DE ENERGÍA EN LAPSOS CORTOS CONSECUTIVOS**	• Departamento de dirección de TIC's. • Departamento de electricidad.
	• Monitorear el UPS cada 20min, para programar acciones mayores.	
	• Valorar la decisión de dar de baja los equipos activos y/o servicios para evitar daños y/o pérdida de información y de equipos.	
	• Comunicarse con servicios generales para la supervisión de la Planta de emergencia, en caso de contar con una.	
	CORTE DE ENERGÍA NO MAYOR A UNA HORA	
	• Monitorear el UPS cada 10min, para programar acciones mayores.	
	• Apagar los equipos no prioritarios como impresoras, monitores o PC que no demanden su uso.	
	• Contar con los procedimientos para dar de baja los equipos activos.	
	CORTE DE ENERGÍA NO MAYOR A UNA HORA	
	• Preparar el apagado de los equipos prioritarios.	
	• Monitorear el UPS cada 5min, para programar acciones mayores.	
	• Dar aviso de la contingencia a los usuarios prioritarios.	

6. Fallas en la climatización	**GENERALES**	• Departamento de dirección de TIC's: centro de datos, oficinas.
	• Reubicar las rejillas del piso, colocarlas correctamente	
	• Alinear las unidades de CRAC, con los pasillos calientes, para optimizar la eficiencia del enfriamiento.	
	• En caso de daño en sistemas de enfriamiento, comunicarse con personal capacitado para su debida revisión.	
	• Si existen problemas de sobrecalentamiento de los equipos informáticos, ajustar las temperaturas de la sala y de los racks del centro de datos.	
	• Informar al director de sistemas el daño y registrarlo inmediatamente.	
	• Reacomodar el cableado del centro de cómputo de forma estructurada para asegurar una circulación de aire apropiada.	
	• Trasladar los equipos a un área idónea de climatización hasta solucionar los problemas de enfriamiento.	
7. Fallas en protección de archivos	**GENERALES**	• Departamento de dirección de TIC's: área de infraestructura y comunicaciones.
	• Cambiar las contraseñas de seguridad a los sistemas informáticos	
	• Realizar un análisis de toda la red a través de herramientas de escaneo para determinar intrusos.	
	• Realizar un análisis completo de las todas las unidades de almacenamiento utilizando sistemas antispyware actualizados para detectar espías.	
	• Reforzar la seguridad de los sistemas firewalls	
	• Restaurar los Backups de los sistemas y archivos para reanudar los servicios de ser necesario	

8. Virus, daño de información	**GENERALES**	• Departamento de dirección de TIC's
	• Desconectar el equipo de la red de la institución	
	• Verificar si el equipo se encuentra infectado, mediante un análisis rápido, utilizando un detector de virus actualizado.	
	• Realizar un análisis completo a modo prueba de errores, eliminar el agente causante de la infección	
	• Remover el virus del sistema.	
	• Probar el correcto funcionamiento del sistema.	
	EN CASO DE NO SOLUCIONAR EL PROBLEMA:	
	• Realizar respaldo de datos del equipo.	
	• Formatear el equipo e instalar los aplicativos.	
	• Verificar que no exista riesgo de virus, personalizar el equipo para el usuario.	
	• Conectar el equipo a la red de la institución.	
	• Efectuar las pruebas necesarias con el usuario.	
9. Acceso no autorizado, filtrado de información	**FÍSICO**	• Departamento de dirección de TIC's.
	• Cerrar las puertas principales de la dirección de TIC's.	
	• Llamar a los guardias de seguridad, para su posterior captura e investigación.	
	• De ser necesario llamar a la Policía Nacional.	
	• Verificar las grabaciones del personal sospechoso que estuvo en las instalaciones de la institución.	
	LÓGICO	
	• Deshabilitar servicios prioritarios de los sistemas hasta identificar el sospechoso.	
	• Realizar un escaneo de los puertos por los cuales pudieron haber ingresado al sistema.	
	• Analizar la lista de personas que ingresaron al sistema y verificar sus datos personales para investigaciones.	

10. Robo común	**FÍSICO** • Activar las alarmas de seguridad. • Cerrar las puertas de la salida del departamento de TI. **GENERALES** • Informar del robo al Director de sistemas. • Comunicarse con el guardia de seguridad para emplear una revisión detallada de las posibles ubicaciones del delincuente en toda la institución. • Llamar a la Policía Nacional inmediatamente, e informar el robo. • Mantener la calma, no oponer resistencia, en especial si el ladrón está armado o se nota que esté bajo la influencia de drogas.	• Departamento de dirección de TIC's.
11. Robo de información	**FÍSICO** • Reportar el robo al Director de sistemas. • Cerrar las puertas de salida principal del departamento de TI. • Revisión de archivos log para buscar sospechosos. **LÓGICO** • Realizar un análisis de toda la red a través de herramientas de escaneo para determinar intrusos. • Implementar mayor seguridad en las bases de datos y sistemas. • Cambiar las contraseñas de seguridad. • Reforzar la seguridad del sistema a través de firewalls, antimalware, etc. • Realizar el proceso de restablecer la información de las bases de datos y programas.	• Departamento de dirección de TIC's.
12. Fallas en UPS, respaldo de información.	**GENERALES** • Cambiar las baterías del UPS, y realizar la respectiva prueba. • Instalar un UPS de repuesto en caso de que no exista solución en el equipo. • Si existe conexiones sueltas, revisarlas y reconectar los cables nuevamente, cumpliendo normas de seguridad.	• Departamento de dirección de TIC's. • Departamento de mantenimiento y electricidad.

	• Informar del daño al director para comunicarse con personal de mantenimiento.	
	• Aplicar mecanismos de copias de seguridad, para verificar el estado de la copia.	

Tabla 28. Actividades de seguridad durante el riesgo.

4.10.5.3. Salvaguardas después del riesgo

Riesgo	Salvaguardas	Área responsable
1. Fuego	**INFRAESTRUCTURA** • Realizar la evaluación de daños ocasionados por el fuego sobre las instalaciones, físicas, eléctricas, áreas de trabajo documentos, estanterías, etc. • Probar los equipos para determinar el grado de daños. • Realizar un inventario general del personal y equipos, o recursos afectados, indicando el estado de operatividad de los mismos. • Reanudar las operaciones de preferencia en otras oficinas, en caso de que se requiera. • Realizar limpieza de las áreas afectadas por el incendio. • Verificar la infraestructura del centro de cómputo y determinar si está en condiciones de ser utilizada normalmente. • El director de sistemas deberá reunirse con sus inmediatos superiores para analizar daños, y determinar si es posible o no continuar utilizando las instalaciones y/o por cuánto tiempo se deberá operar fuera de las mismas. • Determinar las ubicaciones alternas de las áreas y el control de las actividades por parte del director de sistemas.	• Departamento de dirección de TIC's. • Departamento de electricidad. • Departamento de análisis y prevención de riesgos.

	• Tomar medidas correspondientes en caso de haber personal afectado físicamente que este incapacitado para continuar con los servicios, para impedir que afecte en las actividades diarias.	
	• Definir al personal que apoyará en la recuperación, retiro de documentos, equipos informáticos, por parte del director de sistemas.	
	SERVIDORES	
	• Comprobar en estado se encuentran los servidores, racks y bastidores y emitir un informe completo detallado.	
	• Restablecer respaldos en caso de ser necesario.	
	• Reanudar los sistemas y servicios del depto. de TIC's.	
	• Efectuar pruebas en los servidores y equipos informáticos para comprobar su funcionalidad.	
2. Terremoto	**INFRAESTRUCTURA**	• Departamento de dirección de TIC's. • Departamento de análisis y gestión de riesgos.
	• Evitar colocarse sobre cables eléctricos caídos o sueltos.	
	• Revisar daños en techos, tumbado dañado, grietas en paredes, escombros, vidrios rotos, daño en puertas y ventanas, daños en lámparas, etc. del depto. de TIC's y confirmar si es adecuado habitarla.	
	• Localizar fugas de agua, líneas eléctricas rotas, drenajes colapsados, procurar repararlos.	
	GENERALES	
	• Prestar primeros auxilios en caso de heridos, si es posible de lo contrario, buscar ayuda inmediata.	
	• Mantenerse alerta siempre a replicas sísmicas.	

	• Realizar evaluación de daños y pérdidas de equipos informáticos a la dirección de TIC's y poder solicitar asistencia necesaria.	
	• Efectuar inventario general de documentación, personal, equipos, o recursos afectados, indicando el estado de funcionalidad.	
	• Limpiar las áreas afectadas por el sismo.	
	• Mantenerse informado mediante medios de comunicación de avisos por parte de las autoridades.	
	SERVIDORES	
	• Comprobar en estado se encuentran los servidores, racks y bastidores y emitir un informe completo detallado.	
	• Restablecer respaldos en caso de ser necesario.	
	• Reanudar los sistemas y servicios del depto. de TIC's.	
	• Efectuar pruebas en los servidores y equipos informáticos para comprobar su funcionalidad.	
3. Fallas en las comunicaciones de datos	**GENERALES**	• Departamento de dirección de TIC'S, Área de infraestructura y comunicaciones.
	• Analizar los equipos de comunicación verificando su estado de funcionalidad y emitir informes completos sobre fallas.	
	• Comprobar conexiones de red de servidores a la red LAN.	
	• Restaurar respaldos en caso de ser necesario.	
	• Hacer pruebas y comprobaciones.	
4. Daños por agua	**ÁREA FÍSICA**	• Departamento de mantenimiento.
	• Limpiar y secar las instalaciones con el propósito de reanudar las operaciones lo más rápidamente posible	

	• Verificar los daños causados por la inundación, como documentos, archivos, equipos informáticos y otros accesorios, con el respectivo personal, asignado por el director de sistema	• Departamento de dirección de TIC's.
	• Preparar un informe escrito detallando los daños ocurridos en las instalaciones y equipos.	
	• Evitar utilizar las instalaciones eléctricas hasta que hayan sido revisadas por un experto.	
	• Realizar la evaluación de pérdidas y daños de los equipos para informar a la Dirección de Sistemas y poder solicitar la asistencia necesaria.	
	• Realizar un inventario general de la documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos.	
	SERVIDORES	
	• Verificar el estado de los servidores y emitir un informe completo y detallado.	
	• Restaurar respaldos de ser necesario.	
	• Reanudar los sistemas y servicios de la dirección de TIC's.	
	• Realizar pruebas y comprobar su funcionalidad.	
5. Cortes de suministro eléctrico	**GENERALES**	• Departamento de dirección de TIC's. • Departamento de electricidad
	• Establecer un tiempo mínimo (depende de la magnitud de la contingencia) para restablecer los equipos informáticos y los servicios.	
	• Restablecer los equipos informáticos y los servicios que se dieron de baja, en forma paulatina.	
	• Verificar el correcto funcionamiento de los equipos informáticos y los servicios de la Institución.	

	• Notificar a los usuarios afectados el restablecimiento de los servicios y su condición. • Evaluar los daños de los equipos activos, planta de emergencia (en caso de contar con una), y UPS. • Verificar que la planta de energía cuente con combustible necesario, y se active en su momento, en caso de contar con una.	
6. Fallas en la climatización	**GENERALES** • Realizar inventario de activos y daños producidos. • Proporcionar un ambiente de confort en el personal de la dirección de TIC's. • Instalar dispositivos para aumentar la circulación de aire. • Organizar los racks, el cableado y realizar pruebas en el sistema de enfriamiento. • Realizar un inventario general de la documentación, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos.	• Departamento de dirección de TIC's: centro de datos, oficinas
7. Fallas en la protección de archivos	**GENERALES** • Identificar los archivos que fueron sustraídos y hacer un informe completo y detallado de los mimos. • Probar la funcionalidad de los archivos sustraídos. • Realizar una evaluación de los sistemas de seguridad a fin de aplicar correctivos.	• Departamento de dirección de TIC's: área de infraestructura y comunicaciones.
8. Virus, daño de información	**GENERALES** • Verificar los archivos que fueron infectados por el virus informático. • Verificar si los archivos infectados sufrieron alteraciones. • Verificar si el virus afecto a los servidores de la institución, y tomar las medidas respectivas.	• Departamento de dirección de TIC's

9. Acceso no autorizado	**FÍSICO Y LÓGICO** • Presentar un informe detallado del estado de los equipos de cómputo. • Presentar un informe detallado del estado de la información más importante.	• Departamento de dirección de TIC's.
10. Robo común	**GENERALES** • Revisar las grabaciones de las cámaras de vigilancia para identificar al sospechoso. • Aplicar las pólizas de seguro para servidores y equipos por parte de la Dirección Administrativa de la UPSE, así como garantías por medio de los proveedores encargados de la renovación de equipos en caso de daños. • Realizar la evaluación de pérdidas y daños de los equipos para informar a la Dirección de Sistemas y poder solicitar la asistencia necesaria. • Realizar un inventario general de documentación, personal, equipos, etc. y/o recursos afectados, indicando el estado de operatividad de los mismos.	• Departamento de dirección de TIC's.
11. Robo de información	**GENERALES** • Verificar si la información extraída es valiosa para la institución y causará un gran impacto. • Verificar la vía que utilizaron para efectuar el robo y aplicar los correctivos. • Analizar los posibles sospechosos de robo de información. • Reforzar áreas de vulnerabilidad de red. • Verificar el inventario general de la documentación extraviada.	• Departamento de dirección de TIC's.

12. Fallas en UPS, (respaldo de información)	**GENERALES**	• Departamento de dirección de TIC's. • Departamento de mantenimiento y electricidad.
	• Mantener un respaldo "in situ" para mayor facilidad de recuperación, y otro respaldo fuera de las instalaciones de la empresa.	
	• Realizar respaldo de información sin hacer modificaciones a los datos objeto de la copia, de preferencia fuera del horario laboral.	
	• Utilizar una unidad de tape alimentada automáticamente mediante software de respaldo.	
	• Analizar políticas de seguridad para respaldos de información.	

Tabla 29. Actividades de seguridad después del riesgo.

4.11. Estado del riesgo

En este punto se busca analizar los datos recopilados en las actividades anteriores para evaluar principalmente el estado del riesgo que se considere importante. Para aquello será necesario calcular el riesgo residual para mantener una estimación de valores a presentarse después de haber realizado el proceso de mitigación de los mismos. Esta actividad consta principalmente de dos aspectos importantes, constan como parámetros que serán usados para la obtención del riesgo residual:

- El grado de manifestación de los riesgos inherentes.
- La gestión de mitigación establecida por la administración.

A partir de la determinación del riesgo residual, los Directivos y Jefes de Tic's podrán tomar las mejores decisiones en cuanto a continuar o a desertar el proceso en dependencia al nivel del riesgo, a implementar nuevos controles y administrar medidas de contingencia para evaluar las pérdidas en relación a un análisis de económico, todos estos aspectos en función de mejorar la disponibilidad, confiablidad, eficiencia e integridad de la información.

4.11.1. Riesgo residual

Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de riesgo que se denomina residual [10].

El cálculo del riesgo residual se centra en la metodología más utilizada por varias instituciones a nivel mundial, la misma que implementa una matriz de evaluación y respuesta entre riesgos inherentes y el nivel de eficacia de controles asignados a cada uno de los ellos.

La metodología utilizada se encuentra referenciada en el estándar global ISO 27001 donde se establece que el riesgo residual está considerado como un nivel resultante del riesgo que existe después de haber efectuado las salvaguardas necesarias o controles que han sido implementados para la protección de los activos de la información de sus amenazas. El estado de este riesgo se presenta por diversos aspectos en un supuesto caso de que a pesar de la ejecución del plan de mitigación existan pequeños aspectos de demanden aun inseguridades.

Sin embargo, en este plan de recuperación ante desastres informáticos se considera absolutamente todas las medidas o salvaguardas de protección y políticas de seguridad para cada riesgo, y se recomienda que sea ejecutado con la debida responsabilidad por parte de los directivos del departamento de tecnologías de información y comunicación de la UPSE.

Una vez manifestado esto, es necesario conocer los parámetros a combinarse para estimar el riesgo residual para el proyecto:

- ✓ Establecer correctamente una escala numérica para medir la eficacia de los controles.

- ✓ Establecer correctamente una escala numérica para definir la valoración y el nivel del riesgo residual.

- ✓ Determinar la fórmula matemática para apreciar y comprobar el nivel de exposición del riesgo residual.

4.11.2. Escala numérica para medir eficacia de controles

Después de que los riesgos han sido valorizados es indispensable determinar el nivel de eficacia de los controles establecidos y poder evaluar la calidad de la gestión en la institución.

Los encargados de ejecutar los controles existentes tienen como actividad valorar la eficacia de los mismos de acuerdo a los resultados obtenidos de las medidas de seguridad preventivas aplicadas, al buen criterio y a la guía apropiada para la mitigación del riesgo identificado.

Las escalas de valoración de efectividad de los controles de seguridad preventivos a los riesgos estimados se ajustan específicamente a las siguientes opciones numéricas:

EFICACIA DEL CONTROL	
Control	**Efectividad**
Destacado	5
Alto	4
Medio	3
Bajo	2
Inexistente	1

Tabla 30. Escalas de eficacia de controles. Fuente: ISO 27001:2013.

4.11.3. Valoración del riesgo residual

Para determinar el nivel de exposición del riesgo residual en la institución fue obligatorio un análisis sistematizado mediante escalas numéricas para posicionar al riesgo residual en niveles desde aceptable, con valores menores a 3, hasta inaceptable, con valores mayores a 14 dependiendo de la matriz de principal anteriormente evaluada.

ESTIMACIÓN DEL RIESGO RESIDUAL	
Nivel de Riesgo Residual	**Valor**
Inaceptable	> 14
Importante	9 a 14
Tolerable	3 a 8
Aceptable	< 3

Tabla 31. Valoración de Riesgo Residual. Fuente: ISO 27001:2013.

Las escalas mencionadas están relacionadas con los colores utilizados en la matriz de riesgos inherente visualizada anteriormente, con la finalidad de constituir a la clasificación de la cuantificación del riesgo residual, y obtener niveles reales de los mismos dentro del departamento

4.11.4. Fórmula general del riesgo residual

El valor residual es el resultado de la división del nivel de riesgo inherente sobre el valor de efectividad de los controles.

Riesgo inherente es un factor de riesgo intrínseco de cada actividad y nace de la exposición y la incertidumbre de probables sucesos negativos que producen afectaciones en la rentabilidad de la institución.

La fórmula general empleada para el cálculo del riesgo residual está basada en una metodología de evaluación referenciada a la norma ISO 27001:

$$\boldsymbol{Riesgo\ residual} = \frac{nivel\ de\ riesgo\ inherente}{control\ (eficacia)}$$

Figura 24. Fórmula general del riesgo residual. Fuente: ISO 27001:2013.

4.11.5. Cálculo de riesgo residual

La evaluación del riesgo residual está relacionada con el valor total del nivel de los riesgos inherentes que fueron mitigados con anterioridad por medio de medidas preventivas y correctivas y por la valorización de efectividad de cada control ya implantado.

Es importante considerar que en la evaluación del riesgo inherente lo que se aprecia es el nivel de gravedad de las supuestas amenazas sin aplicar ningún tipo control por lo que reflejan una situación irreal, sin embargo, lo que se deriva de realizar el análisis de riesgos inherentes es la seguridad de estar contemplando todas las posibles amenazas que podrían llegar a materializarse e interferir con las operaciones y con el cumplimiento de los objetivos de la organización.

La tabla 32 especifica la calidad de gestión, la evaluación y los niveles de riesgos residuales obtenidos en la dirección de TI después de haber realizado el proceso de mitigación, estimando la situación real a través de la cuantificación de los mismos mediante la importancia de la efectividad en controles propuestos.

CALIDAD DE GESTIÓN							
Riesgos Inherentes	**Nivel de Riesgo**	**Medidas de Control**		**Efectividad**		**Promedio de Eficacia**	**Riesgo Residual**
Fuego	**16 Grave**	control 1	control 17	3	4	**2,66**	**6,02 Tolerable**
		control 2	control 18	3	3		
		control 3	control 19	2	3		
		control 4	control 20	3	2		
		control 5	control 21	1	2		
		control 6	control 22	2	3		
		control 7	control 23	2	3		
		control 8	control 24	2	2		
		control 9	control 25	1	4		
		control 10	control 26	1	1		
		control 11	control 27	3	1		
		control 12	control 28	4	2		
		control 13	control 29	3	3		
		control 14	control 30	4	4		
		control 15	control 31	5	2		
		control 16	control 32	4	3		

Terremoto	**16 Grave**	control 1	control 7	3	1	**2,64**	**6,07 Tolerable**
		control 2	control 8	2	2		
		control 3	control 9	4	3		
		control 4	control 10	2	3		
		control 5	control 11	3	3		
		control 6		3			
Fallas en las comunicaciones	**10,8 Importante**	control 1	control 9	4	3	**3,47**	**3,12 Tolerable**
		control 2	control 10	3	5		
		control 3	control 11	4	3		
		control 4	control 12	2	4		
		control 5	control 13	3	3		
		control 6	control 14	4	4		
		control 7	control 15	4	3		
		control 8		3			
Daños por agua	**9 Importante**	control 1	control 10	3	4	**3,18**	**2,83 Aceptable**
		control 2	control 11	4	1		
		control 3	control 12	3	3		
		control 4	control 13	3	4		
		control 5	control 14	5	1		
		control 6	control 15	3	4		
		control 7	control 16	2	3		
		control 8	control 17	3	3		
		control 9		5			
Cortes de suministro	**10,5 Importante**	control 1	control 12	1	4	**2,9**	**3,61 Tolerable**
		control 2	control 13	2	4		
		control 3	control 14	1	2		
		control 4	control 15	3	3		
		control 5	control 16	2	1		
		control 6	control 17	3	4		
		control 7	control 18	3	4		
		control 8	control 19	3	2		
		control 9	control 20	3	4		
		control 10	control 21	4	5		
		control 11		3			
Fallas en la climatización	**9 Importante**	Control 1	control 8	4	1	**2,85**	**3,16 Tolerable**
		Control 2	control 9	2	3		
		Control 3	control 10	3	5		
		Control 4	control 11	3	3		
		Control 5	control 12	3	4		
		Control 6	control 13	2	2		
		Control 7		2			

Fallas en la protección de archivos	**10,4 Importante**	control 1	control 5	3	4	**3,75**	**2,77 Aceptable**
		control 2	control 6	2	4		
		control 3	control 7	3	5		
		control 4	control 8	4	5		
Virus, daño de información	**11,2 Importante**	control 1	control 10	3	4	**3,56**	**3,15 Tolerable**
		control 2	control 11	4	4		
		control 3	control 12	3	3		
		control 4	control 13	3	4		
		control 5	control 14	5	2		
		control 6	control 15	4	2		
		control 7	control 16	4	4		
		control 8	control 17	4	4		
		control 9	control 18	4	3		
Acceso no autorizado	**10,8 Importante**	control 1	control 8	4	1	**3,08**	**3,51 Tolerable**
		control 2	control 9	3	4		
		control 3	control 10	2	3		
		control 4	control 11	2	3		
		control 5	control 12	4	3		
		control 6	control 13	3	4		
		control 7		4			
Robo común	**12 Importante**	control 1	control 11	4	3	**3,2**	**3,75 Tolerable**
		control 2	control 12	5	2		
		control 3	control 13	1	3		
		control 4	control 14	5	4		
		control 5	control 15	2	4		
		control 6	control 16	3	3		
		control 7	control 17	2	4		
		control 8	control 18	4	3		
		control 9	control 19	2	4		
		control 10	control 20	1	5		
Robo de información	**9 Importante**	control 1	control 14	3	4	**2,81**	**3,21 Tolerable**
		control 2	control 15	2	4		
		control 3	control 16	2	3		
		control 4	control 17	2	4		
		control 5	control 18	3	2		
		control 6	control 19	4	3		
		control 7	control 20	3	2		
		control 8	control 21	1	3		
		control 9	control 22	2	3		
		control 10	control 23	3	3		
		control 11	control 24	3	2		
		control 12	control 25	4	3		
		control 13	control 26	4	1		

Fallas en UPS, respaldo de información	**9 Importante**	control 1	control 5	5	2	**3,43**	**2,63 Aceptable**
		control 2	control 6	2	4		
		control 3	control 7	3	4		
		control 4		4			
Perfil de Riesgo (Promedio Total de riesgo residual) :							**3,65 Tolerable**

Tabla 32. Riesgos Residuales.

Resultados Obtenidos:

- Mediante el análisis de gestión del riesgo residual se obtuvieron dos clasificaciones de riesgos ubicados en el nivel de "Tolerable", exponiendo valores mayores a 3 hasta menores de 7 y "Aceptable" con valores menores a 3.

- El mayor nivel de valor residual recae sobre la amenaza determinada como desastre natural "terremoto" con un valor de 6,07, seguido muy de cerca del factor de riesgo "Fuego" con valor de 6,02 clasificándolos como riesgos residuales Tolerables.

- El menor nivel residual da como resultado a "Fallas en UPS – respaldo de información" con un valor de 2,63 equivalente a riesgo residual aceptable.

- El Promedio de riesgo residual da un total de 3,65.

4.11.6. Fase de seguimiento y monitoreo del riesgo residual

Para asegurar que los riesgos residuales se mantengan en niveles aceptables, se deberá definir mecanismos para efectuar revisiones periódicas del perfil del riesgo evaluando así el nivel de desempeño de su gestión por parte del comité de seguridad. La dirección de TI puede aplicar el tratamiento de seguridad para los riesgos buscando proteger los sistemas de información, esto implica que será optimo implementar las siguientes medidas de acuerdo al nivel de riesgo residual.

De acuerdo con los resultados obtenidos con respecto al riesgo residual en la institución, las condiciones y requerimientos para mitigarlos son los siguientes:

NIVEL DE RIESGO RESIDUAL	CONDICIONES	REQUERIMIENTO
INACEPTABLE	Se deberá realizar un informe para comunicar a la autoridad máxima del departamento de TI.	Se requiere acción inmediata al riesgo.
IMPORTANTE	Será necesario informar al director de TI.	Implantar planes para control y mitigación del riesgo.
TOLERABLE	Se deberá analizar si es posible aplicar puntos de control que permitan mitigar el riesgo.	Mantener las variables controladas
ACEPTABLE	Serán fácil remediarlos, debido a que el nivel de riesgos genera impactos bajos.	No se requiere de medidas adicionales.

Tabla 33. Medidas y condiciones para monitoreo del riesgo residual.

CAPÍTULO V

PLAN DE RECUPERACIÓN ANTE DESASTRES INFORMÁTICOS (DRP) PARA EL CENTRO DE DATOS DEL DEPARTAMENTO DE TIC UPSE

5.1. Introducción

Los últimos sucesos o cambios en las tecnologías de información, las variaciones drásticas en la presencia de desastres naturales, errores físicos y lógicos por parte del ser humano, hace que sea indispensable la elaboración de un manual de políticas de seguridad informática que integren procedimientos óptimos que permitan proteger los procesos críticos, funcionales, y las operaciones diarias de la Dirección de Tic's disminuyendo las pérdidas a nivel económico y resguardando la información estrictamente confidencial con la finalidad de mantenerla segura de impactos producidos por amenazas y vulnerabilidades.

Por esta situación los sistemas de información a cargo de la dirección de TIC's de la UPSE, representan el activo principal siendo la información un elemento crítico que es almacenada en los diferentes equipos y aplicativos tecnológicos de la institución.

El desarrollo y ejecución de un plan de recuperación ante desastres informáticos servirá para la administración de la información en relación a lineamientos que resulten esenciales para permitir reanudar la continuidad de las operaciones en los sistemas de información ante eventualidades negativas y reduzcan el tiempo y costo de las mismas.

En este capítulo es necesario analizar las opciones de recuperación, políticas y la disposición de medidas alternas o procedimientos de seguridad para el centro de datos de la organización, con la finalidad de que sea importante considerar algunos factores altamente eficientes como: la alta disponibilidad, la tolerancia a fallos y la calidad del servicio.

5.2. Alcance del plan

Este plan de recuperación está diseñado para la protección exclusiva de los activos más críticos del centro de datos y comunicaciones de la UPSE y sus diferentes herramientas tecnológicas que soportan los procesos principales de los sistemas de información en la organización, que fueron estrictamente evaluados mediante el análisis de riesgos.

5.3. Objetivos del plan

5.3.1. Objetivo General

Definir un conjunto de directrices, actividades o responsabilidades propuestas a la adopción de procedimientos técnicos y lógicos que permitan mantener la continuidad del centro tecnológico de la entidad, en consecuencia, de un desastre o complicación que conlleve a una eventualidad contingente.

5.3.2. Objetivos Específicos

Los objetivos principales o fundamentales del plan de contingencias de TI del centro de datos UPSE son:

- Establecer medidas o procedimientos mediante un documento formal donde consten acciones a tomar frente a un riesgo existente.
- Optimizar recursos generando una solución tecnológica que salvaguarde los sistemas críticos de la organización, conservándolos operativos en el mayor tiempo posible.

5.4. Modelo de seguridad de la información

5.4.1. Introducción

La realidad de todas las organizaciones que manejan sistemas de información es el enfrentamiento diario de enormes cantidades de riesgos e inseguridades

provenientes de distintas fuentes como por ejemplo las nuevas herramientas relacionadas con las TIC's, las mismas deben ser aplicadas para el uso adecuado de los datos.

Todos los recursos y servicios informáticos de la UPSE, son utilizados y están relacionados ampliamente con las redes, infraestructura, y usuarios, ayudando a delimitar políticas de seguridad de normativas vigentes con el fin de proveer la seguridad física y lógica de los activos informáticos que ofrece la organización.

Gracias a estudios realizados sobre gestión de riesgos en capítulos anteriores y a los antecedentes que presenta la institución, es óptima la implementación, mantenimiento y mejoras de las medidas de seguridad que se adapten a las necesidades de las instituciones públicas como lo es la dirección de TIC's de la UPSE, para la adecuada protección de la información. La construcción de políticas, o procedimientos de seguridad adecuados para las diferentes áreas establecidas en el proyecto, están referenciadas al estándar ISO/IEC 27002:2013 tomado como guía base para la elaboración imprescindible del capítulo.

5.4.2. Políticas generales de seguridad

Para la dirección de TIC's es importante contar con políticas y procedimientos obligatorios de seguridad debido a que son aquellos elementos que guiarán el comportamiento profesional de los usuarios directos e indirectos sobre la información almacenada, generada y procesada.

De igual forma los procedimientos permitirán el manejo de mecanismos esenciales para la base de formulación de un plan maestro para la implementación de instrucciones de seguridad como: la identificación y control de acceso, la seguridad física de áreas o instalaciones, respaldos de información y demás planes de contingencias, para que los funcionarios encargados de las áreas críticas del centro de datos puedan actuar eficientemente y mantener a los servicios, recursos tecnológicos y a la información crítica protegidos, así como también respaldar de manera responsable que la institución cumpla con los requisitos legales a los que está expuesta.

5.4.3. Condiciones generales/Obligaciones

Las políticas consideradas en este documento se desarrollarán solamente para el área del centro de datos de la dirección de TIC's de la UPSE, siendo utilizadas por los directivos encargados con el ánimo de mejorar el uso de tecnologías de información a través del cumplimiento de políticas de seguridad. Es importante conocer que el área de Tic's es responsable de la notificación y socialización, actualización y eliminación de las políticas teniendo en cuenta que las mismas deben ser revisadas periódicamente, de preferencia cada año para cerciorarse de que todavía son pertinentes y efectivas. Para la aprobación y formalización de las políticas, se deberá determinar y notificar al personal de alta gerencia administrativa de la institución (rectorado), para que mediante una firma muestre interés de apoyo a la publicación de las mismas.

5.4.4. Responsabilidades

Es responsabilidad principal del Director del departamento de Tecnologías de Información y Comunicación de la UPSE y del Jefe del área de seguridad cumplir estrictamente con:

- Desarrollar, implementar y someter a revisión los procedimientos de seguridad.
- Capacitar a los usuarios internos y difundir de forma correcta por medio de (intranet, email, sitios web oficiales, otros) los procedimientos de seguridad.

5.5. Plan de implementación de políticas de seguridad

En su mayoría las personas involucradas con la seguridad informática piensen que, para desarrollar políticas de seguridad, solo deben de escribirlas y tratar de ponerlas en práctica para llegar a cumplirlas, es por esto que varias políticas de seguridad informáticas fracasan porque se omite lo que implica el verdadero proceso que conlleva crearlas. El proceso para la implementación de políticas está basado en la ejecución de un ciclo de vida que conlleva un marco normativo legal.

5.5.1. Beneficios de implantar políticas de Seguridad Informática

Establecer políticas de seguridad informática escritas, claras, precisas y bien formuladas, ayudara al departamento de dirección de TI de la Universidad Estatal Península de Santa Elena a generar un nivel de confiabilidad aceptable, una protección ideal de los activos informáticos y de la información más significativa.
Es recomendable implantar políticas por varias razones o beneficios como:

- Ayuda al cumplimiento de las regulaciones legales y técnicas de la institución.
- Sirve como guía para el comportamiento profesional y personal.
- Permite aplicar mejores prácticas en el área de trabajo.
- Mantiene un compromiso con la misión de la institución.
- Aumenta la motivación del personal mejorando las relaciones laborales.

5.5.2. Ciclo de vida de una política de seguridad

Es importante conocer que una política de seguridad tiene un ciclo de vida completo adecuado para ponerlo en práctica mientras esté vigente. El proceso de este ciclo incluye algunas actividades como: realizar un esfuerzo de investigación sobre seguridad, el trabajo de escribirlas detalladamente, lograr que los directivos de la institución las acepten, conseguir que sea aprobada, alcanzar que sea esparcida por la organización, informar a los usuarios responsables de la importancia de la misma, ponerlas en práctica, procurar que estén siempre actualizadas y finalmente eliminarlas siempre y cuando dejen de ser útiles o hayan perdido su vigencia.
Mediante este ciclo de vida se evitará el riesgo de tener políticas de seguridad mal desarrolladas, redundantes e incompletas, poco aplicadas e irrelevantes para los directivos de la UPSE. A continuación, se visualiza las etapas y fases de desarrollo correspondiente al ciclo de vida de las políticas de seguridad de la información, las mismas que deben ser aplicadas e implementadas por los Jefes del área de infraestructura, del área de desarrollo de software y del director del departamento de TIC’s.

Figura 25: Ciclo de vida de una política de seguridad.

5.5.3. Responsabilidad y tiempo de ejecución

Dentro de este punto se desplegarán las etapas, el seguimiento de las políticas, y el recurso humano involucrado durante el proceso de legalización, quienes ejecutarán los procesos y el tiempo que se determine para cada una de las fases a cumplirse bajo disposiciones de los directivos del departamento de Tecnologías de Información y Comunicación de la UPSE.

En la tabla 34 se esquematiza las etapas de: planificación, implementación y el plan de ejecución de las políticas de seguridad que deberán seguir los miembros directivos de la institución. El plan de ejecución de las políticas tiene un periodo de tiempo de 42 días, también se ha tomado en consideración las revisiones regulares y periódicas de las mismas, por tal razón se establece un tiempo no mayor a dos meses para que sea implementado dicho plan de forma inmediata en la institución bajo la aprobación de las máximas autoridades competentes de la institución, teniendo como referencia el apoyo del rector y miembros del departamento dirección de TIC’s.

PLAN DE EJECUCIÓN				
Fases	**Política**	**Recurso Humano**	**Ejecución**	**Tiempo**
Creación	Planificación y documentación de la política de seguridad.	Comité de seguridad Informática	Función del Director de Tecnologías de Información, Jefe de telecomunicaciones, deptos. encargados y representante legal de la institución.	20 días
Revisión	Evaluación Independiente de la política.	Comité de evaluación de políticas	Función de auditor informático y director de área comprometida encargados de seguridad informática.	5 días
Aprobación	Obtener aprobación de la política por parte de los directivos.	Máxima autoridad (Rectorado) y Director de TI de la UPSE.	Apoyo por parte de la Máxima administración universitaria a través de emisión de informe sobre las policías a implementar y aprobación del directivo máximo de TI (Ing. Wellington Robys.)	7 días
Comunicación	Difundir la política.	Oficial de seguridad Informática	Dependencias que los proponen.	4 días
Cumplimiento	Implementar la política	Gerencia Informática	Todo el personal de la institución	Regular mente.
Concienciación	Garantiza la concienciación continuada de la política	Comité de seguridad Informática	Directivos, jefes de seguridad.	3 días
Monitoreo	Seguimiento y reportes de la política	Auditor Informático y Jefe de seguridad.	Auditor Informático y Jefe de seguridad.	3 días
Garantía de cumplimiento	Afrontar las contravenciones de la política	Gerencia Informática, Junta directiva y Gerencia de telecomunicaciones	Gerencia Informática, Junta directiva y Gerencia de telecomunicaciones	Regular Mente

Actualización	Revisiones periódicas	Comité de seguridad Informática.	Función del Director de TI, Jefe /telecomunicaciones, deptos. Encargados.	Periódica
Retiro	Prescindir de la política	Comité de seguridad Informática.	Apoyo de la Máxima autoridad universitaria y Director de TI de la UPSE.	Siempre que sea la política no sea útil.

Tabla 34. Plan de ejecución de una política de seguridad.

5.6.Normas y Estándares de seguridad aplicadas a las TIC's

5.6.1. Descripción de la Norma 27002

Esta norma está estructurada en 14 dominios que puntualizan las áreas que se deben tomar en cuenta para garantizar la seguridad de la información, contiene 35 objetivos de control y 114 controles que, no hace falta cumplirlos todos, pero si es necesario tenerlos en cuenta y pensar en una viable aplicación en la institución en caso de que sea posible por el alto grado de importancia y a los objetivos de la dirección de TI.

Según la ISO 27002 menciona que, "El conjunto de controles, dominios y objetivos de control mencionados están relacionados a la versión ISO/IEC 27002:2013" [28].

El estándar está enfocado para todo tipo de organizaciones, de diferentes tamaños y para todo tipo o naturaleza, como: pequeñas, medianas y grandes empresas, instituciones comerciales, gubernamentales y sin ánimos de lucro.

Esta nueva versión de la norma aplicada a nuestro proyecto se basa en la aplicación de controles que busquen atenuar el impacto y la probabilidad de ocurrencia de los distintos tipos de riesgos a los que se encuentra expuesta el departamento de dirección d TI.

Cabe mencionar que la información y los datos que dispone la institución, siendo manipulados todos los días son pieza clave considerándose como los activos más

valiosos debido a esto la importancia que ofrece la normativa ISO es optimizar la seguridad de la información teniendo en cuenta la confiabilidad, autenticidad e integridad de la misma. El resumen de los dominios, objetivos y controles del estándar ISO/IEC 27002 está detallado en el Anexo 4.

5.6.2. Selección de controles ISO 27002:2013

La norma pretende proporcionar una guía para el desarrollo de normas de seguridad de la organización y prácticas eficaces de gestión para ayudar a construir la confianza en las actividades inter-organizacionales [29].

Dentro del análisis realizado con respecto al estándar a utilizar y de las consecuencias obtenidas en el proceso de la gestión de riesgos, resulta eficaz determinar la implantación de buenas prácticas como plan de recuperación para protección de activos, brindando seguridad informática necesaria al departamento de TI, por esta razón es importante aplicar el estándar internacional ISO 27002:2013 mediante la selección de controles y dominios escogidos según las necesidades de la organización siendo idóneos para cumplir con el objetivo del plan a desarrollarse y ofrecer una solución eficiente ante la falta de políticas de seguridad y aspectos relacionados con la continuidad del negocio.

La implementación de controles de seguridad permitirá asegurar la disponibilidad y trazabilidad de los activos informáticos, de esta manera la organización obtendrá un excelente prestigio ante la comunidad universitaria ofreciendo servicios de calidad.

Cada una de las políticas formuladas por estándares establecidos deben ser aprobadas por el director de TI y notificadas exponiéndose ante la máxima autoridad de la universidad para autorizar su cumplimiento, y posterior a eso, sea socializada a todos los funcionarios responsables que laboran en la institución.

Para lograr el objetivo del proyecto es necesario encaminarse esencialmente en aplicar tres controles de seguridad, los mismos que fueron seleccionados del portal oficial ISO 27002:2013 [28].

DOMINIO	CONTROL	COMO SE IMPLEMENTARÁ	MÉTRICAS A SEGUIR
Políticas de seguridad	Directrices de la dirección en seguridad de la información.	Manual o Documento de políticas de seguridad de la información que contenga un conjunto coherente de políticas, normas, procedimientos y directrices aplicable para la institución (Dirección de TIC's).	Adopción y cumplimiento de la política en la organización (medido por auditoría, gerencia o autoevaluación).
Seguridad Física y Ambiental	Seguridad de los Equipos	Estándares que aseguren la información centrándose en el centro de procesamiento de datos, considerando áreas vulnerables a tratar.	Inspecciones de seguridad física; instalaciones y equipos, incluyendo actualización regular de medidas correctivas identificadas.
Aspectos de la seguridad de la información en la Gestión de la continuidad del negocio.	Continuidad de la seguridad de la información	Considerar la gestión de continuidad de negocio (Planes de continuidad de negocio), llevándose a cabo las pruebas pertinentes para aumentar la confianza de la dirección de los planes y familiarizar a los empleados relevantes con funciones y responsabilidades bajo condiciones de desastre.	Porcentaje de planes de continuidad de negocio en cada una de las fases del ciclo de vida.

Tabla 35. Dominios seleccionados de normativa ISO 27002.

5.7. Estudio de Factibilidad

El estudio de factibilidad está basado en la disponibilidad de recursos necesarios para llevar a cabo los objetivos o metas del proyecto, los resultados del mismo serán útiles para conocer qué tan viable es el desarrollo e implementación del proyecto y fundamental para la toma de decisiones en la institución. Dentro de esta fase se despliegan algunos análisis que son necesarios para dicho estudio que son: Análisis técnico y Análisis económico.

5.7.1. Análisis Técnico

5.7.1.1. Recursos Humanos

Para el desarrollo del proyecto no se ha considerado la contratación del personal puesto que el recurso humano necesario del departamento de Dirección de Tic's forman parte de la ejecución del mismo. El personal involucrado en el proyecto es:

- Director de TI (Ing. Wellington Robys), MSIA.
- Jefe de Infraestructura (Ing. Fabricio Ramos), MSIA.
- Jefe de desarrollo de Software (Ing. Hernán Conforme), MSc.
- Auditor Informático (Estudiante-Tesista)

5.7.1.2. Recursos Tecnológicos

Los recursos tecnológicos utilizados para el desarrollo y la aplicación del proyecto son los siguientes:

- Equipo Portátil.
- Cámara Digital.
- Impresora, Flash memory.
- Documentación de la Metodología de Análisis y Gestión de riesgos (MAGERIT V3.).
- Documentación del Estándar Internacional ISO/IEC 27002 última versión correspondiente a la 2013 (Para implementación de políticas de seguridad).

5.7.2. Análisis Económico

Los costos a considerarse serán valores estimados para la realización del proyecto. A continuación, se establece un análisis económico que se menciona en la siguiente tabla 36.

ANÁLISIS ECONÓMICO DEL PROYECTO					
Categoría	**Recursos/ Descripción**	**Tipo de Unidades**	**Meses**	**Valor**	**TOTAL**
Recursos Humanos	Auditor Informático	Jornada Mensual ($ 1000)	6	$ 6000	
					$ 6000
Recursos Materiales	Materiales y Suministros (Papelería, Copias, 1 CD)	Costo Mensual 10	6	$ 60	
	Servicios Públicos (Luz, teléfono e internet)	Servicios totales mensuales 70	6	$ 420	
	Transporte	75	6	$ 450	
	Flash Memory	1	--	$ 18	
					$ 948
Recursos Tecnológicos	Norma ISO/IEC 27002:2013 - Tecnología de la información. Técnicas de seguridad. Código de prácticas.	1	--	$110,78	
	Metodología MAGERIT V3 - Guía para Análisis y Gestión de Riesgos	1	--	$ 0	
					$110,78

Tabla 36. Análisis económico del proyecto.

El total de los costos de implementación contemplados para el proyecto tecnológico arrojan como resultados los siguientes valores:

COSTOS TOTALES	Costos
Recursos Humanos	$ 6000
Recursos Materiales	$ 948
Recursos Tecnológicos	$ 110,78
Total	**$ 7.058,78**

Tabla 37. Costos totales del Proyecto.

La guía metodológica que sirvió de gran ayuda para la generación del análisis y gestión de riesgos denominada Magerit v3, no tiene costo alguno por motivos de que es una metodología orientada especialmente al carácter público y su contenido es de acceso libre, todos los manuales correspondientes a la guía se encuentran disponibles en el Portal Oficial de administración electrónica: "https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WUAjcmg1_IU".

5.8. Estructura de recuperación de desastres

En el hecho de presentarse un suceso de riesgo que conlleve a recurrir a las estrategias de emergencia, la organización normal del centro de datos deberá actuar como una organización de emergencia.

La dirección de Tecnologías de Información y Comunicación deberá posponer la estructura organizacional actual y sus operaciones respectivas de un día normal de trabajo, y ejercer una estructura de funciones para el plan de recuperación, trabajando en unión para el restablecimiento de las operaciones en un tiempo adecuado. Resulta adecuado proponer una estructura organizacional general incluyendo los roles y responsabilidades de emergencia apropiados al departamento de dirección de Tecnologías de Información y comunicaciones para la correcta ejecución del plan de recuperación ante desastres informáticos.

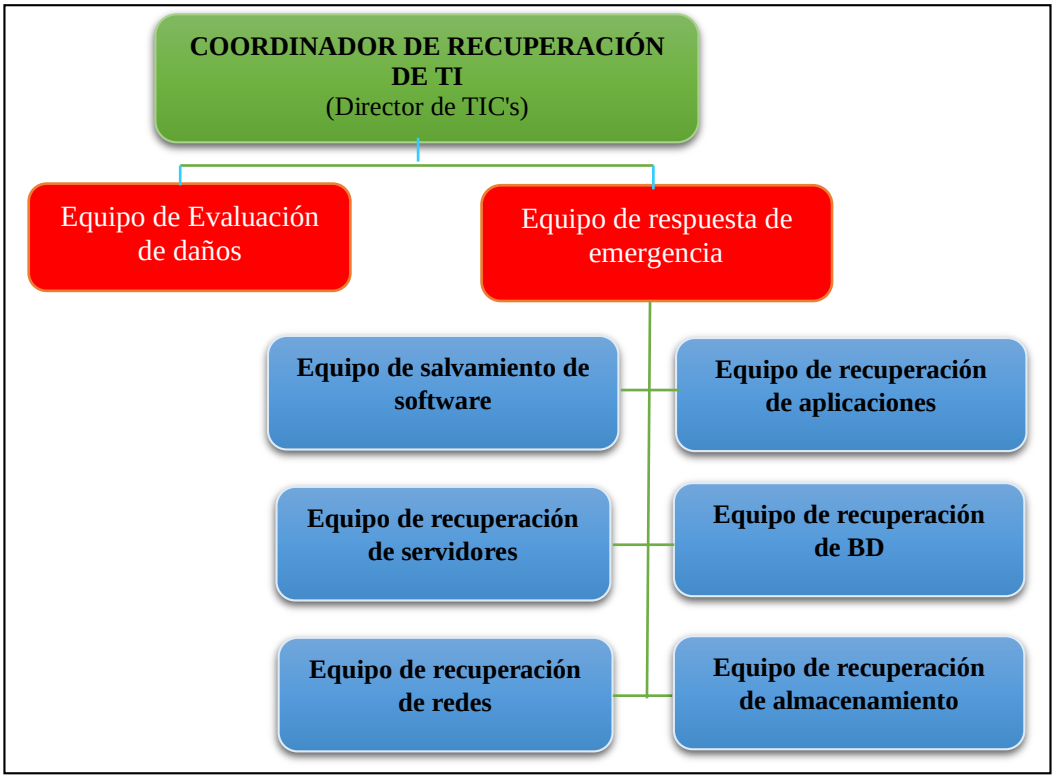


Figura 27. Estructura propuesta organizacional de recuperación.

5.8.1. Roles y Responsabilidades

5.8.1.1. Coordinador de recuperación de TI

La coordinación de recuperación de TI será compromiso del Director de tecnologías de información y comunicación quien definirá absolutamente todas las normas, políticas y procedimientos a desencadenarse durante un suceso de emergencia y al mismo tiempo tendrá como responsabilidad el cumplimiento de todas las acciones a tomarse de acuerdo al plan de recuperación. Entre sus responsabilidades se mencionan las siguientes:

- Sistematizar, administrar y decidir respecto a medidas o estrategias a tomarse en un escenario de contingencia dado.
- Tomar la decisión de activar el plan de recuperación de desastres TI.
- Proveer liderazgo general al equipo de recuperación de desastres mediante las personas involucradas en el proceso de recuperación.
- Regir al personal necesario durante la situación de contingencia y supervisar sus actividades.

- Evaluar la amplificación del desastre y sus resultados negativos potenciales sobre la infraestructura tecnológica.
- Informar a la alta dirección de la organización acerca del evento de desastre, el progreso de la recuperación y posibles problemas ocurridos durante la ejecución del plan.
- Documentar los incidentes de desastres y las actividades realizadas para lograr la recuperación de las operaciones.
- Monitorear la ejecución de los procedimientos de recuperación y asegurar que el cronograma y las prioridades establecidas se cumplan.
- Controlar el proceso de recuperación de infraestructura de TI en el centro de datos alterno.
- Contactar a los proveedores para el hardware de reemplazo para sistemas afectados.
- Asistir a las reuniones del estado de la recuperación y comunicar al personal las necesidades y prioridades.
- Declarar el evento de culminación y cumplimiento de la ejecución de las operaciones del plan de recuperación de desastres, cuando las operaciones del centro de datos primario hayan sido restablecidas.

5.8.1.2. Equipo de evaluación de daños

Las responsabilidades de este equipo son:

- Identificar los activos informáticos de la organización.
- Identificar y evaluar las amenazas y vulnerabilidades.
- Realizar documentación o manual de evaluación final sobre los daños y acciones de respuesta.

5.8.1.3. Equipo de Salvamiento de Hardware

Las responsabilidades de este equipo son:

- Identificar los elementos de hardware que hayan sido dañados por una contingencia.

- Coordinar con los proveedores de hardware el cumplimiento de los contratos de manteniendo, de garantía y niveles de soporte.
- Participar en las instalaciones de los sistemas operativos que realicen los proveedores.
- Verificar el correcto funcionamiento de los elementos de hardware que hayan sido restaurados o reemplazados por los proveedores.

5.8.1.4. Equipo de Salvamiento de Software

Las responsabilidades de este equipo son:

- Identificar los servicios, procesos, bases de datos y aplicaciones que hayan sido afectados por una contingencia.
- Instalar, configurar y ajustar todo el software que haya sido dañado por una contingencia.

5.8.1.5. Equipo de Salvamiento de redes

Las responsabilidades de este equipo son:

- Identificar los elementos de comunicaciones que hayan sido dañados por la contingencia y detectar los problemas de conectividad de los equipos del CPD y determinar las causas.
- Coordinar con el responsable los cambios que haya que realizar en las comunicaciones que no sean internas del centro de cómputo para que los usuarios puedan seguir utilizando los servicios. Y verificar el correcto funcionamiento de los elementos de comunicaciones y la conectividad general para que los usuarios puedan acceder a los recursos del CPD.

5.9. Plan de recuperación de desastres

El plan de recuperación ante desastres es un elemento que favorece a la práctica efectiva de medidas de seguridad que cubra datos, hardware y el software crítico

para garantizar un proceso de reparación adecuado de la funcionalidad de la institución luego de una emergencia. El paso inicial dentro del plan es la identificación del personal encargado de crear y coordinar las funciones del mismo al momento de su ejecución. Las acciones a efectuarse se enfocan en la elaboración de políticas de seguridad.

5.9.1. Información de contacto del equipo de recuperación

Cuando se presente una interrupción o incidente de contingencia, es necesario realizar una cadena de llamadas para localizar y notificar de manera rápida y eficiente a los miembros responsables del plan. En tabla 38 se encuentran los datos de contacto más importantes y de fácil acceso, así como también el cargo que desempeña cada miembro responsable.

NOMBRE	CARGO	E-MAIL
Ing. Wellington Robys, MSIA.	**(Director de TIC's).** Coordinador de recuperación TI. Equipo de Evaluación de daños.	wrobys@upse.edu.ec
Ing. Fabricio Ramos, MSIA.	Equipo de Salvamiento de Redes	framos@upse.edu.ec
Ing. Hernán Conforme, MSc.	Equipo de salvamiento de software, aplicaciones y BD.	hconforme@upse.edu.ec
Ing. Andrés Villao, MGTI.	Equipo de salvamiento de software, aplicaciones y BD.	avillao@upse.edu.ec
Ing. José Perero.	Equipo de salvamiento de software, aplicaciones y BD.	jperero@upse.edu.ec
Lsi. Fráncis Quijano.	Equipo de salvamiento de Hardware	fquijano@upse.edu.ec

Tabla 38. Información de contacto de equipo DRP.

Los medios de comunicación que podrían utilizarse en estos casos son:

- Persona a persona.
- Telefonía fija o celular.
- Correo electrónico.

5.9.2. Pruebas del Plan

Para garantizar la efectividad del plan se recomienda generar actividades de funcionamiento y ejercicios de capacitación del plan 2 veces al año correspondientes a pruebas semestrales para conocer la correcta labor del mismo. Sin embargo, varias instituciones adoptan también la actualización del plan cuando la situación lo requiera independientemente de la fecha de revisión anual.

Los ejes principales que deben someterse a pruebas regulares son: las comunicaciones, la recuperación de datos y la recuperación de las aplicaciones, los demás factores a ser evaluados pueden variar dependiendo de los objetivos de la institución con respecto al tiempo y a los recursos de restauración.

5.9.3. Actualización Periódica de Plan

Sobre el coordinador de recuperación de TI y el líder de seguridad cae la responsabilidad de realizar la actualización adecuada al DRP en caso de ser necesario, además serán los encargados de comunicar a todos los usuarios correspondientes las nuevas versiones del plan. Es necesario actualizarlo como mínimo una vez al año.

El mantenimiento al DRP se debe realizar cuando:

- Se transcurre un año desde la última actualización.
- Los resultados de auditoria informática indiquen el posible mantenimiento.
- Se han dado cambios en las plataformas tecnológicas.
- Los procedimientos y resultados de pruebas requieran actualización del DRP.
- Existan cambios en el personal encargado de ejecutar el DRP.

5.10. Guía para el establecimiento del Plan de Políticas de seguridad

5.10.1. Políticas Generales de Seguridad Informática

Las políticas generales de seguridad formaran la base principal para mantener los recursos y sistemas tecnológicos efectivos y en completo funcionamiento en el departamento de Dirección de Tecnologías de Información. El desarrollo de estas estrategias se enfoca en evaluar los controles de la función informática centrándose en el cumplimiento de las mismas para la correcta utilización de los recursos en la institución.

El conjunto de todas las políticas se encuentra detallado específicamente bajo un Manual de Políticas y Procedimientos de Seguridad Informática que será entregado a la institución para su posterior implementación.

El marco normativo para la elaboración del manual contiene la aplicación de los siguientes estándares:

- Norma internacional ISO/IEC 27001:2013; Tecnología de la información – Técnicas de Seguridad – Sistemas de gestión de la seguridad de la información – Requisitos. (Organización Internacional de Normalización).

- Norma internacional ISO/IEC 27002:2013; Tecnología de la información – Técnicas de Seguridad – Código de prácticas para los controles de seguridad de la información. (Organización Internacional de Normalización).

- Magerit - v.3 Metodología de análisis y gestión de riesgos de los sistemas de información. (Consejo Superior de Administración electrónica).

- Serie CCN-STIC-821 Normas de Seguridad en el Esquema Nacional Seguridad del Centro Criptológico Nacional.

- Normativa Sans (Recursos de políticas de seguridad). El objetivo final del Instituto SANS es ofrecer todo lo necesario para el rápido desarrollo e implementación de políticas de seguridad de la información [30].

En definición con esta política, se debe considerar:

- La seguridad en el uso de la información.
- Requerimientos mínimos para el uso de correo electrónico.
- Directrices para el proceso de antivirus.
- Directrices para construcción de contraseñas.
- Directrices para protección de contraseñas.
- Procedimientos formales para la validación y elaboración de copias de seguridad.
- Requisitos mínimos de seguridad para configuración de servidores.
- Directrices para instalación de software.
- Criterios de seguridad para aplicaciones web.

5.10.2. Políticas de seguridad Física y del entorno

Políticas elaboradas para seguridad física y del entorno destinados a ciertos componentes que generalmente protegen físicamente cualquier recurso del sistema, desde el más pequeño dispositivo hasta una cinta de backup de información que existe en la institución.

Es necesario la implementación de políticas de seguridad física con la finalidad de impedir el acceso por personas no autorizadas, el daño a la infraestructura o recursos de la información de sucesos graves como: desastres naturales, alteraciones del entorno, y más que afecten los datos del departamento.

Estas políticas se encuentran desarrolladas bajo la norma BS 7799-2 incorporada a la serie ISO/IEC 27002 para gestionar el área física y la seguridad en los equipos del centro de datos de la dirección de TI.

En definición con esta política, se debe considerar:

- Controles para instrucción de seguridad en el perímetro físico.
- Seguridad para controles de acceso físico a instalaciones de TI.
- Directrices de seguridad para los equipos.

- Controles para instalación y mantenimiento de cableado.
- Requisitos para mantenimiento de equipos
- Requisitos mínimos para conservar escritorios limpios en las instalaciones de TI.
- Directrices para seguridad en la red.
- Seguridad en la comunicación inalámbrica.
- Seguridad en equipos de comunicaciones (Router y Switch).
- Requisitos mínimos para control de accesos remotos.

5.10.3. Políticas de seguridad para la Gestión de la Continuidad del Negocio

Las políticas principales para el análisis y gestión de la continuidad de una organización resultan indispensables para el desarrollo de planes de contingencias y contribuyen a la restauración de los recursos y/o activos de información en caso eventualidades o desastre físicos y naturales.

En definición con esta política, se debe considerar:

- Requisititos básicos para el desarrollo de un plan de recuperación ante desastres informáticos (DRP).
- Requisitos básicos considerados para la creación y mantención de un plan de respuesta de seguridad.

CONCLUSIONES

- La aplicación de la metodología MAGERIT versión 3 contribuyó en la ejecución del análisis y gestión de riesgos, permitiendo disminuir la probabilidad de daños, a través de medidas de seguridad que garanticen mejor protección de los servicios informáticos en la institución.
- La documentación del presente proyecto tecnológico favoreció a la dirección de TIC's de la UPSE, debido a que no se cuenta con un plan de contingencias informático que facilite actuar de manera eficiente ante posibles amenazas y permita restaurar las operaciones.
- La incorporación y fusión de normas internacionales ISO 27002:2013, de buenas prácticas como el estándar BS 7799-2, y recursos de seguridad del Instituto SANS, permitieron el desarrollo íntegro del plan de contingencias basado en controles y políticas de seguridad que destaca a toda institución de carácter público como un elemento diferenciador sobre otra por el cumplimiento y responsabilidad en la protección de la información.
- El centro de cómputo de la dirección de TIC's carece de un manual de políticas, normas y procedimientos para gestionar las actividades informáticas y no dispone de sistemas de seguridad apropiados para sus instalaciones.
- Con el desarrollo del proyecto se concluye que la creación de un plan de seguridad no representa un gasto, sino más bien una inversión con el objetivo de conservar la funcionalidad del servicio siempre disponible y evitar grandes pérdidas económicas.

RECOMENDACIONES

- Realizar revisiones periódicas de amenazas, vulnerabilidades y riesgos mediante la aplicación de metodologías idóneas como MAGERIT v3, considerando la documentación del proyecto para realizar mitigaciones futuras.
- Recomendar a la dirección de TIC's, difundir adecuadamente el plan creado y controlar que los funcionarios encargados estén altamente comprometidos con el cumplimiento estricto del plan.
- Tomar en cuenta la documentación de este proyecto como base para el crecimiento del centro de datos de la UPSE, y apelar ante la máxima autoridad universitaria obtener el apoyo para mejorar la infraestructura del cuarto de cómputo, obtener servidores y equipos de comunicación de calidad, e incorporar la seguridad y el control de acceso físico a las instalaciones de TIC's.
- Considerar en la administración de las TIC's la certificación de estándares como: ISO/IEC 27002 Código de buenas prácticas para seguridad de la información, COBIT e ITIL normas para la gestión y control de las TI y de auditoria, y CISCO e IEEE (Estándares internacionales correspondientes a las redes y telecomunicaciones).
- Monitorear, evaluar y realizar las pruebas necesarias del plan de recuperación ante desastres informáticos propuesto para la institución universitaria con el fin de apreciar su nivel de eficiencia y eficacia.
- Actualizar constantemente toda la información (responsabilidades, funcionarios, equipos de recuperación, direcciones, teléfonos, controles, métricas y medidas, etc.) del plan de seguridad según se requiera teniendo como preferencia cada año, debido al constante cambio tecnológico lo que evitara problemas futuros.

REFERENCIAS BIBLIOGRÁFICAS

[1] «ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información». [En línea]. Disponible en: http://www.iso27000.es/sgsi.html. [Accedido: 19-may-2017].

[2] G. B. Urbina, *Introducción a la seguridad informática*. Grupo Editorial Patria.

[3] C. Ramírez y F. Andrés, «Desarrollo e implantación de un plan de contingencia informática para la dirección de tecnologías de la información de la Pontificia Universidad Católica del Ecuador Sede Santo Domingo», sep. 2015.

[4] A. J y J. A. Bertolín, *Seguridad de la información. Redes, informática y sistemas de información*. Editorial Paraninfo, 2008.

[5] «Seguridad Informática - EcuRed». [En línea]. Disponible en: https://www.ecured.cu/Seguridad_Inform%C3%A1tica. [Accedido: 04-ago-2017].

[6] J.-F. CARPENTIER, *La seguridad informática en la PYME: Situación actual y mejores prácticas*. Ediciones ENI, 2016.

[7] G. B. Urbina, *Introducción a la seguridad informática*. Grupo Editorial Patria.

[8] P. A. López, *Seguridad informática*. Editex, 2010.

[9] E. C. Tejada, *Auditoría de seguridad informática. IFCT0109*. IC Editorial, 2015.

[10] M. Á. Amutio Gómez y J. Candau, *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I - Método*, © Ministerio de Hacienda y Administraciones Públicas., vol. volumen I. Madrid.: Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012.

[11] DESONGLES, *Ayudantes Tecnicos. Opcion Informatica. Junta de Andalucia. Temario Volumen Ii.e-book*, Editorial Mad, S.L. MAD-Eduforma.

[12] «PAe - CTT - General - MAGERIT versión 3», 09-mar-2010. [En línea]. Disponible en:

https://administracionelectronica.gob.es/ctt/magerit#.WZCocVHyjIW. [Accedido: 13-ago-2017].

[13] P. C. G. A. publicado 14 May 2013 - 02:52PM, «MAGERIT: metodología práctica para gestionar riesgos», *WeLiveSecurity*, 14-may-2013. [En línea]. Disponible en: https://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/. [Accedido: 11-jul-2017].

[14] M. Á. Amutio Gómez y J. Candau, *MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro II - Catálogo de Elementos*, © Ministerio de Hacienda y Administraciones Públicas., vol. Volumen II. Madrid.: Dirección General de Modernización Administrativa, Procedimientos e Impulso de la Administración Electrónica, 2012.

[15] «Plan de contingencia en seguridad Informática - EcuRed». [En línea]. Disponible en: https://www.ecured.cu/Plan_de_contingencia_en_seguridad_Inform%C3%A1tica. [Accedido: 25-jul-2017].

[16] E. C. Tejada, *Gestión de incidentes de seguridad informática. IFCT0109*. IC Editorial, 2015.

[17] C. G. M. Alonso *et al.*, *COMUNICACIONES INDUSTRIALES: PRINCIPIOS BÁSICOS*. Editorial UNED, 2017.

[18] «Seguridad Informática / Políticas de Seguridad». [En línea]. Disponible en: http://www.segu-info.com.ar/politicas/. [Accedido: 13-ago-2017].

[19] «ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información». [En línea]. Disponible en: http://www.iso27000.es/iso27000.html. [Accedido: 19-may-2017].

[20] «ISO / IEC 27002: 2013 (ES), Tecnología de la información - Técnicas de seguridad - Código de prácticas para los controles de seguridad de la información». [En línea]. Disponible en: https://www.iso.org/obp/ui/#iso:std:iso-iec:27002:ed-2:v1:en. [Accedido: 19-may-2017].

[21] Dirección de Tecnología de Información y Comunicaciones, «NORMAS DE CONTROL INTERNO PARA LAS ENTIDADES, ORGANISMOS DEL

SECTOR PÚBLICO Y DE LAS PERSONAS JURÍDICAS DE DERECHO PRIVADO QUE DISPONGAN DE RECURSOS PÚBLICOS». Contraloria General del Estado de la República del Ecuador.

[22] «SANS Seguridad de la Información Formación | Cibernética Certificaciones | Investigación». [En línea]. Disponible en: https://www.sans.org/. [Accedido: 19-may-2017].

[23] «SANS - Information Security Resources | Information Security Policy Templates | General Policy Templates». [En línea]. Disponible en: https://www.sans.org/security-resources/policies/general#disaster-recovery-plan-policy. [Accedido: 09-abr-2017].

[24] «REPÚBLICA BOLIVARIANA DE VENEZUELA». [En línea]. Disponible en: http://webcache.googleusercontent.com/search?q=cache:http://www.uideporte.edu.ve/WEB/pdf/NormasTrabajosdePregrado.pdf. [Accedido: 13-ago-2017].

[25] F. G. Arias, *El Proyecto de Investigación. Introducción a la Metodología Científica. 6ta. Edición*. Fidias G. Arias Odón, 2012.

[26] A. A. Ibáñez y A. F. A. L. Martín, *El proceso de la entrevista: conceptos y modelos*. Editorial Limusa, 1986.

[27] C. Montoya y Y. An, «Desarrollo e implementación de controles para el dominio de seguridad física y ambiental para la empresa Felmova S.A. usando la norma ISO 27002:2013», may 2017.

[28] «ISO27000.es - El portal de ISO 27001 en español. Gestión de Seguridad de la Información». [En línea]. Disponible en: http://www.iso27000.es/iso27002.html. [Accedido: 06-may-2017].

[29] «Introducción a la ISO 27002 / ISO27002», *Directorio de la norma ISO 27000*. [En línea]. Disponible en: http://www.27000.org/iso-27002.htm. [Accedido: 13-jun-2017].

[30] «SANS - Information Security Resources | Information Security Policy Templates |». [En línea]. Disponible en: https://www.sans.org/security-resources/policies. [Accedido: 07-jun-2017].

ANEXOS

Anexo 1: Entrevista para Análisis y Evaluación de Riesgos Informáticos dirigida al director de TIC'S de la UPSE.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
ESCUELA DE INFORMÁTICA

CUESTIONARIO DE ENTREVISTA #1
(ANÁLISIS Y EVALUACIÓN DE RIESGOS)

Objetivo: Determinar las amenazas y principales riesgos que causen mayor impacto en el Data Center de la UPSE mediante la utilización de la metodología Magerit, para proponer medidas adecuadas ante un desastre en el desarrollo de un Plan de contingencias.

Entrevistado: Director de TIC: Ing. Wellington Robys

Indicaciones: Para identificar las amenazas y riesgos en el centro de datos, requerimos su contribución para el llenado de la siguiente entrevista respondiendo adecuadamente y de forma íntegra y leal el cuestionario de preguntas.

RIESGO 1: INCENDIO (FUEGO)

Con respecto a problemas (fallas de instalaciones defectuosas, inadecuado almacenamiento y traslado de sustancias peligrosas, etc.), que pueden causar pérdidas en equipos informáticos y en la información están las siguientes preguntas:

No.	PREGUNTA	RESPUESTA	Evaluación (Impacto)
1	¿El data center cuenta con un sistema para detección y extinción de incendios?	No.	5
2	¿Existen extintores manuales en buen estado de funcionamiento?	No.	5
3	¿Los extintores se encuentran en sitios estratégicos?	No todos.	4
4	¿Cuantos extintores manuales existen en el data center?	2 extintores.	5
5	¿De qué tipo son los extintores?	CO2/equipos electrónicos.	5

6	¿Cerca del data center existen productos inflamables?	Si.	4
7	¿El personal está capacitado contra incendios?, SI ¿Cada que tiempo?	No.	5
8	¿Las instalaciones eléctricas del data center están en buen estado?	SÍ, casi siempre.	2
9	¿Se cuenta con diagramas eléctricos actualizados?	No.	5
10	¿Se cuenta con un sistema de tierra adecuado?	Si.	2
11	¿Se cuenta con salidas de emergencias?, SI ¿Cuántas tiene?	No existe.	5
12	¿En la institución existe señalización contra incendio como por ejemplo: (No fumar,), etc.?	No existe.	5
13	¿En caso de incendio, existen mascarás contra gases o sistemas portátiles de oxígeno?	No existe.	5
14	¿Se posee caja de seguridad para respaldos que sea resistente al incendio?	No existe.	5
15	¿Los racks donde se encuentran los servidores están debidamente aterrizados?	No, falta de piso falso.	5
16	¿Los niveles de voltaje son adecuados para cada equipo informático?	Si.	2
17	¿Son suficientes las instalaciones eléctricas para la conexión de todo el equipo informático?	Muy pocas.	4
18	¿Se dispone de números de emergencia en caso de presentarse un incendio?	No existen.	5
19	¿Los niveles de temperatura para los equipos informáticos es la indicada?	Varían constantemente.	5
Nivel de Impacto:			**4,36**
			4

RIESGO 2: DAÑOS POR AGUA

Con respecto a inundación que ocasionan destrucción en equipos y archivos, que puede ser causa de mayores desastres en el centro de datos, tenemos las siguientes preguntas:

No.	PREGUNTA	RESPUESTA	Evaluación (Impacto)
	POR LLUVIAS		
1	¿Se encuentra ubicado el data center sobre áreas de baja altura?	No.	2
2	¿El techo de la institución se encuentra en buen estado?	Sí, la mayoría.	2

3	¿El techo de la institución es impermeable?	Si.	1
4	¿Se cuenta con un sistema de drenaje en el data center?	Si.	1
5	¿Se dan lluvias frecuentes en la Institución?	No.	2
6	¿Se tiene planos de distribución de la institución? SI, ¿Están debidamente actualizados?	Si.	1
7	¿Cerca del data center se crean desagües, lagunas o conducciones de aguas causadas por lluvias frecuentes ?	Si.	5
	POR ROTURA DE TUBERÍAS		
8	¿Se encuentra ubicado el sistema de agua potable cerca depto. de TIC?	Si.	5
9	¿Están ubicados los equipos informáticos en lugares estratégicos?	No.	4
10	¿Se realiza mantenimiento preventivo a los sistemas de agua potable en la institución?	Sí.	1
11	¿Los tomacorrientes están en una altura correcta para prevenir cortocircuitos?	No.	5
12	¿Está capacitado el personal del depto. de TIC para actuar frente a casos de inundaciones?	No al 100 %	3
13	¿Se tiene lugares alternos apropiados para el traslado de los equipos informáticos en caso de inundaciones?	No, solo laboratorios de la U.	3
14	¿ El tipo de tuberías y diámetro utilizados para el agua son los adecuados?	Si.	1
15	¿Existe demasiada presión en las tuberías de agua de la institución?	Rara vez.	3
	POR LLAVES ABIERTAS		
16	¿En un corte de agua potable, se mantiene el uso adecuado de los grifos de agua (llaves cerradas)?	30% de control sobre llaves cerradas.	3
17	¿Existen llaves de agua cerca del centro de datos?	Si.	5
18	¿La institución dispone de un departamento equipado para el mantenimiento y revisión de llaves y tuberías?	No.	5
19	¿Existen equipos informáticos dispersos en el suelo?	Si.	5
Nivel de Impacto:			**3**
			3

RIESGO 3: TERREMOTO

Con relación a las pérdidas de equipos y archivos tenemos las siguientes preguntas:

No.	PREGUNTA	RESPUESTA	Evaluación (Impacto)
1	¿La institución se encuentra en una zona sísmica?	Si.	5
2	¿La estructura física del depto. de TIC cumple favorablemente con las normas antisísmicas?	No, existen casos de daños apreciables.	3
3	¿Se cuenta con señalización de seguridad sobre terremotos en la Institución? SI, ¿Cuántas señaléticas tiene?	No.	4
4	¿Se efectúan simulacros de evacuación en la institución? SI, ¿Cada que tiempo?	Nunca.	5
5	¿En el depto. de TIC los accesos y/o vías de evacuaciones son los adecuados?	No.	5
6	¿Existen paredes agrietadas o cimientos en las oficinas del depto. de TIC?	Sí.	4
7	¿Se efectúan charlas constantes sobre medidas de prevención para terremotos?	Rara vez.	4
8	¿El personal se encuentra capacitado para actuar frente a un terremoto?	No.	4
9	¿Se cuenta con dispositivos como radios portátiles para su comunicación oportuna en la Institución?	Si.	1
10	¿Se cuenta con equipos de primeros auxilios en el depto. de TIC? SI, ¿Con cuántos Kits se tiene?	No existe.	3
11	¿Se tiene linternas de mano y baterías en el departamento de TIC?	No existe.	5
12	¿Existen equipos informáticos ubicados sobre el suelo, o en lugares de peligro dentro del depto. de TIC?	Si existen algunos.	5
13	¿Están los objetos de gran tamaño y pesados fijados debidamente al suelo o paredes?	Pocos.	4
14	¿Cerca del data center existen productos inflamables?	Si.	5
15	¿El personal del depto. de TIC, está capacitado para brindar primeros auxilios?	Pocos.	3
16	¿El techo del data center y del departamento está debidamente reforzado según normas establecidas?	Pocos.	3
17	¿Se cuenta con el equipo necesario para protección personal, por ejemplo: (cascos)?	No.	5
Nivel de Impacto:			**4**
			4

RIESGO 4: TSUNAMI

Con relación a las pérdidas de equipos y archivos tenemos las siguientes preguntas:

No.	PREGUNTA	RESPUESTA	Evaluación (Impacto)
1	¿Se tiene la colaboración de un departamento que capacite constantemente al personal para enfrentar un Tsunami? Sí, ¿Menciónelo?	No.	4
2	¿Se cuenta con un plan de evacuación en caso de Tsunami en la Institución?	No existe. Solo conocimientos básicos.	4
3	¿Existen sistemas de monitoreo para detección de Tsunami en la Institución? SI, ¿Menciónelo?	No, Solo redes sociales.	4
4	¿Han existido la presencia de Tsunamis en la provincia de Santa Elena?	No.	3
5	¿En caso de Tsunami, cuáles serían las consecuencias que sufriría el depto. de TIC?	Afectaciones en instalaciones eléctricas, daños en equipos electrónicos, daños en infraestructura.	5
6	¿Podría indicar a qué altura se encuentra la institución sobre el nivel del mar?	A unos 200 o 300m.	1
7	¿Existen lugares de almacenamiento de respaldos en lugares externos de la institución?	No.	5
Nivel de Impacto:			**3,71** **4**

RIESGO 5: CONTAMINACION EN LOS EQUIPOS

Con respecto a la humedad, salinidad y elementos peligrosos que provoquen daños en los equipos informáticos tenemos las siguientes preguntas

No	PREGUNTA	RESPUESTA	Evaluación (Impacto)
1	¿La institución se encuentra cerca de zonas costeras?	No exactamente.	2
2	¿Mencione las medidas preventivas de salinidad para los equipos informáticos?	Mantenimiento preventivo y correctivo.	2
3	¿Cada qué tiempo se realiza mantenimiento preventivo?	Cada 6 meses.	3

4	¿Se dispone de un área separada exclusivamente para el mantenimiento de equipos?	Sí, el área de soporte técnico, pero el espacio es reducido.	3
5	¿Existen diagramas del área para el mantenimiento de equipos?	No.	4
6	¿Existe personal capacitado para realizar este tipo de mantenimiento?	Sí.	1
7	¿Se dispone de herramientas suficientes y adecuadas para realizar dicho mantenimiento?	Si.	1
8	¿Cuáles son las herramientas que utiliza para mantenimiento de equipos?	Destornilladores, guantes, brochas, sopladores, contracleaners, etc.	2
9	¿Los dispositivos de comunicación están ubicados en los sitios correctos, libres de polvo o algún elemento peligroso?	No..	5
10	¿El área donde se encuentra el data center es limpia, libre de materiales de embalaje, madera, cartón o gases?	No.	5
11	¿Los dispositivos de comunicación son los adecuados para el medio en cuanto a salinidad?	Si.	2
12	¿Existe la presencia de humedad en el piso del departamento de TIC?	Poca.	2
	Nivel de Impacto:		**2,7**
			3

RIESGO 6: FALLAS EN LAS COMUNICACIONES DE DATOS

Con respecto a errores en las comunicaciones (hardware, políticas de red, mantenimientos, medios de transmisión, etc.) contamos con las siguientes preguntas:

No	PREGUNTA	RESPUESTA	Evaluación (Impacto)
1	¿El hardware para las comunicaciones es extremadamente moderno, adecuado y fiable?	Si.	1
2	¿Los dispositivos de comunicación del depto. de TIC son administrables?	Si.	1
3	¿El personal encargado de las comunicaciones está capacitado? SI, ¿ Cada que tiempo se capacita?	Sí, todos los días.	1

4	¿Es suficiente el personal encargado de las comunicaciones?	No.	4
5	¿Existen seguridades para las comunicaciones? SI, ¿Mencione los tipos de seguridad?	Sí, credenciales de acceso a equipos, VLANS.	4
6	¿Se dispone de políticas de operación de red?	No.	4
7	¿Existe un control sobre el tiempo de uso de los equipos de comunicación?	Sí, Control "PRTG".	2
8	¿Los equipos de comunicación tienen garantía?	licencia "Smart net" (RMA).	1
9	¿Se realiza mantenimiento periódico en los puntos de comunicación?	Sí, cada 6 meses.	3
10	¿Los equipos de comunicación son administrados correctamente?	Si.	1
11	¿Mencione las perturbaciones en la transmisión de datos de la institución?	Aislamiento del sector, cortes de energía eléctrica.	3
12	¿Se analiza la distancia, el medio y los dispositivos para la comunicación de datos correctamente?	Sí, siempre.	1
13	¿Cuál es el tipo de cable y categoría utilizado para cableado horizontal?	UTP Categoría 6.	4
14	¿Cuál es el tipo de cable y categoría utilizado para cableado vertical?	UTP Categoría 6 y Fibra Óptica.	4
15	¿Se realizan certificaciones de redes para cada implementación?	No.	3
16	¿El cableado de datos cumple las normas internacionales de instalación?	Cumple con ciertas normas IEEE.	3
17	¿Se realiza monitoreo frecuentes de las redes?	Sí.	1
18	¿Utilizan software para gestionar fallos en la red?	No.	5
19	¿Se dispone de diagramas actualizados de las redes de la institución? SI, ¿Mencione los software que utiliza?	Sí, pero no son completos.	3
20	¿Se dispone de procedimientos apropiados de identificación de errores en los segmentos de las redes de datos?	No.	4
Nivel de Impacto:			**2,65** **3**

RIESGO 7: CORTES DE SUMINISTRO ELÉCTRICO

Con respecto a problemas de energía eléctrica que pueden afectar a los equipos y archivos tenemos las siguientes preguntas:

No	PREGUNTA	RESPUESTA	Evaluación (Impacto)
1	¿La institución cuenta con una planta de emergencia de energía eléctrica?	No.	5
2	¿Dispone de generadores eléctricos adecuados en caso de cortes de energía?	No.	5
3	¿Cuentan con UPS los equipos informáticos?	Si, 1 UPS de 10KVA, para el centro de datos.	2
4	¿Existe tablero de Bypass para los UPS?	Si.	1
5	¿Cuál es el tiempo de alimentación de los UPS?	8 horas.	2
6	¿Cuántos equipos soportan los UPS?	20.	3
7	¿Cuáles son las causas que producen corte de energía?	Lluvias, problemas eléctricos.	3
8	¿Existen bitácoras para el control de cortes de energía en la institución?	No.	5
9	¿Existe sabotaje de energía eléctrica?	No se ha presenciado este caso en la institución.	1
10	¿Las instalaciones eléctricas en el depto. de TIC están diseñadas bajo normas internacionales y de forma independiente al resto de las demás instalaciones?	Solo las instalaciones del centro de datos.	3
11	¿Existe un sistema correcto de ductería para cableado eléctrico?	No, todo es aéreo.	5
12	¿Se dispone procedimientos adecuados para actuar frente a cortes de energía? SI, ¿Están documentados?	No, solo se anticipa cuando CNEL hace el anuncio general.	5
13	¿Se realiza mantenimiento periódico de las instalaciones eléctricas? SI, ¿Cada que tiempo?	Sí, mantenimiento anual.	3
14	¿Los equipos informáticos están correctamente conectados?	Solo los del centro de datos.	4
15	¿Las tomas de los equipos están polarizados?	Si se encuentran polarizados.	2

16	¿Los cables se encuentran debidamente identificados (positivo, negativo, tierra)?	Si pero no al 100%	4
17	¿Se tiene reguladores para equipos de cómputo?	No existen reguladores.	4
18	¿Existen tableros de distribución eléctrica?	Si.	2
19	¿El cableado eléctrico está ubicado por debajo de un piso falso?	No existe piso falso.	4
Nivel de Impacto:			**3,5** **4**

RIESGO 8: FALLAS EN LA CLIMATIZACIÓN

Con respecto a problemas de temperatura y humedad se tiene las siguientes preguntas:

No	PREGUNTA	RESPUESTA	Evaluación (Impacto)
1	¿Existen en el data center indicadores o sensores de temperatura y humedad?	No.	5
2	¿Existen interruptores cerca del cuarto de concentración para encender o apagar el sistema de aire acondicionado?	No.	5
3	¿El centro de datos cuenta con equipos acondicionados de precisión para temperatura y humedad? SI, ¿Cuántos aires acondicionados tiene?	1.	4
4	¿Existe sobrecalentamiento de equipos en el data center?	No hasta el momento.	1
5	¿Han existido daños a causa del sobrecalentamiento?	No hasta el momento.	1
6	¿han existido apagones de los equipos en centros de datos?	No hasta el momento.	3
7	¿El aire acondicionado de precisión está respaldado por UPS o generador eléctrico?	No.	5
8	¿Los equipos de enfriamiento se encuentran instalados bajo normas y estándares?	No.	4

9	¿Los servidores se encuentran instalados en racks cerrados o racks de gabinete?	Están en armarios de gabinete.	3
10	¿Los racks se encuentran correctamente conectados bajo normas de instalación?	Se encuentran unos juntos de otros.	4
11	¿El aire acondicionado que posee el centro de datos genera una buena distribución de aire en pasillos fríos y calientes?	Tiene una capacidad de 7000 BTU.	4
12	¿Los servidores se encuentran bien ubicados en los racks, con el objetivo de no dejar espacios entre servidores?	Se encuentran organizados.	2
13	¿El sistema de enfriamiento se encuentra directamente dirigido hacia los gabinetes de servidores?	No al 100%.	3
14	¿Al momento de adquirir equipos de enfriamiento, se toman en cuenta la densidad de carga que manejan los gabinetes con el fin de dar la solución adecuada?	No.	4
15	¿Se realizan mantenimiento adecuado a los aires acondicionados? SI, ¿Cada que tiempo?	Sí, cada 3 meses, por personal capacitado.	1
Nivel de Impacto:			**3,27**
			3

RIESGO 9: FALLAS EN LA PROTECCIÒN DE ARCHIVOS

Con respecto a fallas en la protección de archivos (respaldos de información, permisos y restricciones, etc.) se presentan las siguientes preguntas:

No	PREGUNTA	RESPUESTA	Evaluación (Impacto)
1	¿Existen en el data center indicadores o sensores de temperatura y humedad?	No existen.	5
2	¿Existen interruptores cerca del cuarto de concentración para encender o apagar el sistema de aire acondicionado?	No.	5

3	¿El centro de datos cuenta con equipos acondicionados de precisión para temperatura y humedad? SI, ¿Cuántos aires acondicionados tiene?	1 aire acondicionado para el data center.	4
4	¿Existe sobrecalentamiento de equipos en el data center?	No hasta el momento.	1
5	¿Han existido daños a causa del sobrecalentamiento?	No hasta el momento.	1
6	¿han existido apagones de los equipos en centros de datos?	No hasta el momento.	3
7	¿El aire acondicionado de precisión está respaldado por UPS o generador eléctrico?	No.	5
8	¿Los equipos de enfriamiento se encuentran instalados bajo normas y estándares?	No.	4
9	¿Los servidores se encuentran instalados en racks cerrados o racks de gabinete?	Están en armarios de gabinete.	3
10	¿Los racks se encuentran correctamente conectados bajo normas de instalación?	No.	4
11	¿El aire acondicionado que posee el centro de datos genera una buena distribución de aire en pasillos fríos y calientes?	Tiene una capacidad de 7000 BTU.	4
12	¿Los servidores se encuentran bien ubicados en los racks, con el objetivo de no dejar espacios entre servidores?	Se encuentran organizados.	2
13	¿El sistema de enfriamiento se encuentra directamente dirigido hacia los gabinetes de servidores?	Se encuentra en la parte superior de los armarios de gabinete.	3
14	¿Al momento de adquirir equipos de enfriamiento, se toman en cuenta la densidad de carga que manejan los gabinetes con el fin de dar la solución adecuada?	Si en ciertos casos.	4
15	¿Se realizan mantenimiento adecuado a los aires acondicionados? SI, ¿Cada que tiempo?	Sí, cada 3 meses, por personal capacitado.	1
Nivel de Impacto:			**3,27** **3**

RIESGO 10: EQUIVOCACIONES, DAÑO DE ARCHIVOS

Con respecto a equivocaciones y daños de archivos tenemos las siguientes preguntas:

No	PREGUNTA	RESPUESTA	Evaluación (Impacto)
1	¿Se realizan capacitaciones para el personal sobre el uso de los equipos informáticos con sus respectivos sistemas?	Si.	1
2	¿Cuánto saben los empleados de tecnología y sistemas de información? ¿Poco?, ¿Suficiente o bastante?	Suficiente.	1
3	¿Los sistemas de la institución están correctamente validados para el ingreso de datos?	Si.	1
4	¿En caso de que se presente algún incidente, se dispone de una lista adecuada de contactos para que los usuarios puedan pedir ayuda?	Sí, Guardias de seguridad.	1
5	¿Durante el tiempo de vacaciones de los empleados, ¿Qué tipo de personal los reemplaza?	Solo personal capacitado.	2
6	¿Saben sus reemplazos del manejo de los equipos?	Si tienen conocimiento	1
7	¿Es de confianza el personal de reemplazo para la institución?	No, al 100%, dependiente del área.	3
8	¿El personal del Departamento de TIC tiene experiencia laboral?	Sí, superiores realizados.	1
9	¿El personal del depto. TIC tiene programas de capacitación sobre equipos nuevos?	Sí, capacitaciones para servidores y equipos de comunicación.	1
10	¿Se dispone de manuales de procedimientos ante eminentes fallas en el data center?	No.	5
Nivel de Impacto:			**1,7** **2**

RIESGO 11: ACCESO NO AUTORIZADO

Con respecto a seguridad, políticas de control, sistemas de vigilancia, etc. que pueden afectar a los equipos y a la información, tenemos las siguientes preguntas:

No	PREGUNTA	RESPUESTA	Evaluación (Impacto)
1	¿El depto. de TIC cuenta con un sistema de seguridad para correo electrónico e Internet?	Anti Spam (Microsoft) para correo electrónico en la Nube.	2
2	¿Cómo se lleva a cabo la seguridad de los equipos y sistemas?	Firewalls. Electricidad para el data center.	2
3	¿Hay alguna persona encargada de la seguridad de la red?	Si, 2 Analistas de Tecnologías.	2
4	¿La funciones de administrador de red son cumplidas en su totalidad?	Si, por el director de TIC.	1
5	¿Se cuenta con políticas de control e identificación de accesos para visitantes del depto. de TIC?	No.	4
6	¿Se tiene conocimiento exacto del personal que tiene acceso a los diferentes sistemas informáticos, ya sean locales, en red o vía Internet, debidamente identificados?	Sí, los usuarios generan una auditoria.	3
7	¿Se tiene políticas de uso de servicios de red y seguridad sobre los sistemas, servidores y demás áreas del depto. de TIC? SI, ¿Son adecuados?	lineamientos empíricos pero no documentación.	4
8	¿El personal autorizado del data center cuenta con privilegios y contraseñas de usuario?	Sí, administrador de servidores y director de TIC.	2
9	¿Se realiza en el depto. de TIC, controles de conexión a las redes?	Sí, firewalls y el monitoreo a diario a las redes.	3
10	¿Se cuenta con procedimientos de autenticación de los sistemas operativos?	Sí, solo para los servidores	4
11	¿Las ventanas del depto. de tic, son 100% seguras?	No.	5
12	¿Se cuenta con tarjetas de identificación para el personal de trabajo?	No.	5
13	¿Existe sistema de vigilancia en el depto. de tic todo el tiempo?	No.	5
14	¿Existen puertas con llaves especiales o dispositivos biométricos?	No.	5
15	¿El depto. de TIC, cuenta con sistemas de alarma para detectar personal no autorizado?	No.	5

16	¿Se revisa frecuentemente que no esté abierta o descompuesta la puerta y ventanas del depto. de TIC?	A veces.	3
17	¿Los equipos informáticos disponen de llave de bloqueo de teclado?	No.	5
18	¿Existen controles adecuados de seguridad en el depto. TIC?	No.	5
Nivel de Impacto:			**3,6**
			4

RIESGO 12: ROBO COMÚN

En relación con la seguridad física del centro de datos, tenemos las siguientes preguntas:

No	PREGUNTA	RESPUESTA	Evaluación (Impacto)
1	¿El depto. de Tic cuenta con alarmas de seguridad?	No.	5
2	¿Se cuenta con personal responsable de la seguridad exclusivamente para el depto. de TIC?	No.	4
3	¿Existe un listado de las personas autorizadas para ingresar al centro de datos?	No.	3
4	¿En el sector donde se encuentra la Institución es peligroso?	Si.	5
5	¿Los equipos informáticos se encuentran visibles desde la calle?	Están en lugares estratégicos.	2
6	¿Cuenta con guardias de seguridad la institución?	Si.	1
7	¿Cuántos guardias de seguridad existen en la institución?	32 guardias de seguridad.	3
8	¿El personal de seguridad es suficiente?	No es suficiente.	4
9	¿En el lugar donde se ubica la institución, venden bebidas alcohólicas?	Sí, fuera de las instalaciones.	3
10	¿Alrededor de la institución venden drogas?	No, se desconoce.	2
11	¿Los guardias de seguridad reciben capacitación adecuada para enfrentar un hecho delictivo?	Si.	2
12	¿Los guardias utilizan equipos de seguridad?	Si.	1

13	¿Mencione los equipos de seguridad?	Pistolas y radios	2
14	¿Todos los ingresos a la institución se encuentran bien resguardados?	Algunos, no todos.	4
15	¿Se cuenta con un lugar externo para almacenamiento de los respaldos de la información?	No.	5
16	¿Se realiza controles adecuados para el acceso de los empleados?	Si.	1
17	¿Los guardias de seguridad se encuentran en sitios estratégicos?	No.	4
18	¿Se tiene un control de entrada y salida de los visitantes al depto. de TIC, manual o a través de un sistema informático?	Solo cuando vienen los proveedores.	3
19	¿Los equipos informáticos se encuentran en un lugar accesible para una persona en particular?	Si.	5
20	¿Se investiga al personal contratado para el depto. de TIC?	Sí, perfil profesional.	2
21	¿Existe vigilancia en el cuarto de máquinas las 24 horas?	No, solo horas laborales.	3
22	¿Se ha instruido a estas personas sobre que medias tomar en caso de que alguien pretenda entrar sin autorización al depto. de TIC?	Pocas.	3
23	¿Los delincuentes podrían ingresar a través de las ventanas?	Sí, ventanas sin protección.	5
24	¿Se cuenta con un sistema de vigilancia en el depto. de TIC, para monitoreo de seguridad?	No.	5
Nivel de Impacto:			**3,2** **3**

RIESGO 13: VANDALISMO

Con respecto a problemas de vandalismo, tenemos las siguientes preguntas:

No	**Pregunta**	**Respuesta**	**Evaluación (Impacto)**
1	¿Tienen antecedentes vandálicos o trastornos mentales el personal que trabaja en el depto. de TIC?	NO.	1

2	¿El personal de la institución tienen conflictos internos que podrían causar problemas vandálicos?	No siempre.	2
3	¿La documentación importante está debidamente almacenada en medios seguros estrictamente fuera de la organización?	No.	5
4	¿Existe algún empleado que haya salido de la institución con algún resentimiento?	La mayoría.	4
5	¿Está capacitado el personal para actuar en caso de vandalismo?	No.	4
6	¿Se han presenciado hechos vandálicos en los exteriores de la institución?	Muy pocos.	2
7	¿El personal de limpieza tiene antecedentes peligrosos que pueden ocasionar actos vandálicos?	No.	2
8	¿Se realizan cursos motivacionales para el personal de trabajo?	Rara vez.	3
19	¿Existe la posibilidad de que se den represarías por parte de algún ex empleado para causar daño directo o indirecto a los equipos de la institución?	Sí.	5
10	¿El personal de limpieza realiza específicamente su trabajo respetando áreas importantes del depto. de Tic a las que no tiene acceso?	Sí, siempre.	1
11	¿Existen malos hábitos en el data center como: fumar, almacenar materiales inflamables o elementos peligrosos?	No.	1
12	¿Existe la posibilidad que un ladrón desilusionado o frustrado cause daños a los equipos y a la información?	Si.	5
13	¿Las ventanas del depto. de TIC son bastantes confiables para impedir el ingreso de personas vandálicas?	No son seguras.	5
14	¿Brindan un nivel de seguridad adecuado las puertas del depto. de TIC?	No son seguras.	4
15	¿Se encuentra el techo del depto. de TIC en condiciones adecuadas y debidamente sellado?	El techo es de tumbado.	1

16	¿Se cuenta con una lista de contactos telefónicos de la Policía Nacional en caso de vandalismo?	Si.	1
17	¿Se tiene un control de acceso de las personas que ingresa a la institución?	Si pero todas las entradas de la institución.	4
Nivel de Impacto:			**2,9**
			3

RIESGO 14: INDISPONIBILIDAD DEL PERSONAL

Haciendo referencia a la ausencia del personal, responsabilidades, eficiencia y eficacia, etc., contamos con las siguientes preguntas:

No	PREGUNTA	RESPUESTA	Evaluación (Impacto)
1	¿Existe personal que esté capacitado para varias funciones?	Si.	1
2	¿El personal permanece en sus puestos durante todas las horas de trabajo?	Sí, dependiendo de sus funciones.	2
3	¿El personal cumple con los horarios establecidos de trabajo al 100%?	Sí, siempre.	1
4	¿Existe ausencia de empleados por alguna enfermedad?	Casi nunca.	2
5	¿Existe ausencia de empleados por infecciones bacteriológicas?	Pocos casos.	3
6	¿El depto. de TIC sabe cómo actuar frente a situaciones de ausencia de personal?	Sí, pero existe personal limitado en el depto.	3
7	¿Existen políticas actualizadas óptimas para casos de indisponibilidad del personal?	Existen lineamientos.	2
8	¿El depto. de TIC cuenta con perfiles, funciones y responsabilidades para sus empleados?	Si.	1
9	¿Se cumplen a cabalidad dichas responsabilidades por los empleados?	Sí, pero no en el tiempo requerido.	2
10	¿Los empleados del depto. de TIC, desempeñan sus obligaciones y tareas en el tiempo establecido?	La mayoría sí.	2

11	¿Existen demoras para entregar tareas asignadas?	Sí, regularmente.	3
12	¿Se cuenta con diagramas organizacionales? SI, ¿Están actualizados?	Si.	1
13	¿Cuenta con requisitos mínimos el depto. de TIC para otorgar cargos?	Si.	1
14	¿En caso de licencias o vacaciones, el depto. de TIC reemplaza dicho puesto por otro usuario o que sin ser ejercido?	Se reemplaza por otro usuario capacitado.	1
Nivel de Impacto:			**1,7** **2**

RIESGO 15: USO NO PREVISTO (MAL USO DE RECURSOS)

Con respecto al mal uso de equipos, sistemas, cuentas de usuario, políticas, se tiene las siguientes preguntas:

No	PREGUNTA	RESPUESTA	Evaluación (Impacto)
1	¿Los usuarios del depto. de TIC, tienen suficiente cuidado y uso de los equipos informáticos?	Sí, la mayoría.	2
2	¿Se cuentan con políticas actualizadas donde se fija el acceso a los sistemas de información por parte de los usuarios?	No.	4
3	¿Las cuentas de usuario de los empleados, son utilizadas estrictamente para uso académico, personal e intransferible?	Si.	1
4	¿Se cuenta con un sistema de monitorización y vigilancia, para visualizar los trabajos que están realizando los usuarios?	No.	4
5	¿Se cuenta con acceso restringido a páginas en los navegadores?	Si.	1
6	¿Se realizan los respaldos de información, bajo supervisión del director del depto. de TIC?	Sí, siempre.	1
7	¿Se realiza informes sobre incidencias que se han detectado y que puedan afectar al funcionamiento de los recursos informáticos?	Si.	2

8	¿Se realiza un seguimiento del uso de las cuentas de usuario y de los recursos informáticos del depto. de TIC?	No, solo usuarios restringidos.	4
9	¿Se realizan inventarios de los equipos informáticos?	Si.	1
10	¿La información es manejada de forma confidencial?	Sí, siempre.	1
11	¿Existen políticas adecuadas para evitar descargas de información?	Sí, pero no documentadas.	3
Nivel de Impacto:			**2,12**
			2

RIESGO 16: DELITOS INFORMATICOS (fraude, alteración de información)

Con respecto a fraude y piratería informática, tenemos las siguientes preguntas:

No	PREGUNTA	RESPUESTA	Evaluación (Impacto)
	FRAUDE		
1	¿Los sistemas o módulos cumplen con todas las características de un software ya sea confiabilidad, fiabilidad, seguridad, etc.?	Sí, la mayoría.	2
2	¿Las claves de acceso a los sistemas se mantienen secretas, sin ser triviales o simples identificar?	Sí, la mayoría.	2
3	¿Realizan informes ante sospechas de violación de confidencialidad de la información a los director del depto. de TIC?	No.	5
4	¿Qué tan frecuente se cambian las contraseñas de los sistemas desarrollados?	Se cambian 2 veces al año.	3
5	¿Los cambios de claves de las cuentas de los sistemas informáticos se realizan personalmente previa a la identificación del usuario otorgado por parte del director de TIC?	Sí, Bajo la solicitud del usuario.	2
6	¿Se sigue un formato de generación de contraseñas para los sistemas informáticos desarrollados ?	No.	5

7	¿Existe acceso a los sistemas desde otros sistemas o Personas y son seguros?	Son estrictamente de usuario.	2
8	¿Los sistemas desarrollados de la institución son compatibles con las aplicaciones existentes?	Sí, la mayoría.	2
9	¿Es probable la manipulación de los sistemas por personas no autorizadas?	Si.	4
10	¿Todos los sistemas cuentan con un administrador de red y con políticas de seguridad a nivel de red?	Si.	1
11	¿La información de la institución está clasificada y protegida?	Si.	1
	PIRATERÍA INFORMÁTICA		
12	¿Los sistemas operativos tienen licencias originales?	Si.	1
13	¿Se controla la reproducción o comercialización de programas informáticos para beneficio propio en el institución?	No es controlada en su totalidad.	3
14	¿Se cumplen políticas para la no generación de copias de sistemas informáticas con intención de hacerlas pasar por originales?	No se cumplen.	5
15	¿Se han presentado casos de hurto de tiempo de máquina o empleo del computado sin autorización en un horario no permitido?	No se han presentado casos de este tipo.	2
16	¿Se han presentado casos de hurto de software y datos, con la intención de acceder a sesiones de usuario ajenas y extraer información confidencial y almacenarlo en un soporte para fines propios?	Podría darse el caso.	3
17	¿Se cuenta con medidas de seguridad ante estos casos de hurto y son las adecuadas?	No.	5
Nivel de Impacto:			**2,8** **3**

RIESGO 17: DELITOS INFORMATICOS (fraude, alteración de información)

En relación a fallas en Ups (mantenimientos, backups, etc.), tenemos las siguientes preguntas:

No	PREGUNTA	RESPUESTA	Evaluación (Impacto)
1	¿El centro de datos cuenta con UPS de calidad?	No al 100%.	3
2	¿Cuántos UPS existen en el data center?	1 UPS.	5
3	¿Existen fallos frecuentes en las baterías de los sistemas de UPS?	No.	2
4	¿Tiene conocimiento de cuál es la vida útil de las baterías de los UPS?	Sí, la vida útil de 5 años, de cuales se van ocupando 2 años.	2
5	¿Se realiza mantenimiento de UPS, específicamente de las celdas? SI, ¿Cada que tiempo?	Sí, cada 6 meses.	2
6	¿El mantenimiento de los UPS es el adecuado?	Sí.	1
7	¿Se siguen estándares marcados de instalación para tener un mantenimiento adecuado de los sistemas de backup?	Sí, se siguen pero no al 100%.	4
8	¿Existen ciclos de descarga frecuentes en el centro de datos?	No.	2
9	¿Existen conexiones sueltas, y sobrecarga en los polos de las baterías?	No.	2
10	¿Cuándo existen problemas en los sistemas de backup, como enfrentan los empleados estos casos?	En esos casos se apaga todo y se localiza a los proveedores.	4
11	¿Se tienen repuestos de baterías para poder realizar los respaldos diarios?	No.	5
12	¿Cada que tiempo se realizan los respaldos en el data center?	Todos los días dependiendo de los sistemas críticos.	3
13	¿Se tiene almacenado los soportes de respaldos de información en armarios, estanterías o elementos refractarios al fuego y puertas blindadas apropiados para soportes informáticos?	No.	4

14	¿En el depto. de TIC se maneja un control de acceso a los datos archivados?	Si.	2
15	¿Se cuenta con un lugar de almacenaje externo para los respaldos de información?	No.	5
Nivel de Impacto:			**3,0** **3**

Gracias por brindarnos su tiempo.

Elaborado por: Autor.

Anexo 2: Entrevista para Análisis y Evaluación de Riesgos Informáticos dirigida al Jefe Redes e infraestructura de TIC'S de la UPSE.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
ESCUELA DE INFORMÁTICA

CUESTIONARIO DE ENTREVISTA #2
(ANÁLISIS Y EVALUACIÓN DE RIESGOS)

Objetivo: Determinar las amenazas y principales riesgos que causen mayor impacto en el Data Center de la UPSE mediante la utilización de la metodología Magerit, para proponer medidas adecuadas ante un desastre en el desarrollo de un Plan de contingencias.

Entrevistado: Jefe de Redes e Infraestructura: Ing. Fabricio Ramos, MSc.

Indicaciones: Para identificar las amenazas y riesgos en el centro de datos, requerimos su contribución para el llenado de la siguiente entrevista respondiendo adecuadamente y de forma íntegra y leal el cuestionario de preguntas.

RIESGO 18: FALLAS EN LOS SERVIDORES

En relación a los errores físicos y lógicos que puedan tener los servidores y los demás equipos informáticos (políticas de acceso, mantenimientos, instalaciones físicas, actualizaciones, etc.) que causen daños significativos tenemos las siguientes preguntas:

No	PREGUNTA	RESPUESTA	Evaluación (Impacto)
1	¿Suelen dañarse los servidores? SI, ¿Con que frecuencia?	No se han presentado daños.	2
2	¿El centro de datos cuenta con políticas de acceso a los servidores?	No.	4
3	¿Existe políticas para cambio de servidores?	No.	4
4	¿Se realiza mantenimiento preventivo a los servidores? SI, ¿Cada que tiempo?	Sí, cada trimestre.	1

5	¿Está capacitado el personal encargado del mantenimiento preventivo?	Sí.	1
6	¿El personal a cargo de los servidores está capacitado?	Sí.	2
7	¿Existen políticas de cambios de contraseña para los servidores?	No.	4
8	¿Los servidores tienen los sistemas operativos actualizados?	Sí.	2
9	¿Los sistemas operativos de los servidores utilizan software libre para su seguridad?	Sí, la mayoría utilizan S.O. Linux..	2
10	¿Existen servidores auxiliares para utilizarlos como reemplazo en caso de problemas?	Solo 2 servidores físicos, no hay auxiliares.	5
11	¿Los servidores cuentan con un Data Center con las especificaciones técnicas requeridas?	No en un 100%.	4
12	¿El centro de datos cuenta con un cableado estructurado con las especificaciones técnicas requeridas?	Se utilizan algunas normas IEE.	2
13	¿La puerta de ingreso al cuarto de servidores cumple con normas establecidas?	No.	5
14	¿Existe un sistema de aire acondicionado de precisión para regular una adecuada temperatura a los servidores?	Sí, existe un aire acondicionado de precisión.	1
15	¿Existe un manual de errores sobre los sistemas operativos para servidores?	No.	4
16	¿Los servidores cuentan con UPS?	Sí.	2
17	¿El cuarto de servidores cuenta con un sistema de detección y extinción de incendios?	No.	5
18	¿Las instalaciones eléctricas del cuarto de servidores cumplen con los requerimientos mínimos?	Cumplen, pero no al 100%.	4
19	¿Los racks para los servidores se encuentran debidamente aterrizados?	Si.	1
	FALLAS EN LOS EQUIPOS		
20	¿Los equipos se encuentran en un lugar limpio y sin humedad?	Algunos.	3
21	¿Existen políticas de administración de equipos y software?	No.	5

22	¿Existe un adecuado control de información sobre el equipo informático en el depto. de TIC?	Sí.	1
23	¿Se realiza las debidas copias de respaldo o backups al momento de iniciar la reparación de equipos?	Sí, siempre.	1
24	¿El personal es suficiente para el departamento de soporte técnico?	No es suficiente.	3
25	¿Se realiza mantenimiento preventivo a los equipos informáticos? SI, ¿Cada que tiempo?	A nivel de servidores = cada 6 meses. A nivel de PC y portátiles = 3 meses.	2
26	¿Está calificado el personal para realizar mantenimiento de equipos?	Sí.	1
27	¿Se cuenta con herramientas de trabajo apropiadas como: Kit de mantenimiento?	Si.	1
28	¿Se cuenta con UPS para los equipos?	No.	3
29	¿Cada qué tiempo se realiza mantenimiento a los UPS?	Cada 6 meses.	3
30	¿Cuánto tiempo proporcionan energía ininterrumpida los UPS en caso de corte eléctrico?	De 3 a 4 horas.	3
31	¿Se dispone al instante de repuestos para cambiar los elementos dañados del hardware?	Sí, de hardware más comunes.	3
32	¿El personal a cargo realiza el inventario de mantenimiento de equipos y de sus fallas?	No.	5
33	¿Se dispone de software de prevención que permita identificar problemas en los equipos informáticos?	Sí, el Deep Freeze y el ADW Cleaner.	2
34	¿Existen equipos informáticos auxiliares para utilizarlos como reemplazo en caso de emergencias?	Si.	2
35	¿En qué condiciones están actualmente los equipos informáticos?	Los servidores están óptimos, los PC en 80%.	5
36	¿Cuentan los equipos con garantías vigentes o seguros?	Sí.	2
Nivel de Impacto:			**2,7** **3**

RIESGO 19: VIRUS, DAÑOS DE INFORMACIÓN

Con respecto a virus y daño de información tenemos las siguientes preguntas:

No	PREGUNTA	RESPUESTA	Evaluación (Impacto)
1	¿Se cuentan con políticas y procedimientos adecuados para actuar en caso de virus?	No.	5
2	¿Se instala software en los equipos sin hacerle un examen previo?	No.	1
3	¿Está permitido el uso de Pendrive u otro dispositivo de almacenamiento externo en la oficina?	Si está permitido	4
4	¿Se realiza un análisis previo de revisión de virus a estos dispositivos de almacenamiento externo?	Sí, se utiliza el antivirus, Avast.	4
5	¿La institución invierte o tiene asignado un presupuesto a la adquisición de software administrativo y de seguridad informático?	Se asigna un presupuesto para el depto. De TIC.	1
6	¿Se cuenta con un sistema de Backups actualizado?	Si.	1
7	¿El Sistema de Backups que utilizan es 100% confiable?	Sí, hasta el momento.	2
8	¿Utilizan software para bloquear aplicaciones y programas no autorizados a los servidores?	No, porque se utiliza S.O. Linux.	3
9	¿Se tiene personal designado como único para ejercer ciertas funciones de seguridad?	Sí, el administrador de servidores.	1
10	¿Se han presentado problemas graves en la información a causa de virus?	Si, en el área de mantenimiento de equipos informáticos.	5
11	¿Los sistemas operativos con los que trabaja la institución están actualizados? SI, ¿Enumerar parches de los sistemas operativos?	Sí, son licenciados.	1
12	¿Qué antivirus tiene actualmente la institución?	No tienen ningún antivirus.	5
13	¿Cuentan con licencia original los antivirus?	No.	5
14	¿Se actualizan los sistemas de antivirus? SI, ¿Cada que tiempo?	Rara vez.	4

15	¿Es seguro el sistema de antivirus que utiliza la institución?	No.	4
16	¿Los equipos informáticos tienen sus puertos bloqueados?	Si.	1
17	¿El antivirus muestra un detalle completo de los archivos infectados, y ofrece soluciones de recuperación de archivos?	Si.	2
18	¿Se dispone de software para protección de las redes? SI, ¿Cuáles son?	Sí, "PFSense", realiza escaneo de tráfico de red, firewall, ancha de banda, puertos.	1
19	¿Se dispone de software de antivirus exclusivamente para los servidores?	No.	5
20	¿Se cuenta con manuales de procedimientos para limpieza de virus?	No.	5
21	¿Existen políticas para evitar descargas de información desde internet?	Sí, pero no documentadas.	3
22	¿Se instala software pirateado en la Institución?	No en el área de servidores, todos son licenciados.	2
23	¿Se tiene control sobre el acceso a páginas web en la institución?	Sil.	1
Nivel de Impacto:			**2,8** **3**

Gracias por brindarnos su tiempo.

Elaborado por: Autor.

Anexo 3: Entrevista para Análisis y Evaluación de Riesgos Informáticos dirigida al Jefe Desarrollo de Software de TIC'S de la UPSE.

UNIVERSIDAD ESTATAL PENÍNSULA DE SANTA ELENA
FACULTAD DE SISTEMAS Y TELECOMUNICACIONES
ESCUELA DE INFORMÁTICA

CUESTIONARIO DE ENTREVISTA #3
(ANÁLISIS Y EVALUACIÓN DE RIESGOS)

Objetivo: Determinar las amenazas y principales riesgos que causen mayor impacto en el Data Center de la UPSE mediante la utilización de la metodología Magerit, para proponer medidas adecuadas ante un desastre en el desarrollo de un Plan de contingencias.

Entrevistado: Jefe de Desarrollo de Software: Ing. Hernán Conforme.

Indicaciones: Para identificar las amenazas y riesgos en el centro de datos, requerimos su contribución para el llenado de la siguiente entrevista respondiendo adecuadamente y de forma íntegra y leal el cuestionario de preguntas.

RIESGO 20: FALLAS EN LOS SISTEMAS

Se hace referencia a errores (actualizaciones, seguridad, mantenimiento) que puedan sufrir los sistemas tenemos las siguientes preguntas:

No	PREGUNTA	RESPUESTA	Evaluación (Impacto)
1	¿Los sistemas implementados son 100% seguros?	Sí, controles acceso, códigos de seguridad, encriptación de clave, inicio de sesión.	2
2	¿Los sistemas implementados son disponibles y confiables?	A nivel web sí.	3
3	¿Se realizan copias de seguridad en los sistemas informáticos? SI, ¿Cada que tiempo?	Sí, los respaldos son diarios y mensuales por .	4

4	¿Los usuarios son capacitados cuando se implementa un nuevo sistema?	Si, por módulos de los sistemas.	2
5	¿Se dispone políticas de usuario en los sistemas?	No.	5
6	¿Se dispone de manuales de usuarios de los sistemas?	Sí, de los sistemas más relevantes.	3
7	¿Se tiene un manual de errores de cada uno de los sistemas?	No.	5
8	¿Presentan errores los sistemas? SI, ¿Cuánto es el tiempo del error?	Sí, menos complejos de 3 - 4 horas y más complejos 2 - 3 días,.	4
9	¿Se efectúan mantenimiento preventivo a los sistemas?	No es el óptimo. cada 6 meses.	3
10	¿Son originales los sistemas implementados?	Sí, la mayoría.	2
11	¿Se realizan pruebas oportunas para seguimiento de los sistemas implementados?	Sí.	2
12	¿Los sistemas cumplen con los requerimientos de usuario?	La mayoría sí.	3
13	¿Se realizan actualizaciones de los sistemas operativos?	Sí.	1
14	¿Los equipos informáticos cumplen con los requisitos mínimos para soportar los sistemas instalados?	Si.	1
15	¿Las versiones de los programas son 100% actualizados? Cuáles son las versiones que utilizan?	No existe control de las versiones.	5
16	¿La información de cada sistema incluyendo configuraciones está documentada?	Sí.	2
17	¿Se dispone de inventarios de software? SI, ¿Están Actualizados y disponibles?	Sí, se realiza un informe cuatrimestral.	1
18	¿Se realizan las actualizaciones de bases de datos? SI, ¿Cada que tiempo?	Sí, se realizan a diario.	1
19	¿Están los antivirus actualizados? SI, ¿Qué tipo de antivirus poseen?	No.	4
Nivel de Impacto:			**2,7**
			3

RIESGO 21: ERRORES DE CONFIGURACIÓN

Con respecto a errores de configuración se presentan las siguientes preguntas:

No	PREGUNTA	RESPUESTA	Evaluación (Impacto)
1	¿Suelen existir errores en los sistemas desarrollados? SI, ¿Cada que tiempo?	Sí, pero no son muy frecuentes.	3
2	¿Qué tipo de errores en los sistemas son los más comunes?	Problemas de conexión de red, de registros de datos, de configuración.	4
3	¿Suelen existir errores en los equipos de comunicación?	No.	2
4	¿Qué tipo de errores en los equipos de comunicación son los más comunes?	Errores de conexión/internet (CNT/TELCONET) .	4
5	¿Realizan revisiones en la configuración de las aplicaciones y bases de datos? SI, ¿Con que Frecuencia?	Sí, cada 6 meses.	3
6	¿El personal está capacitado para realizar configuraciones en los equipos?	Si.	2
7	¿Disponen de manuales de usuario? SI, ¿Menciónelos?	Solo tutoriales.	3
8	¿Hacen uso de los manuales de usuario para la instalación de nuevos equipos?	No.	5
9	¿Dispone el depto. de TIC de manuales de errores actualizados en caso de emergencia?	No.	5
Nivel de Impacto:			**3,4** **3**

RIESGO 22: ROBO DE INFORMACIÓN

Con relación a robo de información (confidencialidad, herramientas seguras, etc.), tenemos las siguientes preguntas:

No	PREGUNTA	RESPUESTA	Evaluación (Impacto)
1	¿El software de la institución es? ¿Licenciado, pirateado, distribución libre?	A nivel web es software libre, a nivel de escritorio es software licenciado	1

2	¿La herramienta administradora de base de datos de la Institución es segura?	Se utiliza SQL Server 2005, hasta el momento no han existido problemas.	2
3	¿Las herramientas de programación utilizadas son seguras?	Sí, la mayoría.	2
4	¿Cuánta pérdida podría causar en caso de que se divulgase públicamente información del depto. de TIC?	Graves daños.	4
5	¿El personal que labora en el depto. de Tic es discreto con la información?	Sí.	2
6	¿Se ha elaborado una lista de los posibles sospechosos que pudieran efectuar un robo?	No.	3
7	La información que se maneja, ¿debe ser mostrada con hermetismo, o es de libre acceso?	La información es privada.	1
8	¿Las contraseñas de los sistemas son difíciles de descifrar?	No.	5
9	¿El acceso a la información está restringido para personal no autorizado?	Si.	2
10	¿El sistema de firewall utilizado es el adecuado?	Si.	1
11	¿Cuál es el personal autorizado para trabajar en la base de datos y aplicativos?	El jefe de desarrollo.	1
12	¿Existen cámaras de seguridad en el depto. de TIC? SI, ¿Son suficientes?	No existen.	5
13	¿Existen políticas de usuario para acceso a los sistemas?	No.	5
14	¿Se cuenta con copias de los archivos en un lugar distinto al de la computadora?	No.	5
15	¿Explique la forma en que están protegidas físicamente estas copias (bóveda, cajas de seguridad, etc.) para garantizar su integridad?	Se encuentran en un disco del servidor, dentro del depto. de TIC.	5
Nivel de Impacto:			**2,9** **3**

Gracias por brindarnos su tiempo.

Elaborado por: Autor.

Anexo 4. Estructura del estándar ISO/IEC 27002: 2013 (14 Dominios, 35 Objetivos de Control, 114 Controles) http://www.iso27000.es/iso27002.html.

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 INFORMACIÓN
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 seguridad de la información.
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 publicas
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.

Tabla 39. Dominios de control de la norma ISO 27002:2013.
Fuente: http://www.iso27000.es/iso27002.html

Anexo 5. Diseño Físico del Departamento de Direccion de las Tecnologias de Información de la UPSE.

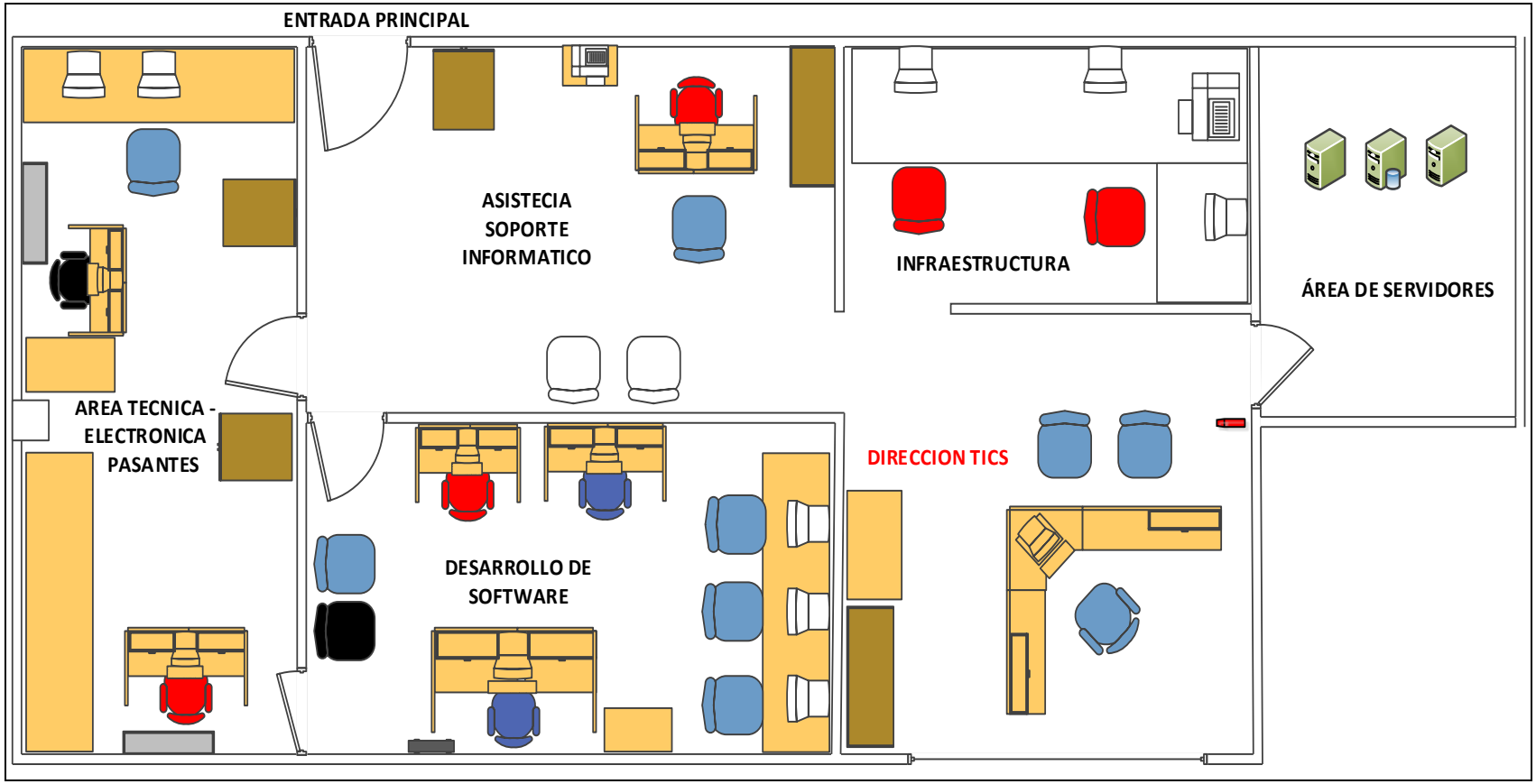


Figura 27. Diseño Físico del departamento de TIC's de la UPSE.