ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

“ELABORACIÓN DE UN PLAN DE CONTINGENCIA PARA EL DEPARTAMENTO DE SOPORTE TÉCNICO DE LA FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN (FIEC) PARA GARANTIZAR LA CONTINUIDAD DE SUS ACTIVIDADES ANTE DESASTRES INFORMÁTICOS.”

TRABAJO DE TITULACIÓN

Previa la obtención del Título de:

MAGISTER EN SEGURIDAD INFORMÁTICA

Presentada por:

DIANA MARÍA ORDÓÑEZ PAREDES

Guayaquil – Ecuador

Año 2017

AGRADECIMIENTO

Agradezco primeramente a Dios por la oportunidad de culminar mis estudios de maestría, a mis padres por todo el apoyo brindado durante todo este tiempo de estudio, compañeros, amigos y profesores que gracias a su ayuda y colaboración puedo culminar esta meta profesional.

DEDICATORIA

A mis padres, pilares fundamentales de mi vida, quienes siempre han sido un gran apoyo a lo largo de toda mi vida y en todo este tiempo que ha durado mi preparación profesional.

TRIBUNAL DE SUSTENTACIÓN

_____

Mgs. Lenin Freire C.

Director MSIG / MSIA

_____

Mgs. Lenin Freire C.

Director de Trabajo de Titulación

_____

Mgs. Robert Andrade

Miembro Principal

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este Trabajo de Titulación, me corresponden exclusivamente; y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL"

Diana María Ordóñez Paredes

RESUMEN

El presente trabajo de tesis tiene como finalidad, la posibilidad de establecer un plan de contingencia informático para el Departamento de Soporte Técnico de la Facultad de Ingeniería en Electricidad y Computación para garantizar la continuidad de sus actividades y servicios que brinda a sus usuarios, durante desastres informáticos o naturales, tales como terremotos, incendios o inundaciones.

Para la realización del plan de contingencia se han tomado como base algunas de las buenas prácticas y normas internacionales utilizadas en la actualidad tales como: MAGERIT versión 3, BS 25999, ISO 22301:2012.; las mismas que han permitido realizar un adecuado análisis de riesgos y elaboración de un plan de contingencia informático que permita al Departamento de Soporte Técnico estar preparado ante un evento catastrófico, que cause la falta de entrega de sus recursos tecnológicos, mediante la elaboración de este plan de contingencia se intenta mitigar estos eventos para que los servicios brindados por el Departamento de Soporte Técnico puedan estar en continuo funcionamiento.

ÍNDICE GENERAL

AGRADECIMIENTO II

DEDICATORIA III

TRIBUNAL DE SUSTENTACIÓN IV

DECLARACIÓN EXPRESA V

RESUMEN VI

ABREVIATURAS Y SIMBOLOGÍA XI

ÍNDICE DE FIGURAS XII

ÍNDICE DE TABLAS XIII

INTRODUCCIÓN XIV

CAPÍTULO 1 16

GENERALIDADES 16

1.1 Antecedentes 16

1.2 Descripción del Problema 17

1.3 Solución Propuesta 19

1.4 Objetivo General 20

1.5 Objetivos Específicos 20

1.6 Alcance 21

1.7 Metodología 21

CAPÍTULO 2 23

MARCO TEÓRICO 23

2.1 Introducción al Plan de Contingencia 23
2.2 Conceptos Básicos del Plan de Contingencias 24
2.3 Objetivos del Plan de Contingencia 27
2.4 Gestión de riesgos de Seguridad de la Información 27
2.5 Familias BS 25999-1, BS 25999-2, ISO 22301:2012. 30
CAPÍTULO 3 39
ANÁLISIS DEL RIESGO E IMPACTO EN EL NEGOCIO 39
3.1 Metodología de Análisis y Gestión de Riesgos 39
3.2 Identificar los procesos y recursos críticos de IT del negocio 46
3.3 Identificar los eventos o incidentes que puedan ocasionar interrupciones en los servicios críticos de la organización. 59
3.4 Analizar y evaluar la probabilidad de ocurrencia y el impacto causado por incidentes de seguridad de la Información 61
CAPÍTULO 4 69
ANÁLISIS Y DISEÑO DEL PLAN DE CONTINGENCIA INFORMÁTICO 69
4.1 Identificar los requerimientos estratégicos para la recuperación de la plataforma de TIC 69
4.2 Seleccionar métodos alternos de respaldo y almacenamiento de datos. 75
4.3 Determinar los requerimientos del plan de contingencia informático. . 77
4.4 Determinar la estructura del plan 78
4.5 Diseñar el plan de contingencia informático 85

4.6 Definir y Documentar los procedimientos de recuperación 109
4.7 Determinar los documentos requeridos a utilizar durante y después del desastre 111
CAPÍTULO 5 114
IMPLEMENTACIÓN DEL PLAN DE CONTINGENCIA INFORMÁTICO 114
5.1 Antecedentes 114
5.2 Pruebas y Verificación 116
5.3 Análisis de Resultados 125
5.4 Modelo del Acta de Prueba del Plan de Contingencia 128
CONCLUSIONES Y RECOMENDACIONES 131
BIBLIOGRAFÍA 136
ANEXOS 140
ANEXO A 141
ANEXO B 144
ANEXO C 148
ANEXO D 152
ANEXO E 168
ANEXO F 169
ANEXO G 170
ANEXO H 172
ANEXO I 173
ANEXO J 174

ANEXO K 175

ANEXO L 176

ANEXO M 179

ABREVIATURAS Y SIMBOLOGÍA

BSI	British Standards Institution
FIEC	Facultad de Ingeniería en Electricidad y Computación
GTySI	Gerencia de Tecnologías y Sistemas de Información.
ISACA	Asociación de Auditoría y Control de Sistemas de Información
ISO	Organización Internacional de Normalización
ISO 27005	Gestión del Riesgo en la Seguridad de la Información
ISP	Proveedor de Servicio de Internet
ITIL	Biblioteca de Infraestructura de Tecnologías de la Información
MAGERIT	Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información
NIST	Instituto Nacional de Normas y Tecnología
PDCA	Plan Do Check Act
SAO	Sitio Alterno de Operaciones
SGCN	Sistema de Gestión de la Continuidad del Negocio
TIC	Tecnología de la Información y Comunicación

ÍNDICE DE FIGURAS

Figura 2.1 Ciclo de Continuidad del Negocio 26

Figura 2.2 Gestión de Riesgos de una Organización..... 30

Figura 2.3 Gestión del Programa BCM - BS25999 35

Figura 2.4 Modelo PDCA aplicado al SACNe 37

Figura 2.5 ISO 22301 PDCA aplicado al proceso BCM 38

Figura 3.1 ISO 31000- Marco de trabajo para la gestión de riesgos..... 41

Figura 3.2 Gestión de riesgos según MAGERIT 43

Figura 3.3 Proceso de gestión de riesgos..... 46

Figura 3.4 Diagrama de Red de la Infraestructura Física de la FIEC..... 49

Figura 3.5 Organigrama de la FIEC 50

Figura 3.6 Gráfica estadística de la Valoración de los tipos de Activos de la FIEC..... 58

Figura 7 Gráfico Mapa de Riesgos de los Activos de [D] Datos..... 65

Figura 8 Gráfica del Mapa de Riesgos de activos [HW] Equipos Informáticos 66

Figura 4.1 Equipo del PCI. 80

Figura 4.2 CPCI 81

Figura 4.3 Diagrama de Procedimiento de Recuperación 110

Figura 5.1 Diagrama del ControlPC 120

Figura 5.2 Esquema de Funcionamiento con el SAO 123

Figura 5.3 Mapa de Riesgos de [HW]. 128

ÍNDICE DE TABLAS

Tabla 1 Activos de la FIEC [14]..... 53

Tabla 2 Valoración de los Activos..... 55

Tabla 3 Valoración de los Activos de la FIEC..... 56

Tabla 4 Valoración de las amenazas por Activos de Información..... 59

Tabla 5 Valoración de la Probabilidad y el Impacto..... 62

Tabla 6 Análisis de Riesgos..... 63

Tabla 7 Activos de Información con Riesgos Altos..... 67

Tabla 8 Almacenamiento de Datos..... 76

Tabla 9 Listado de Integrantes de los Equipos de Recuperación. 85

Tabla 10 Análisis de los Activos [HW]..... 126

INTRODUCCIÓN

En la actualidad la tecnología se encuentra involucrada en muchos aspectos de nuestro diario vivir, sea en escuelas, nuestros hogares, empresas de toda índole; la misma que es una herramienta importante para el uso diario así mismo con la entrega de productos o servicios asociados, en especial en el ámbito educativo, se ha notado cambios importantes tanto así que se depende de estos elementos tecnológicos cada vez más, en este aspecto las facultades de la ESPOL, en especial la FIEC, cuenta con su propio Departamento de Soporte Técnico, el mismo que debe estar a la vanguardia en cuanto a avances tecnológicos y medidas de seguridad informática.

Para el Departamento de Soporte Técnico contar con un Plan de Contingencia Informático, que le permita estar preparado ante un desastre, sea este de origen industrial o natural, es de vital importancia, debido a que en el Ecuador en este último año que pasó, el 2016, ha sufrido de un terremoto muy fuerte de magnitud 7.8 en la Escala de Richter, el mismo que ha dejado a su paso muchas víctimas afectadas, y replicas constantes hasta la fecha.

Por este motivo el presente trabajo es, elaborar un plan de contingencia que

dará una visión general en cuanto a la continuidad del negocio y su recuperación ante desastres informáticos y naturales, para cumplir este objetivo, se ha realizado un análisis de la organización, se define su misión, visión y estructura como tal, además de las responsabilidades respectivas del personal que labora en el Departamento de Soporte Técnico, se realiza un análisis de riesgos e impacto en el negocio utilizando la metodología MAGERIT v3 y se determinan procedimientos de contingencia que mitiguen estos riesgos.

CAPÍTULO 1

GENERALIDADES

En este capítulo describo de manera general el planteamiento del proyecto, así como sus alcances y limitaciones, explicando la razón de esta implementación y la solución propuesta al problema planteado.

1.1 Antecedentes

La Facultad de Ingeniería en Electricidad y Computación es una de las facultades más grandes de ESPOL, por lo tanto el número de estudiantes que ingresan a las carreras semestralmente son

numerosos, por este motivo la implementación de los laboratorios de computación y servicios informáticos que se necesitan, también deben cubrir las exigencias actuales con respecto a la calidad del estudio. La facultad cuenta con su propio Departamento de Soporte Técnico (DST), el mismo que se encarga de la administración de la infraestructura y servicios de soporte a laboratorios, docentes y personal administrativo que labora en la facultad.

En la actualidad uno de los aspectos fundamentales que han venido predominando tanto en centros educativos como en empresas de todo ámbito es el uso de la tecnología como herramienta importante e infaltable para el convivir a diario y entrega de productos o servicios. En el caso de la FIEC como una de las facultades con mayor número de estudiantes es de vital importancia que sus sistemas de administración se encuentren funcionando continuamente. Por este motivo, el desarrollo de un plan de contingencia informático es de mucho beneficio para la facultad.

1.2 Descripción del Problema

El DST tiene a cargo un personal capacitado para brindar soporte técnico tanto a personal administrativo como a los laboratorios que se encuentran en la facultad, al manejar muchos requerimientos por parte de los usuarios, y contar con servicios de mail, redes

inalámbricas, seguridad por video vigilancia y aplicativos que facilitan el ingreso de información, es necesario que siempre se encuentren en un correcto y constante funcionamiento. Además el DST tiene sistemas de información críticos que siempre deben estar protegidos ya que administra información de suma importancia y la infraestructura debe estar lo suficientemente preparada ante algún incidente sea a nivel de seguridad de la información o desastres naturales.

El Departamento de Soporte Técnico (DST) de la FIEC actualmente posee políticas y procedimientos que establecen controles de seguridad en cuanto a accesos y uso de los recursos informáticos mediante la norma ISO 27002. Estos controles fueron recientemente implementados y puestos a prueba por parte del personal del departamento para mitigar los riesgos tecnológicos que afectan el correcto funcionamiento de los sistemas informáticos.

Por otro lado; se debe considerar que la mayoría de las organizaciones poseen bienes tangibles, empleados, sistemas y tecnologías de la información, si alguno de estos componentes es dañado o deja de ser accesible causará un gran impacto en el correcto funcionamiento de la organización, en este caso específico de la FIEC; entre los incidentes que se contemplan y que trataré se

encuentran los de gran escala como desastres naturales (incendios, inundaciones, terremotos, etc.) que provocarían indisponibilidad de los servicios, o sistemas; incidentes de seguridad o intrusión a servidores de la facultad. Son problemas de los cuales deben estar protegidos, por esa razón elaborar un plan de contingencia que analice estas situaciones servirá de mucha ayuda para la facultad.

1.3 Solución Propuesta

El DST (Departamento de soporte técnico) necesita contar con un plan de contingencia informático que le permita estar preparado ante un desastre o una interrupción prolongada de los servicios informáticos que presta a sus usuarios. Por este motivo el presente trabajo es, elaborar un plan de contingencia que dará una visión general en cuanto a la continuidad del negocio y recuperación de desastres informáticos, que es un conjunto de procedimientos de tipo preventivo, que aporta la infraestructura necesaria para la recuperación de un sistema en caso de producirse un desastre, o un incidente que pueda paralizar de forma parcial o total los servicios de la facultad, de tal manera que pueda seguir operando a un nivel predefinido aceptable.

Un plan de continuidad del negocio beneficiará al Departamento de Soporte Técnico de la FIEC, a estar a la vanguardia de las actuales

exigencias del mercado, porque la tendencia mundial es que las empresas ya no compitan entre sí, la competencia es ahora entre cadenas de suministros para mantenerse operando; ninguno de sus componentes puede dejar de operar ya que si un elemento dejara de funcionar paraliza todo, generando el caos. Cada miembro del DST tiene que demostrar que es un proveedor confiable, y esto se logra teniendo un plan de continuidad del negocio que proteja los procesos esenciales y más importantes que permitan originar los servicios que desean nuestros usuarios.

1.4 Objetivo General

Elaborar un Plan de contingencia para el DST (Departamento de soporte técnico) de la FIEC para garantizar continuidad en sus actividades ante incidentes relacionados con tecnología de la información y comunicaciones, así como desastres naturales.

1.5 Objetivos Específicos

Entre los objetivos específicos tenemos:

- Reconocer los componentes principales relacionados con la infraestructura del DST.
- Identificar los posibles riesgos relacionados con tecnologías de la información que pueden afectar al normal

funcionamiento de los servicios que se brindan a la facultad.

- Identificar de manera clara y concisa todos los procedimientos y requerimientos a realizar en caso de que se presentes incidentes, fallos o daños sobre los Sistemas que utiliza la facultad.
- Proveer y desarrollar una solución de continuidad de funcionamiento de servicios críticos que son administrados por el DST y que son fundamentales para el correcto funcionamiento de las actividades en la facultad.

1.6 Alcance

En el plan de contingencia se debe tener las siguientes fases a considerar: Dentro de comprender el negocio se tiene que realizar un análisis de riesgos e impacto del mismo. Dentro de estrategia de continuidad se encuentra el desarrollo de estrategias de recuperación, se procede con el desarrollo del plan de contingencia del negocio para la recuperación ante desastres informáticos, la última fase es la de pruebas y la documentación respectiva del plan de contingencia.

1.7 Metodología

Entre las normas más conocidas para sistemas de gestión de la

continuidad del negocio y que se emplearán como referencia para el plan de contingencia del DST, se encuentra la Norma BS 25999 es una norma británica muy ampliamente utilizada y se compone de dos partes: BS 25999-1: Gestión de la continuidad del negocio-Código de práctica, es una guía de implantación del modelo de gestión; el BS 25999-2: Gestión de la continuidad del negocio-Especificación, es una especificación de requisitos para un sistema de gestión de continuidad de negocio y con la posibilidad de certificación. Otra de las normas que actualmente se emplea es la ISO 22301:2012 “Seguridad de la Sociedad: Sistemas de Continuidad del Negocio-Requisitos” que aplica el ciclo Plan-Do-Check-Act para la planificación, establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y la mejora continua.

CAPÍTULO 2

MARCO TEÓRICO

En este capítulo se presentan los principales conceptos que se utilizan en este proyecto, para de esta manera conocer cada uno de ellos.

2.1 Introducción al Plan de Contingencia

En la actualidad, toda empresa basa su actividad comercial y el cumplir sus objetivos organizacionales, en el funcionamiento completo de sus equipos informáticos, para brindar un servicio de calidad a sus clientes.

Cualquier daño a los sistemas informáticos que maneja la

organización, podría paralizar o interrumpir su normal funcionamiento, ocasionando pérdidas económicas irreparables para la organización.

Una forma de prevenir estos eventos negativos se basa en la elaboración e implementación de un Plan de Contingencia Informático, el mismo que se define como “Un conjunto de medidas preventivas tales como técnicas, humanas y organizativas, para aportar a la infraestructura física y lógica de una organización en caso de producirse un situación de emergencia, para garantizar la continuidad de sus operaciones ” [1] también se lo define como un eventos o incidente que pueda detener, ya sea de forma parcial o total el normal funcionamiento de los servicios que brinda alguna compañía, mediante el restablecimiento de estos servicios por un conjunto de procedimientos alternativos, poder seguir operando aunque sea a un nivel mínimo aceptable.

2.2 Conceptos Básicos del Plan de Contingencias

Instituciones y entidades controladas por algún ente gubernamental deben implementar planes de contingencia y de continuidad a fin de garantizar sus operaciones de forma continua para minimizar algún tipo de pérdida en caso de eventos o incidentes, que puedan paralizar su normal funcionamiento. Para esto, se deben realizar adecuados estudios de riesgos y balancear costos de implementación de un plan

de continuidad, esto depende de la criticidad de los procesos de la entidad, para los de alta criticidad se debe implementar un plan de continuidad, para otros será suficiente un plan de contingencia.

Es un documento con un conjunto de procedimientos e información que es desarrollado y está en constante mantenimiento, listo para su utilización ante un incidente o evento que pueda paralizar a la organización, para que así la misma pueda seguir entregando sus productos y servicios críticos en un nivel predefinido aceptable [2].

Recrea porciones del negocio, pérdidas, incluyendo procesos críticos, datos, infraestructura tecnológica, personal calificado, transferencia de la carga de trabajo, comunicación con proveedores, clientes, etc.

Incluye a la recuperación de desastres (DRP). El mismo que se refiere a un plan enfocado en sistemas, diseñado para restaurar la operatividad del sistema, tecnología, aplicación o facilidad de cómputo critica en un sitio alterno después de una emergencia, aplica a eventos importantes usualmente catastróficos que niegan la facilidad normal de operación durante un periodo extendido [3].

Enfoque metodológico del ciclo de un plan de contingencia:

Comprender el negocio: En esta etapa se debe evaluar riesgos e Impacto en el negocio u organización. Valorar las amenazas sobre la

vulnerabilidad. Comenzar a priorizar la recuperación del negocio.

Desarrollar estrategia de continuidad: desarrollar respuestas efectivas en costo para las amenazas identificadas. Desarrolla acuerdos de niveles de servicio realistas.

Implementación de las estrategias: Estrategias de recuperación de desastres y de continuidad para cumplir con los niveles de servicio. Desarrollar e implementar los planes y procesos del plan.

Ejecutar y Mantener el plan: Realizar pruebas y revisar el plan de recuperación de desastres y de continuidad en intervalos regulares.

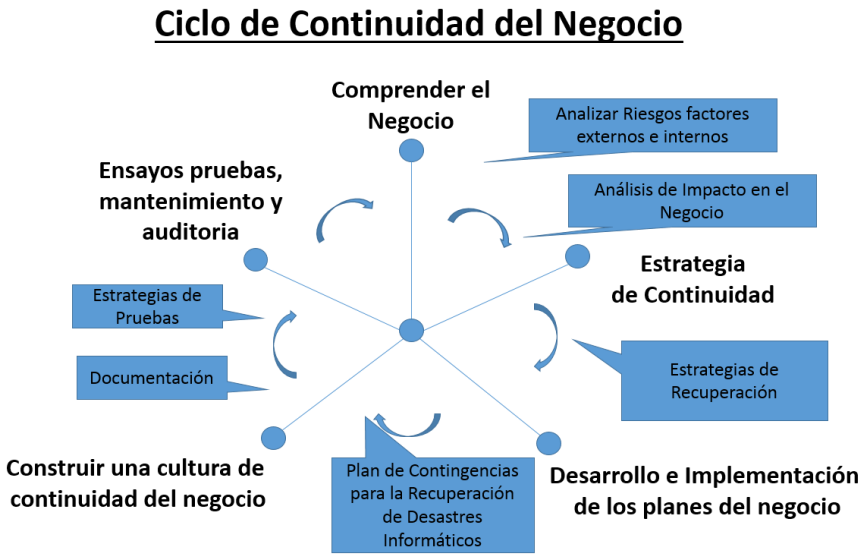


Figura 2.1 Ciclo de Continuidad del Negocio

Fuente: El autor

2.3 Objetivos del Plan de Contingencia

Puedo detallar los siguientes:

- Proveer una solución efectiva para mantener operativos los activos informáticos, que albergan los servicios críticos que componen los Sistemas de Información, los cuales son de vital importancia para el normal funcionamiento de la organización.
- Conocer todos los métodos o procedimientos a realizar en el caso que se presenten incidentes, o daños sobre los elementos que conforman el Sistema de Información.
- Capacitar y concientizar sobre las respuestas inmediatas a incidentes a todo el personal que labora dentro de la organización, así como a los miembros responsables del soporte de la infraestructura.

2.4 Gestión de riesgos de Seguridad de la Información

Riesgo

Es “el efecto de la incertidumbre en la consecución de los objetivos” según la ISO 31000:2009.

El riesgo es la probabilidad de que ocurra un evento o acontecimiento que tenga un gran impacto en el alcance de los objetivos organizacionales, se mide en términos de consecuencia o impacto y probabilidad.

“Algo que podría suceder y su efecto en el logro de sus objetivos” según la norma BS 25999-1. Combinación de la probabilidad (posibilidad) de un evento y su consecuencia (Risk Management: Vocabulary Guide 73 ISO). Es la posibilidad de que ocurra un acontecimiento que tenga un impacto en el alcance de los objetivos. El riesgo se mide en términos de consecuencias y probabilidad.

A continuación se lista los principales marcos metodológicos sobre Gestión de Riesgos de Tecnología de la información TI:

- COBIT – Control Objectives for Information and related Technology (ISACA).
- IT Risk (ISACA).
- ISO 27005 Gestión del Riesgo en la Seguridad de la Información.
- MAGERIT - Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información (Gobierno de España).
- OCTAVE - Evaluación de Amenazas y Vulnerabilidades de Recursos Críticos Operacionales.
- NIST – National Institute of Standards and Technology; Risk Management Guide for Information Technology Systems.

Existen dos componentes que se tienen que considerar al referirme al riesgo:

Impacto (efectos que pueda tener para el negocio); y, probabilidad de ocurrencia (posibilidad de que suceda el evento incidente).

El análisis de riesgos es la etapa en la que se obtiene toda la información acerca de los activos de la organización y como están expuestos ante eventos o incidentes que puedan mermar las operaciones de la misma así como medir la magnitud de estos eventos, con el fin de administrar los riesgos de forma apropiada.

El propósito de gestión de riesgos es minimizar el impacto de los riesgos negativos y maximizar los riesgos positivos (oportunidades) identificados en la organización. Esto se logrará identificando todos los riesgos conocidos, efectuando una valoración de la probabilidad de su ocurrencia y de su impacto potencial, y creando planes de acción para responder a los riesgos que lo requieran. Por lo tanto un plan de riesgos debería describir [4]:

- Una estrategia de gestión de riesgos
- Alcance del esfuerzo en gestión de riesgos
- Cómo se piensa llevar a cabo la identificación de riesgos
- Cómo se va a llevar a cabo el análisis de riesgos (cualitativo, cuantitativo)
- Cómo se va a llevar a cabo el plan de respuesta (no debe contener los propios planes de respuesta ni tratar riesgos concretos)

- Cómo se va a llevar a cabo la monitorización y control
- Presupuesto de gestión de riesgos
- Calendario de actividades de gestión de riesgos
- Roles y responsabilidades

A continuación en la siguiente figura, se muestra el proceso de la gestión de riesgos.

Figura 2.2 Gestión de Riesgos de una Organización

Fuente: Gustavo A. Solís Montes- CobiT User Convention-CobiT y la administración de riesgos.

2.5 Familias BS 25999-1, BS 25999-2, ISO 22301:2012.

Familia BS 25999

La ocurrencia de desastres (terremotos, incendios, inundaciones, etc.)

en grandes edificios e instalaciones de empresas de todo ámbito, han incrementado la gestión de la continuidad del negocio, y ha generado una demanda en relación a un modelo de gestión que pueda enfrentar estas situaciones de la manera más eficientemente posible.

Para evitar al máximo que estos eventos lleven a la empresa a una situación de inestabilidad económica o de producción, se debe cumplir en la empresa con estándares de administración de continuidad del negocio (BCM – Business Continuity Magnament). Estos estándares se plasman en un plan de continuidad del negocio, este debe estar listo para entrar en acción en cualquier momento, ya que los eventos de terrorismo o naturales no dan aviso.

A BCM se le unen algunos estándares que apoyan sus objetivos en cada área de la empresa, como lo es el BS 25999, que trata a la continuidad del negocio como un sistema de gestión [5].

Esta demanda motivó que el BSI iniciase un proceso de desarrollo de normas específicas sobre la gestión de la continuidad del negocio, que ha dado como resultado la publicación de dos normas:

- BS 25999-1 Gestión de la continuidad del negocio. Código de práctica: Publicada en el 2006, como una guía de implantación del modelo de gestión.
- BS 25999-2 Gestión de la continuidad del negocio. Especificación: Publicada en el 2007, como una especificación

de requisitos para un sistema de gestión de continuidad de negocio y, por lo tanto, con la posibilidad de certificación para aquellas organizaciones que cumplan los requisitos de esta norma.

De este modo, cada organización deberá identificar cuáles son los riesgos que pueden afectar de forma a la continuidad de su negocio y realizar la planificación necesaria para poder seguir manteniendo un funcionamiento regular, hasta que se restablezcan sus condiciones normales de trabajo [6].

A continuación se describe los elementos del ciclo de vida de un BCM, comprende seis elementos:

a. Gestión del programa BCM

Indica que la capacidad de la continuidad del negocio debe ser establecido y mantenido de una forma apropiada de acuerdo al tamaño y complejidad de la organización, comprende:

- Asignar responsabilidades.
- Implementar Continuidad del negocio en la organización.
- La gestión permanente de la continuidad del negocio.

b. Entender a la Organización.

Provee información que habilita la priorización de productos y servicios

que son críticos en una organización ante eventos que puedan paralizarla. El primer paso es la realización del Análisis de impacto del negocio (BIA). Este análisis incluye:

- Que activos de información tales como: suministro eléctrico, disponibilidad de comunicaciones, acceso a equipos de cómputo, son importantes para dar soporte.
- El impacto que produce la interrupción en los servicios que se brinda por parte de la organización.
- Establecer el periodo máximo tolerable de interrupción para cada servicio brindado.

c. Determinar la estrategia de continuidad del negocio

Una vez identificados los riesgos para la continuidad del negocio se debe definir la mejor estrategia para mitigarlo. Para ello, es necesario definir la estructura y documentación del plan de contingencia para que sea implementado de forma óptima en el caso de una interrupción real.

d. Desarrollar e Implementar una respuesta al BCM

Los documentos fundamentales a desarrollar como herramienta para responder de forma eficaz, en el caso de una interrupción que pueda afectar al negocio, son los Planes de Gestión de la Continuidad del

Negocio:

- Estructura la respuesta a incidentes.
- Desarrollo de los planes GCN (Gestión de la Continuidad del Negocio).
- Desarrollo de los Planes de Gestión de Incidentes.

e. Ejercicios, mantenimiento y revisión de los acuerdos para la gestión de la continuidad del negocio.

Debe considerarse la realización de ejercicios (pruebas) para validar los planes y procedimientos desarrollados, así como realizar su revisión y mantenimiento de forma periódica y en intervalos definidos. Esta revisión puede realizarse mediante ejercicios de autoevaluación o auditoría.

f. Incorporación de BCM en la cultura de la organización

Permite que el BCM se convierta en parte de los valores centrales de la organización e infunde confianza en todas las partes interesadas en la capacidad de la organización para hacer frente a interrupciones.

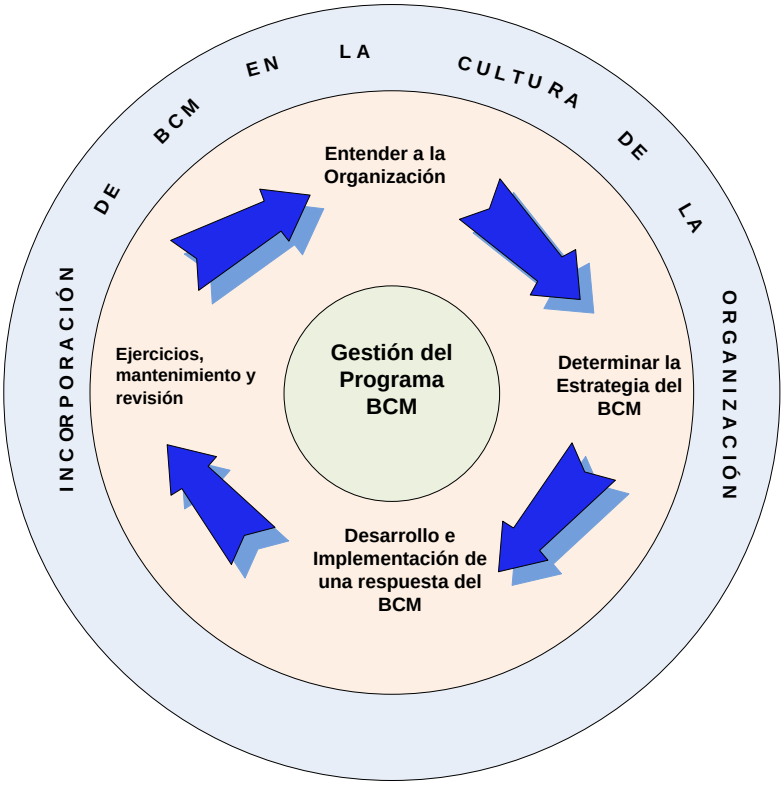


Figura 2.3 Gestión del Programa BCM - BS25999

Fuente: BS 25999-1:2006– Part. 1: Código de practica

Familia ISO

ISO 22301:2012 – Seguridad de la Sociedad – Sistema de Gestión de la continuidad del Negocio – Requerimientos.

Esta norma fue redactada por los principales especialistas en el tema y proporciona el mejor marco de referencia para gestionar la continuidad del negocio en una organización. Esta norma reemplazará al estándar BS 25999-2:2007 “Gestión de la Continuidad del Negocio: Especificaciones”. El nuevo modelo es certificable y auditable.

Poseer un sistema de continuidad del negocio se ha convertido en una exigencia para las empresas que compiten el día de hoy en los mercados globalizados.

Cada miembro involucrado en el plan de contingencia tiene que demostrar que es un proveedor confiable, esto se logra teniendo un SGCN en cada organización para que de esta manera se pueda proteger los procesos esenciales para mantener los productos o servicios que desea el cliente.

Un SGCN es parte del sistema de gestión gerencial que establece, implementa, opera, mantiene y mejora la continuidad del negocio. "Mediante un SGCN se han identificado los procesos esenciales que soportan a los productos o servicios que se desean proteger de escenarios de amenazas" (Alexander, 2007) [7].

En el año 2012, la Organización Internacional para la Normalización (ISO) publicó el estándar "Seguridad de la Sociedad: Sistemas de Continuidad del Negocio-Requisitos". Este estándar es certificable y auditable.

El estándar ISO 22301:2012 aplica el ciclo PDCA para la planificación, establecimiento, implementación, operación, monitoreo, revisión, mantenimiento y la mejora continua de sus operaciones.

El modelo ha sido creado con consistencia con otros estándares de gestión, tales como: ISO 9001:2008, ISO 27001:2005, ISO 20000-

1:2011, ISO 14001:2004 y con el ISO 28000:2007 [7].

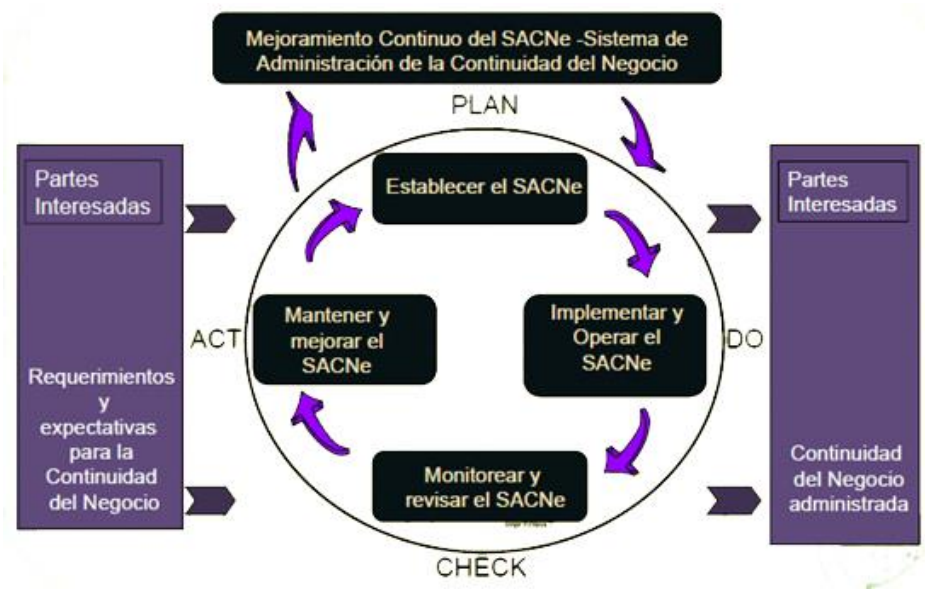


Figura 2.4 Modelo PDCA aplicado al SACNe

Fuente: ISO 22301Societal security

En la Figura 2.4, se observa cada componente del modelo.

El "establecimiento" es el **Plan**. Allí se aprecian los principales requerimientos: Contexto de la Organización, Liderazgo, Planeamiento y Soporte. Las cláusulas 4, 5, 6 y 7 de la norma corresponden al establecimiento.

Seguidamente se tiene la "implementación y operación", el cual es el **Do**; esta etapa del proceso está compuesta por los requerimientos de la cláusula 8. Contemplamos sus principales requerimientos: Planeamiento operativo y Control, Análisis de Impacto en el Negocio (BIA), Evaluación de Riesgos, Estrategias de continuidad,

Procedimientos de Continuidad, Ejercicios y Pruebas.

Luego se tiene la fase “monitoreo y revisión”, la cual representa al **Check**. Allí se pueden apreciar los principales requerimientos de esta sección: Monitoreo y Medición, Análisis y Evaluación Auditoria y Revisión. Esta fase comprende los requerimientos de la cláusula 9 de la norma.

Finalmente, se tiene la fase de “mantenimiento y mejora”, representando a la fase **Act**, la cual engloba todos los requerimientos de la cláusula 10 de la norma: No conformidad y Acción Correctiva, Mejora Continua.

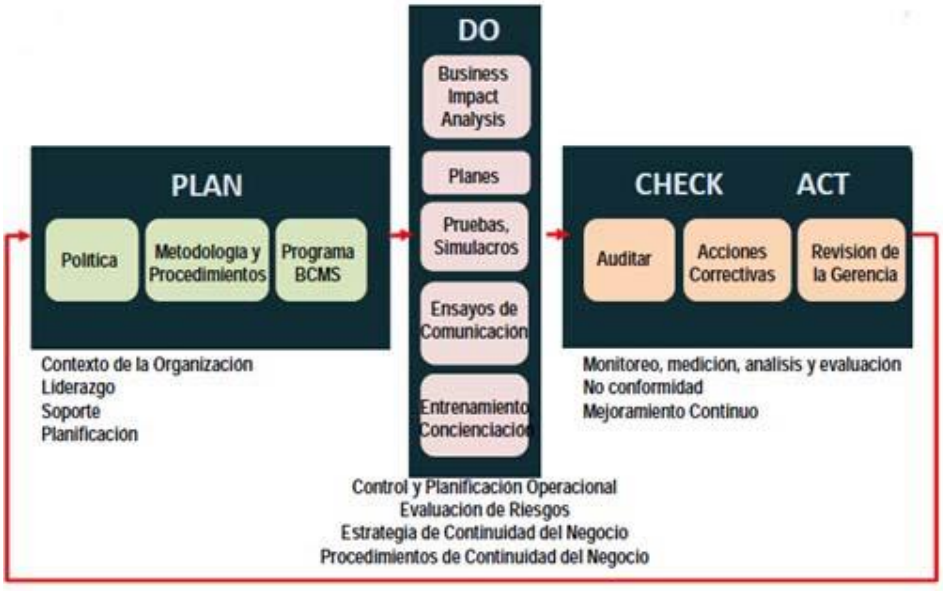


Figura 2.5 ISO 22301 PDCA aplicado al proceso BCM

Fuente: Jorge Olaya - BCM

CAPÍTULO 3

ANÁLISIS DEL RIESGO E IMPACTO EN EL NEGOCIO

3.1 Metodología de Análisis y Gestión de Riesgos

Una parte importante del Análisis y Gestión de Riesgos radica básicamente en que va a permitir identificar las amenazas a las que se encuentran expuestos los diferentes activos de información que posee la facultad, pudiendo estimar con qué frecuencia se materialización dichas amenazas y valorar el impacto que provoca dichas amenazas.

Para este análisis de riesgo voy a utilizar MAGERIT en su versión 3 [8]

que fue elaborada por el Consejo Superior de Administración Electrónica CSAE de España, la cual facilita la gestión de riesgos y permite valorizar dichos activos ante las amenazas que los puedan perjudicar. La metodología está incorporada en 3 libros que son:

1. El libro de los Método: Describe la estructura que debe tener el modelo de gestión de riesgos acorde a lo que propone ISO para la gestión de riesgos.

2. El libro de Catálogo de Elementos: Es parecido a un inventario, en donde se establecen los activos de información y características que deben tomarse en cuenta al momento de valorarlos, junto con un listado de amenazas y controles para los mismos.

3. El libro de Guía de Técnicas: Describe técnicas utilizadas en el análisis de riesgos y ejemplos con tablas, árboles de ataque, análisis de costo beneficio, diagramas de flujo y buenas prácticas [9].

La metodología de MAGERIT se ajusta perfectamente dentro de la implementación de la gestión de riesgos expresada en la Norma ISO 31000 (Figura 3.1), a lo que se “denomina “Proceso de Gestión de los Riesgos”

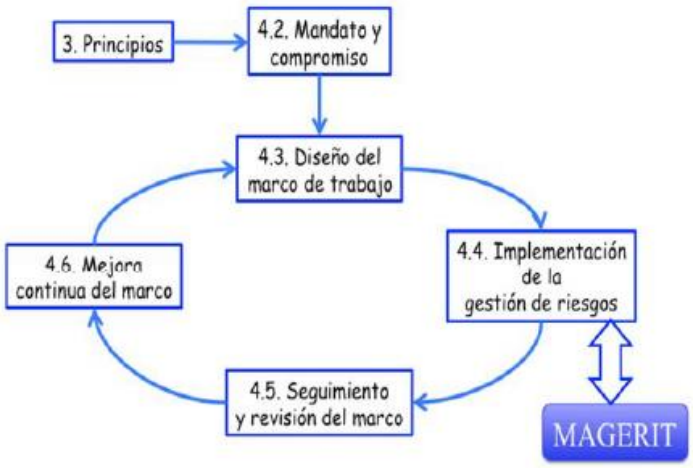


Figura 3.1 ISO 31000- Marco de trabajo para la gestión de riesgos

Fuente: MAGERIT – versión 3.0 Libro 1: Método

MAGERIT tiene los siguientes objetivos:

Directos:

- Concientizar a los responsables del manejo de información de la existencia de riesgos o amenazas y la necesidad de gestionarlos.
- Posee un método sistemático para analizar riesgos tecnológicos.
- Descubre y planifica tratamientos para mantener los riesgos bajo control.

Indirectos:

- Prepara a la organización u empresa para procesos como la auditoria, certificaciones o acreditaciones.

Elementos y dimensiones de Seguridad para el análisis y gestión de riesgos

La seguridad es la capacidad de las redes y de los sistemas de información para resistir con un nivel de confianza aceptado, los incidentes o acciones ilícitas o malintencionadas que comprometen la disponibilidad, integridad y confiablidad de la información almacenada o transmitida en los servicios de dichas redes y sistemas.

A continuación detallo las diferentes dimensiones o propiedades de la seguridad:

Confidencialidad: Es una propiedad que impide la divulgación de información a individuos o entidades no autorizadas. Asegura el acceso a la información solo a aquellas personas debidamente autorizadas

Integridad: Es mantener con exactitud la información tal cual fue generada, sin ser manipulada ni alterada por personas no autorizada.

Disponibilidad: Es la característica o propiedad de la información de encontrarse a disposición para quienes deban acceder a ella, ya sea personas, procesos u aplicaciones. Es el acceso a la información y a los sistemas por personas debidamente autorizadas en el momento que así lo requieran.

A estas propiedades de la seguridad de la información se pueden

añadir otras, utilizadas por la metodología MAGERIT a continuación se detallan:

Autenticidad: es una propiedad o característica que permite identificar el generador de la información. Consiste en asegurar que una entidad u persona es quien dice ser o bien que garantice la fuente de la que proceden los datos.

Trazabilidad: es el aseguramiento de que en todo momento se podrá determinar quién hizo que y en qué momento. La trazabilidad se materializa en la integridad de los registros de actividad [10].

Con una visión en conjunto MAGERIT tiene dos grandes tareas a realizar para la Gestión de Riesgos:

1.- Análisis de Riesgos: determinar lo que posee la organización o entidad y estimar los posibles riesgos que podrían ocurrir.

2.- Tratamiento de los Riesgos: cómo sobrevivir a los posibles incidentes que puedan suscitarse y seguir operando en las mejores condiciones posibles. El riesgo se reduce a un nivel residual que la gerencia puede asumir [10].

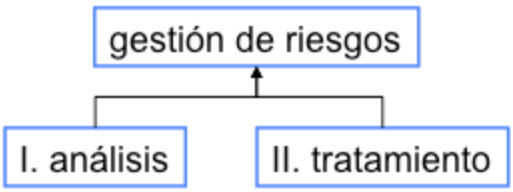


Figura 3.2 Gestión de riesgos según MAGERIT

Fuente: MAGERIT – versión 3.0 Libro 1: Método

El análisis de riesgos considera los siguientes elementos:

Activos, son los elementos del sistema de información.

Amenazas, son personas, objetos, o situaciones que pueden comprometer a los activos causando un perjuicio a la Organización.

Salvaguardas (o contra medidas), son medidas de protección desplegadas para que aquellas amenazas no causen tanto daño

Con estos elementos se puede estimar:

El impacto: lo que podría pasar o suceder dentro de la organización.

El riesgo: lo que probablemente pase para la organización.

Formalmente, la gestión de los riesgos está estructurada de forma metódica en las normas ISO y se propone el siguiente esquema:

La determinación del contexto permite determinar las políticas y procedimientos tanto internos como externos, a llevar a cabo para gestionar los riesgos dentro de una organización.

La identificación de los riesgos busca una relación de los posibles puntos de peligro. Lo que se identifique será analizado. Lo que no se identifique quedará como riesgo ignorado.

El análisis de los riesgos busca catalogar los riesgos identificados, bien cuantificando sus consecuencias (análisis cuantitativo), o bien ordenando su importancia relativa (análisis cualitativo).

La evaluación de los riesgos va un paso más allá del análisis técnico y traduce las consecuencias a términos de negocio. Aquí entran

factores de estrategia y de política permitiendo tomar decisiones respecto de qué riesgos se aceptan y cuáles no, así como en qué caso podemos aceptarlo y trabajar en su tratamiento.

El tratamiento de los riesgos recopila las actividades involucradas a modificar la situación del riesgo.

Comunicación y consulta. Es importante recordar que los sistemas de información deben ser soporte de la productividad de la Organización. Es ilógico un sistema muy seguro pero que impide que la Organización alcance sus objetivos. Hay que contar con la colaboración: los usuarios cuyas necesidades deben ser tenidas en cuenta, los proveedores externos, a los que hay proporcionar instrucciones claras para poder exigirles el cumplimiento de los niveles de servicio requeridos, como la gestión de incidentes de seguridad, los órganos de gobierno para establecer canales de comunicación que consoliden la con-fianza de que el sistema de información responderá sin sorpresas para atender a la misión de la Entidad.

Seguimiento y revisión. Es importante nunca olvidar que el análisis de riesgos es una actividad de despacho y que es imprescindible ver las consecuencias en la práctica y actuar en consecuencia, tanto reaccionando diligentemente a los incidentes, como mejorando continuamente nuestro conocimiento del sistema.

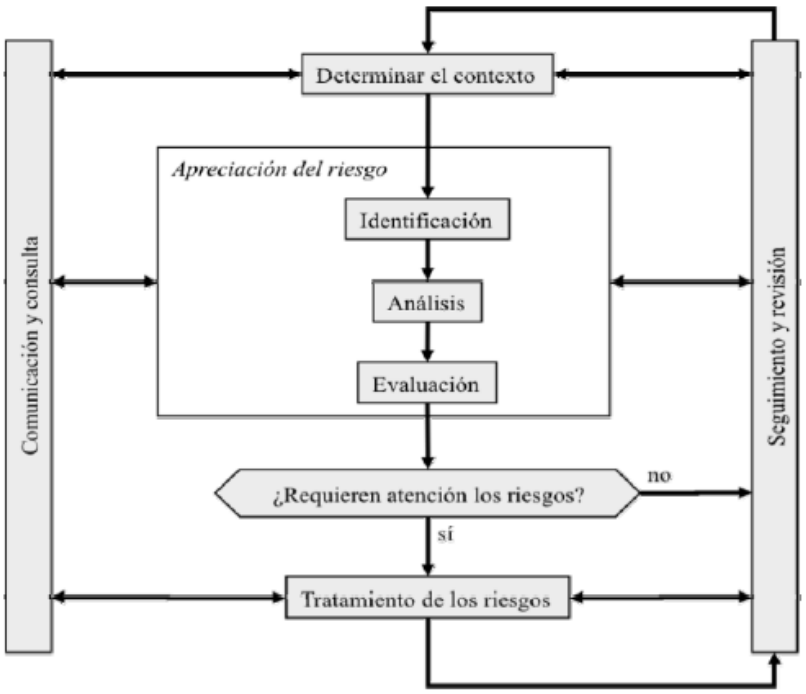


Figura 3.3 Proceso de gestión de riesgos
Fuente: ISO 31000

3.2 Identificar los procesos y recursos críticos de IT del negocio

Para identificar los procesos críticos del Departamento de Soporte Técnico, es necesario entender la estructura organizacional del DST y su contexto, identificar y establecer en base a su conocimiento y experiencia, cuales son los procesos y recursos que se ven involucrados en la entrega de los productos o servicios que entrega a sus usuarios.

Entendiendo a la Organización y su contexto

Es de vital importancia entender y conocer el entorno de la

organización del Departamento de Soporte Técnico, y todos los servicios que brinda a sus usuarios, así como tomo aquello que no permita cumplir los objetivos del negocio.

Descripción del Departamento de Soporte Técnico

El Departamento de Soporte Técnico (DST-FIEC) de la Facultad de Ingeniería en Electricidad y Computación, es quien se encarga de administrar los recursos informáticos de la facultad y del correcto funcionamiento de los laboratorios de computación. Desde el año 2001 en vista del progresivo desarrollo en infraestructura técnica, comunicaciones y de edificios se incorporaron personal de planta para atender lo mejor posible los requerimientos informáticos de la Facultad y desde el año 2003 se crea la “Sala de Asistentes” que le da la figura administrativa interna. En el año 2012, el Decano de la facultad propone crear el “Departamento de Soporte Técnico” (DST-FIEC).

Entre las tareas que tiene el Departamento (DST) están las siguientes:

- Administración tecnológica en el ámbito informático y de comunicaciones de la Facultad.
- Servicio de correo y aplicaciones bajo plataforma google, con dominio FIEC.

- Soporte Técnico informático a los 34 laboratorios, personal administrativo y profesores de la Facultad, con un aproximado de 850 computadoras.
- Administración y soporte de redes de datos y servidores.
- Desarrollo, implementación, Desarrollo, implementación, administración y soporte de sistemas informáticos internos: CRM (Asistencia Técnica), Controlac, Reservar Salas, Creación de Cuentas, ARA, Sistema de Pasantías, Sistema de Reuniones, Correos.
- Soporte a sistemas de audio y video proyección en Aulas, Auditorio y Laboratorios.
- Administración y soporte del Sitio Web.
- Administración del Laboratorio de Computación (Lab-Fiec), edificio 16-C, 16A, 15, 15A y 24A.

Diseño de Red de la Infraestructura Física del DST

En la siguiente Figura 3.4 se puede observar los equipos de telecomunicaciones que se encuentran distribuidos en los distintos cuartos de Rack ubicados en toda la Faculta de Ingeniería en Electricidad y Computación así como las conexiones entre el edificio principal y los demás laboratorios de la FIEC.

La conexión a internet es proporcionada por el ISP Telconet, pero además el DST se comunica con los equipos de GTySI (Gerencia de Tecnologías y Sistemas de Información).

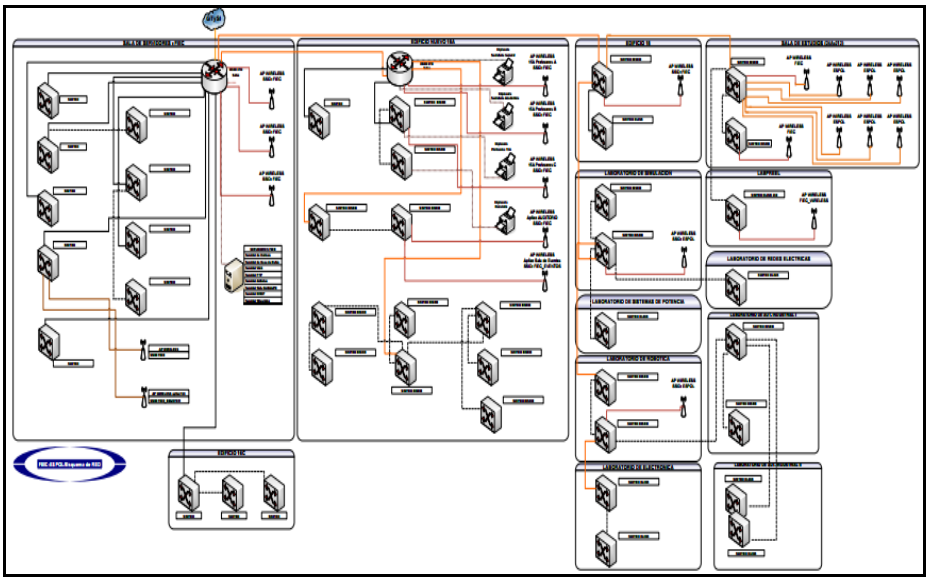


Figura 3.4 Diagrama de Red de la Infraestructura Física de la FIEC

Fuente: DST

Organigrama

A continuación el organigrama estructural de la FIEC, en el cual se puede apreciar la estructura del Departamento de Soporte Técnico [11].

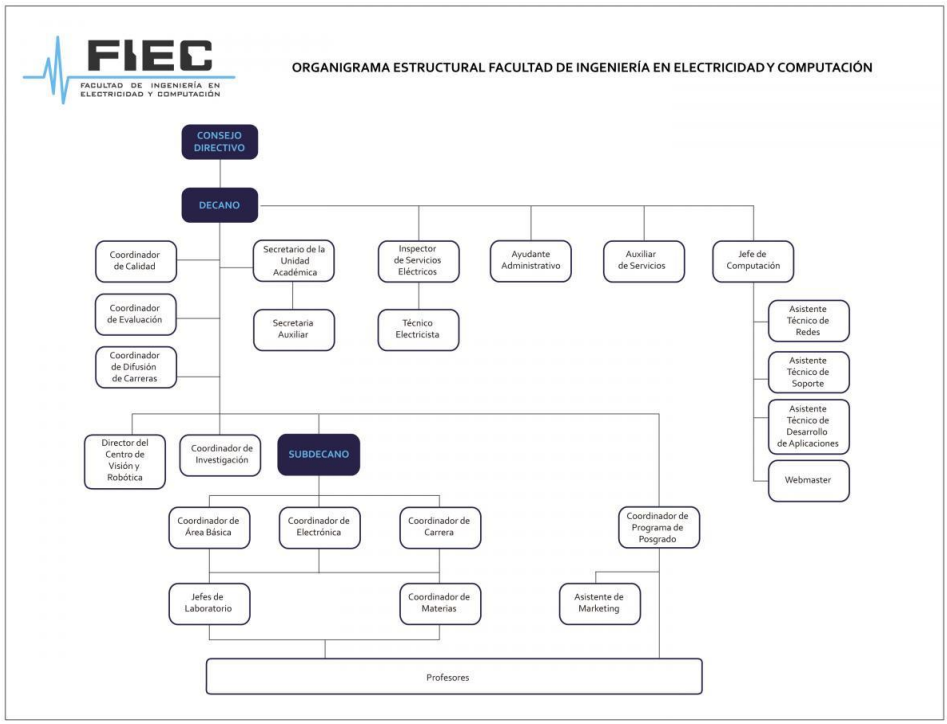


Figura 3.5 Organigrama de la FIEC

Fuente: **https://www.fiec.espol.edu.ec/es/organigrama.**

Análisis Interno del DST

En este análisis se podrá conocer como están alineados los diferentes procesos para conseguir los objetivos del DST, su misión, visión, lo servicios que ofrece a sus usuarios en la FIEC, los procesos q los soportan y los recursos que utilizan.

Misión del DST-FIEC

Servir de apoyo tecnológico para profesores y estudiantes, a fin de que los recursos informáticos con los que cuenta la Facultad sean

aprovechados al máximo, para potenciar el desarrollo académico-científico de la FIEC [12].

Visión del DST-FIEC

Forjar líderes emprendedores para que aportando con sus capacidades, seamos referentes en implementaciones tecnológicas, que colaboren con el desarrollo de la ESPOL y de la sociedad en general [12].

Estrategia del DST-FIEC

El Departamento de Soporte Técnico de la FIEC tiene los siguientes puntos como lineamientos básicos para establecer su conducta organizacional y estrategia administrativa:

- Establecer aptitudes internas dentro del personal, tales como:
  - Puntualidad
  - Responsabilidad
  - Efectividad
  - Eficiencia
  - Orden

- Incentivar a los integrantes que conforman el DST-FIEC estén continuamente actualizando sus conocimientos en el área tecnológica.
- Incentivar que los integrantes del DST-FIEC que asuman su trabajo no sólo como una obligación, sino como una forma de aprendizaje. De esta forma, podrán aplicar los conocimientos adquiridos en su futuro profesional.
- Mantener un estatus de calidad, alineado con los objetivos establecidos en la Política de Calidad de la ESPOL.

Identificar activos de Información

Para identificar los recursos críticos de TI del DST, se debe, primeramente identificarlos, a continuación en la siguiente tabla se detallan los activos de información.

Los activos de información en la Tabla 1 se han agrupado en tipos específicos dada la naturaleza de los mismos, de esta forma facilitará su mejor entendimiento.

Tabla 1 Activos de la FIEC

Fuente: [14]

ACTIVOS DE LA FIEC	
[D] Datos	
[bd_crm]	Base de Datos de CRM
[bd_reservar]	Base de Datos de Reservar Salas
[bd_controlac]	Base de Datos de CONTROLAC
[bd_reunion]	Base de Datos de Reuniones
[bd_ara]	Base de Datos de ARA
[bd_satt]	Base de Datos de SATT
[backup]	Copias de Respaldo
[source]	Código Fuente
[files]	Archivos
[bd_controlpc]	Base de Datos de CONTROLPC
[conf]	Datos de Configuración
[log]	Registro de Actividad
[bd_ldap]	LDAP
[bd_sitioFiec]	Base de Datos del Sitio Web de la FIEC
[S] Servicios	
[serv_a/v]	Audio y Video
[serv_equi]	Préstamo de Equipos
[serv_support]	Asistencia Técnica
[serv_dev]	Implementación y Administración de sistemas/sitio web para la FIEC
[serv_acco]	Gestión de Identidades (Creación de cuentas)
[serv_wifi]	Red Inalámbrica exclusiva de la FIEC
[email]	Correo Electrónico
[serv_mante]	Mantenimiento a Equipos
[serv_file]	Almacenamiento de archivos y aplicaciones desarrolladas por estudiantes
[serv_labs]	Préstamo de Laboratorios
[SW] Software - Aplicaciones Informáticas	
[sis_crm]	Sistema CRM
[sis_controlac]	Sistema CONTROLAC
[sis_creacion]	Sistema Creación de Cuentas
[sis_reunion]	Sistema de Reuniones
[sis_reservar]	Sistema Reservar Salas
[sis_ara]	Sistema ARA
[sis_satt]	Sistema SATT
[pkt]	Repositorio de Software Vario

[sis_controlpc]	Sistema CONTROLPC
[av]	Antivirus
[sis_portal]	Portal Cautivo
[HW] Equipos Informáticos	
[print]	Medios de Impresión
[scan]	Escáneres
[cam]	Cámara IP
[mobile]	Laptop
[srv_stmg]	Streaming
[wap]	Punto de Acceso Inalámbrico
[pc]	Computador
[srv_files]	Archivos
[srv_control]	Control-PC
[srv_dhcp]	DHCP
[srv_radius]	Radius
[switch]	Conmutadores
[router]	Ruteadores
[srv_mail]	Correos
[srv_db]	Base de Datos
[srv_web]	Web
[srv_ant]	Antivirus
[**COM] Redes de Comunicaciones**	
[wifi]	Red Inalámbrica
[lan]	Red cableada
[**MEDIA] Soportes de Información**	
[disk]	Discos
[san]	Almacenamiento en red
[tape]	Cinta Magnética
[AUX] Equipamiento Auxiliar	
[furniture]	Mobiliario: armarios, racks etc
[tools]	Herramientas de Soporte y Mantenimiento
[tools_network]	Herramientas de Soporte y Mantenimiento redes
[ss]	Sistema de Seguridad
[ups]	Sistema de Alimentación Ininterrumpida
[ac]	Equipos de Climatización
[L] Instalaciones	
[building]	Edificio
[local]	Cuarto de rack y servidores
[P] Personal	
[adm]	Administradores de la Infraestructura Tecnológica
[com]	Administrador de Redes y Servidores
[ast]	Analista de Soporte Técnico

[des]	Desarrolladores / Programadores
[wm]	Web master

Valoración de los activos

Para la valoración de los activos se ha tomado en cuenta una escala cualitativa de criterios que va del 0 al 10, se muestra la Tabla 2.

Tabla 2 Valoración de los Activos

Fuente: El autor

Valor		Criterio
10	Extremo	Daño extremadamente grave
9	Muy alto	Daño muy grave
6-8	Alto	Daño grave
3-5	Medio	Daño importante
1-2	Bajo	Daño menor
0	Despreciable	Irrelevante a efectos prácticos

Los activos de información del DST, han sido valorados de acuerdo a los criterios mencionados anteriormente y en las dimensiones de Disponibilidad, Integridad y Confidencialidad, además se presenta una representación gráfica, en barras de los diferentes tipos de activos de información, ver Figura 3.6.

Tabla 3 Valoración de los Activos de la FIEC

Fuente: El autor

ACTIVOS DE LA FIEC		[D]	[I]	[C]
[D] Datos		**5**	**6**	**5**
[bd_crm]	Base de Datos de CRM	1	3	3
[bd_reservar]	Base de Datos de Reservar Salas	3	3	3
[bd_controlac]	Base de Datos de CONTROLAC	5	5	3
[bd_reunion]	Base de Datos de Reuniones	3	4	3
[bd_ara]	Base de Datos de ARA	5	5	5
[bd_satt]	Base de Datos de SATT	5	5	7
[backup]	Copias de Respaldo	7	7	5
[source]	Código Fuente	7	7	5
[files]	Archivos	7	7	6
[bd_controlpc]	Base de Datos de CONTROLPC	5	6	7
[conf]	Datos de Configuración	7	7	7
[log]	Registro de Actividad	7	7	3
[bd_ldap]	LDAP	7	7	9
[bd_sitioFiec]	Base de Datos del Sitio Web de la FIEC	7	7	7
[S] Servicios		**5**	**5**	**4**
[serv_a/v]	Audio y Video	3	1	1
[serv_equi]	Préstamo de Equipos	3	1	1
[serv_support]	Asistencia Técnica	5	5	3
[serv_dev]	Implementación y Administración de sistemas/sitio web para la FIEC	7	7	5
[serv_acco]	Gestión de Identidades (Creación de cuentas)	3	3	2
[serv_wifi]	Red Inalámbrica exclusiva de la FIEC	5	5	5
[email]	Correo Electrónico	9	9	7
[serv_mante]	Mantenimiento a Equipos	5	3	3
[serv_file]	Almacenamiento de archivos y aplicaciones desarrolladas por estudiantes	1	7	5
[serv_labs]	Préstamo de Laboratorios	7	5	3
[SW] Software - Aplicaciones Informáticas		**5**	**5**	**3**

[sis_crm]	Sistema CRM	1	1	3
[sis_controlac]	Sistema CONTROLAC	5	4	3
[sis_creacion]	Sistema Creación de Cuentas	5	4	2
[sis_reunion]	Sistema de Reuniones	3	3	3
[sis_reservar]	Sistema Reservar Salas	3	5	3
[sis_ara]	Sistema ARA	7	5	3
[sis_satt]	Sistema SATT	7	5	3
[pkt]	Repositorio de Software Vario	7	5	5
[sis_controlpc]	Sistema CONTROLPC	5	5	1
[av]	Antivirus	9	9	7
[sis_portal]	Portal Cautivo	5	5	3
[HW] Equipos Informáticos		**5**	**5**	**4**
[print]	Medios de Impresión	3	1	0
[scan]	Escáneres	1	1	1
[cam]	Cámara IP	3	3	3
[mobile]	Laptop	1	1	3
[srv_stmg]	Streaming	1	1	3
[wap]	Punto de Acceso Inalámbrico	3	3	3
[pc]	Computador	7	3	3
[srv_files]	Archivos	5	6	7
[srv_control]	Control-PC	5	5	5
[srv_dhcp]	DHCP	5	5	3
[srv_radius]	Radius	5	5	3
[switch]	Conmutadores	9	9	6
[router]	Ruteadores	9	9	6
[srv_mail]	Correos	7	9	7
[srv_db]	Base de Datos	7	9	8
[srv_web]	Web	7	9	7
[srv_ant]	Antivirus	9	9	7
[COM] Redes de Comunicaciones		**8**	**8**	**7**
[wifi]	Red Inalámbrica	7	7	5
[lan]	Red cableada	9	9	9
[MEDIA] Soportes de Información		**7**	**5**	**4**
[disk]	Discos	7	5	5
[san]	Almacenamiento en red	7	6	3
[tape]	Cinta Magnética	7	5	5
[AUX] Equipamiento Auxiliar		**5**	**3**	**1**
[furniture]	Mobiliario: armarios, racks etc	5	0	0
[tools]	Herramientas de Soporte y Mantenimiento	1	1	0

[tools_network]	Herramientas de Soporte y Mantenimiento redes	1	1	0
[ss]	Sistema de Seguridad	7	3	7
[ups]	Sistema de Alimentación Ininterrumpida	7	6	0
[ac]	Equipos de Climatización	7	7	0
[L] Instalaciones		**9**	**2**	**2**
[building]	Edificio	9	1	0
[local]	Cuarto de rack y servidores	9	3	3
[P] Personal		**7**	**5**	**5**
[adm]	Administradores de la Infraestructura Tecnológica	7	5	5
[com]	Administrador de Redes y Servidores	7	5	5
[ast]	Analista de Soporte Técnico	7	5	5
[des]	Desarrolladores / Programadores	7	5	5
[wm]	Web master	7	5	5

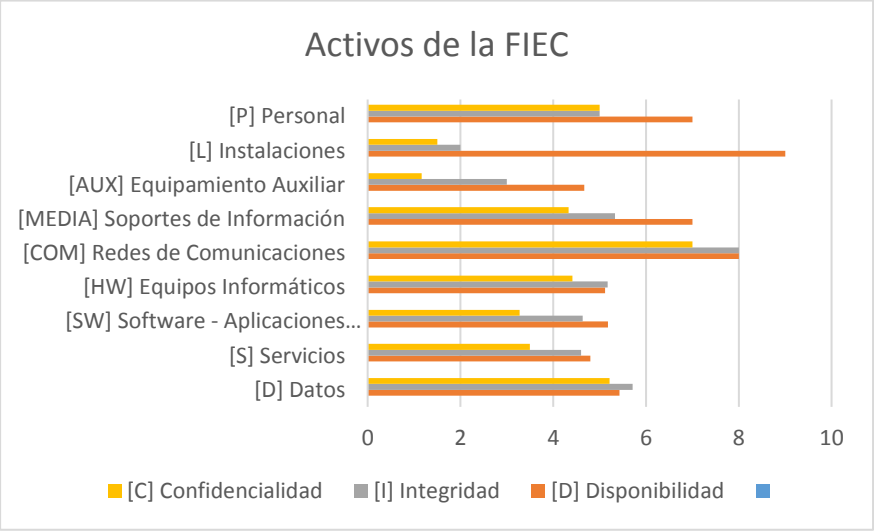


Figura 3.6 Gráfica estadística de la Valoración de los tipos de Activos de la FIEC

Fuente: El autor

3.3 Identificar los eventos o incidentes que puedan ocasionar interrupciones en los servicios críticos de la organización.

Luego de haber identificado los diferentes activos de información que posee el DST, y analizado los activos de acuerdo a su valoración, se puede detectar las siguientes amenazas como posibles desencadenadores de interrupciones en el correcto funcionamiento del DST, los mismos que se dividen en cuatro grupos principales: [N] Desastres Naturales, en este caso voy hacer especial énfasis en los Terremotos. Según análisis y fuentes del Gobierno [13] se ha registrado 671 personas fallecidas durante el terremoto del 16 de abril del 2016, según la escala de Richter de magnitud de 7.8, con epicentro entre las parroquias Pedernales y Cojimíes del cantón Pedernales, en la provincia de Manabí, aproximadamente 1629 réplicas se han tenido después del suceso, y este riesgo de gran magnitud es uno de los más desastrosos que puede llegar a suceder en la actualidad en nuestro país, luego tenemos las amenazas de [I] De Origen Industrial, los [E] Errores y fallos no intencionados, y los [A] Ataques intencionados.

A continuación se detalla las diferentes amenazas detectadas para cada activo de acuerdo a su afectación en la disponibilidad, integridad y confidencialidad (Tabla 4).

Tabla 4 Valoración de las amenazas por Activos de Información

Fuente: El autor

	ACTIVOS																											
	[D]			[S]			[SW]			[HW]			[COM]			[MEDIA]			[AUX]			[L]			[P]		
Amenazas	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]
[N] Desastres Naturales																												
[N.1] Fuego										X						X			X			X						
[N.2] Daños por agua										X						X			X			X						
[N.*] Desastres naturales - Terremotos										X						X			X			X						
[I] De Origen Industrial																												
[I.1] Fuego										X						X			X			X						
[I.2] Daños por agua										X						X			X			X						
[I.*] Desastres industriales										X						X			X			X						
[I.3] Contaminación mecánica										X						X			X									
[I.4] Contaminación electromagnética										X						X			X									
[I.5] Avería de origen físico o lógico							X			X						X			X									
[I.6] Corte del suministro eléctrico										X						X			X									
[I.7] Condiciones inadecuadas de temperatura o humedad										X						X			X									
[I.8] Fallo de servicios de comunicaciones													X															
[I.9] Interrupción de otros servicios y suministros esenciales																			X									
[I.10] Degradación de los soportes de almacenamiento de la información																X												
[I.11] Emanaciones electromagnéticas												X						X			X			X				
[E] Errores y fallos no intencionados																												
[E.1] Errores de los usuarios	X	X	X	X	X	X	X	X	X							X	X	X										
[E.2] Errores del administrador	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X										
[E.3] Errores de monitorización (log)		X																										
[E.4] Errores de Configuración		X																										
[E.7] Deficiencias en la organización																									X			
[E.8] Difusión de software dañino							X	X	X																			
[E.9] Errores de [re]encaminamiento						X			X					X														
[E.10] Errores de secuencia				X				X						X														
[E.14] Escapes de información			X																									
[E.15] Alteración accidental de la información		X			X			X						X			X						X					
[E.18] Destrucción de información	X			X			X						X			X						X						
[E.19] Fugas de información			X			X			X						X			X						X				X
[E.20] Vulnerabilidades de los programas (software)							X	X	X																			
[E.21] Errores de mantenimiento/actualización de programas (software)							X	X																				
[E.23] Errores de mantenimiento/actualización de equipos (hardware)										X						X			X									
[E.24] Caída del sistema por agotamiento de recursos				X						X			X															
[E.25] Pérdida de equipos										X		X				X		X	X		X							
[E.28] Indisponibilidad del personal																									X			

	ACTIVOS																												
	[D]			[S]			[SW]			[HW]			[COM]			[MEDIA]			[AUX]			[L]			[P]		
Amenazas	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]	[D]	[I]	[C]
[A] Ataques intencionados																											
[A.3] Manipulación de los registros de actividad (log)		x																									
[A.4] Manipulación de la configuración	x	x	x																								
[A.5] Suplantación de la identidad del usuario		x	x		x	x		x	x					x	x												
[A.6] Abuso de privilegios de acceso	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x												
[A.7] Uso no previsto				x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x	x			
[A.8] Difusión de software dañino							x	x	x																		
[A.9] [Re-] encaminamiento de mensajes						x			x						x												
[A.10] Alteración de secuencia					x			x						x													
[A.11] Acceso no autorizado		x	x		x	x		x	x		x	x		x	x		x	x		x	x		x	x			
[A.12] Análisis de tráfico															x												
[A.13] Repudio		x			x																						
[A.14] Interceptación de información (escucha)															x												
[A.15] Modificación deliberada de la información		x			x			x						x			x						x				
[A.18] Destrucción de información	x			x			x									x						x					
[A.19] Divulgación de información			x			x			x						x			x						x				
[A.22] Manipulación de programas							x	x	x																		
[A.23] Manipulación de los equipos										x		x				x		x	x		x						
[A.24] Denegación de servicio				x						x			x														
[A.25] Robo										x		x				x		x	x		x						
[A.26] Ataque destructivo										x						x			x			x					
[A.27] Ocupación enemiga																						x		x			
[A.28] Indisponibilidad del personal																									x		
[A.29] Extorsión																									x	x	x
[A.30] Ingeniería Social (picaresca)																									x	x	x

3.4 Analizar y evaluar la probabilidad de ocurrencia y el impacto causado por incidentes de seguridad de la Información.

Para valorizar las amenazas, se ha tomado en cuenta una escala cualitativa, dentro de estas propiedades están la probabilidad y el impacto; para la probabilidad de ocurrencia de una determinada amenaza se tiene una escala del uno- Sería Excepcional, al cinco- Casi seguro que suceda, y el impacto que causaría esa amenaza sobre el activo de información, la escala va desde uno- Insignificante hasta el cinco- Catástrofe. Tal como muestra la siguiente Tabla 5.

Tabla 5 Valoración de la Probabilidad y el Impacto

Fuente: el autor

	IMPACTO				
PROBABILIDAD	1– Insignificante	2– Pequeño	3– Moderado	4– Grande	5– Catástrofe
5- Casi seguro que sucede	Medio (5)	Alto (10)	Alto (15)	Muy alto (20)	Muy alto (25)
4- Muy probable	Medio (4)	Medio (6)	Alto (12)	Alto (16)	Muy alto (20)
3- Es posible	Bajo (3)	Medio (5)	Medio (9)	Alto (12)	Alto (15)
2- Es raro que suceda	Bajo (2)	Bajo (4)	Medio (6)	Medio (8)	Alto (10)
1- Sería excepcional	Bajo (1)	Bajo (2)	Bajo (3)	Bajo (4)	Medio (5)

Tomando en cuenta estos criterios se ha procedido a valorar tanto la probabilidad como el impacto a cada uno de los activos de información, por ejemplo en este caso voy a mostrar la valoración de los [D] Datos y [S] Servicios así como su Matriz de Riesgos de acuerdo a la Tabla 6.

Se distinguen mediante los colores Alto (rojo), Medio (naranja) y Bajo (verde).

Tabla 6 Análisis de Riesgos

Fuente: El autor

ANÁLISIS DE RIESGOS				
ACTIVOS	**AMENAZA**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**
[D] Datos	[E.1] Errores de los usuarios	4- Muy probable	2–Pequeño	Medio
	[E.2] Errores del administrador	3- Es posible	4–Grande	**Alto**
	[E.3] Errores de monitorización (log)	2- Es raro que suceda	4–Grande	Medio
	[E.4] Errores de Configuración	2- Es raro que suceda	4–Grande	Medio
	[E.14] Escapes de información	1- Sería excepcional	3–Moderado	Bajo
	[E.15] Alteración accidental de la información	1- Sería excepcional	4–Grande	Bajo
	[E.18] Destrucción de información	1- Sería excepcional	5–Catástrofe	Medio
	[E.19] Fugas de información	1- Sería excepcional	4–Grande	Bajo
	[A.4] Manipulación de la configuración	1- Sería excepcional	4–Grande	Bajo
	[A.5] Suplantación de la identidad del usuario	2- Es raro que suceda	3–Moderado	Medio
	[A.6] Abuso de privilegios de acceso	1- Sería excepcional	4–Grande	Bajo
	[A.11] Acceso no autorizado	1- Sería excepcional	3–Moderado	Bajo
	[A.13] Repudio	2- Es raro que suceda	3–Moderado	Medio
	[A.15] Modificación deliberada de la información	1- Sería excepcional	5–Catástrofe	Medio
	[A.18] Destrucción de información	3- Es posible	4–Grande	**Alto**
	[A.19] Divulgación de información	2- Es raro que suceda	4–Grande	Medio

[S] Servicios	[E.1] Errores de los usuarios	4- Muy probable	1– Insignificante	Bajo
	[E.2] Errores del administrador	3- Es posible	2–Pequeño	Medio
	[E.9] Errores de [re]encaminamiento	1- Sería excepcional	4–Grande	Bajo
	[E.10] Errores de secuencia	2- Es raro que suceda	2–Pequeño	Bajo
	[E.15] Alteración accidental de la información	2- Es raro que suceda	4–Grande	Medio
	[E.18] Destrucción de información	1- Sería excepcional	5–Catástrofe	Medio
	[E.19] Fugas de información	1- Sería excepcional	1– Insignificante	Bajo
	[E.24] Caída del sistema por agotamiento de recursos	3- Es posible	4–Grande	**Alto**
	[A.5] Suplantación de la identidad del usuario	1- Sería excepcional	4–Grande	Bajo
	[A.6] Abuso de privilegios de acceso	3- Es posible	4–Grande	**Alto**
	[A.7] Uso no previsto	3- Es posible	2–Pequeño	Medio
	[A.9] [Re-] encaminamiento de mensajes	1- Sería excepcional	3–Moderado	Bajo
	[A.10] Alteración de secuencia	2- Es raro que suceda	2–Pequeño	Bajo
	[A.11] Acceso no autorizado	1- Sería excepcional	4–Grande	Bajo
	[A.13] Repudio [A.15] Modificación deliberada de la información	1- Sería excepcional 1- Sería excepcional	2–Pequeño 4–Grande	Bajo Bajo
	[A.18] Destrucción de información	1- Sería excepcional	5–Catástrofe	Medio
	[A.19] Divulgación de información	2- Es raro que suceda	2–Pequeño	Bajo
	[A.24] Denegación de servicio	1- Sería excepcional	4–Grande	Bajo

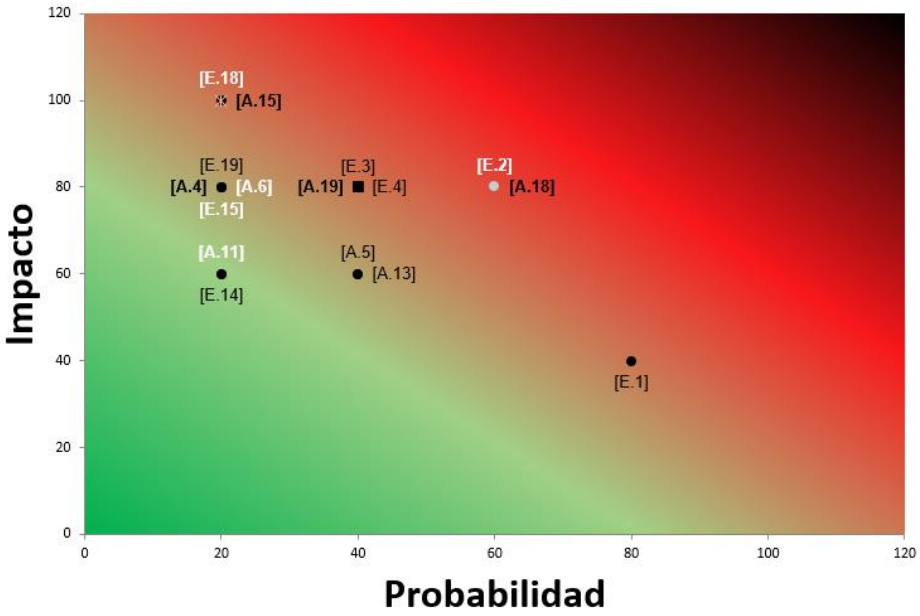


Figura 7 Gráfico Mapa de Riesgos de los Activos de [D] Datos

Fuente: El autor

Se puede apreciar otros gráficos de mapas de riesgos los mismos que se muestran en una escala un poco más grande para poder visualizarlos mejor, pero para este análisis, se obtiene el riesgo multiplicando la probabilidad por el impacto.

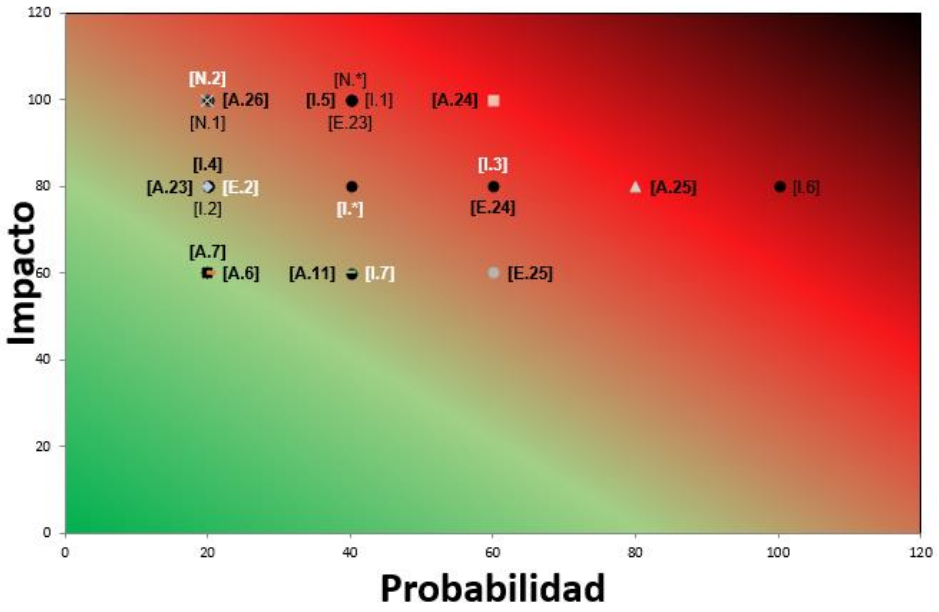


Figura 8 Gráfica del Mapa de Riesgos de activos [HW] Equipos Informáticos

Fuente: El autor

En la siguiente Tabla 7 se muestra los activos de información con los riesgos con valoración más altos y altos, entre la probabilidad de ocurrencia y el impacto que genera, estas son las amenazas en las que se basará el diseño del plan de contingencia.

En el siguiente capítulo se deben analizar estas amenazas y poner especial atención de cómo mitigarlos mediante el plan de contingencia.

Tabla 7 Activos de Información con Riesgos Altos

Fuente: El autor

ACTIVOS	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
[D] Datos	[E.2] Errores del administrador	3- Es posible	4–Grande	**Alto**
	[A.18] Destrucción de información	3- Es posible	4–Grande	**Alto**
[S] Servicios	[E.24] Caída del sistema por agotamiento de recursos	3- Es posible	4–Grande	**Alto**
	[A.6] Abuso de privilegios de acceso	3- Es posible	4–Grande	**Alto**
[SW] Software	[I.5] Avería de origen físico o lógico	2- Es raro que suceda	5–Catástrofe	**Alto**
	[E.8] Difusión de software dañino	3- Es posible	5–Catástrofe	**Alto**
	[E.20] Vulnerabilidades de los programas (software)	2- Es raro que suceda	5–Catástrofe	**Alto**
[HW] Equipos Informáticos	[N.*] Desastres naturales-Terremotos	2- Es raro que suceda	5–Catástrofe	**Alto**
	[I.1] Fuego	2- Es raro que suceda	5–Catástrofe	**Alto**
	[I.3] Contaminación mecánica	3- Es posible	4–Grande	**Alto**
	[I.5] Avería de origen físico o lógico	2- Es raro que suceda	5–Catástrofe	**Alto**
	[I.6] Corte del suministro eléctrico	5- Casi seguro que sucede	4–Grande	**Muy alto**
	[E.23] Errores de mantenimiento /actualización de equipos (hardware)	2- Es raro que suceda	5–Catástrofe	**Alto**
	[E.24] Caída del sistema por agotamiento de recursos	3- Es posible	4–Grande	**Alto**
	[A.24] Denegación de servicio	3- Es posible	5–Catástrofe	**Alto**
	[A.25] Robo	4- Muy probable	4–Grande	**Alto**
[COM] Redes de Comunicaciones	[I.8] Fallo de servicios de comunicaciones	2- Es raro que suceda	5–Catástrofe	**Alto**
	[E.24] Caída del sistema por agotamiento de recursos	3- Es posible	4–Grande	**Alto**
	[A.15] Modificación deliberada de la información	2- Es raro que suceda	5–Catástrofe	**Alto**
	[A.24] Denegación de servicio	3- Es posible	4–Grande	**Alto**

[MEDIA] Soportes de Información	[I.1] Fuego	3- Es posible	5– Catástrofe	**Alto**
	[I.3] Contaminación mecánica	3- Es posible	4–Grande	**Alto**
	[I.5] Avería de origen físico o lógico	3- Es posible	4–Grande	**Alto**
	[I.10] Degradación de los soportes de almacenamiento de la información	4- Muy probable	4–Grande	**Alto**
	[E.25] Pérdida de equipos	3- Es posible	4–Grande	**Alto**
[AUX] Equipamiento Auxiliar	[N.1] Fuego	2- Es raro que suceda	5– Catástrofe	**Alto**
	[N.*] Desastres naturales-Terremotos	3- Es posible	5– Catástrofe	**Alto**
	[I.1] Fuego	3- Es posible	4–Grande	**Alto**
	[I.5] Avería de origen físico o lógico	3- Es posible	4–Grande	**Alto**
	[I.6] Corte del suministro eléctrico	5- Casi seguro que sucede	5– Catástrofe	**Muy alto**
	[E.25] Pérdida de equipos	4- Muy probable	4–Grande	**Alto**
[L] Instalaciones	[A.27] Ocupación enemiga	3- Es posible	4–Grande	**Alto**

CAPÍTULO 4

ANÁLISIS Y DISEÑO DEL PLAN DE CONTINGENCIA INFORMÁTICO

4.1 Identificar los requerimientos estratégicos para la recuperación de la plataforma de TIC

Una vez realizado el análisis de riesgo y verificando los activos de información relacionados, se puede identificar los requerimientos necesarios para la recuperación de la plataforma de TIC de la Facultad.

El DST posee un cuarto de RACK en el edificio 16C y es un rack de

mucha importancia debido a que posee el switch-router principal, desde donde se distribuye mediante fibra óptica a los demás edificios que conforman la FIEC (edificio 15A, 15), el mismo cuarto ha sido provisto de un almacenamiento eléctrico con un generador eléctrico y UPS que además brindará energía a los Laboratorios de Computación que se encuentran en ese edificio, algunos activos importantes de información se encuentran en esta área.

Entre los componentes a tomar en cuenta se detalla: la infraestructura, el personal, recursos, proveedores críticos. También se debe considerar la seguridad del personal de la información y sitios alternos de operaciones [15].

Tipos de centros de hardware de respaldo en sede alterna

Hot Side: Recuperación inmediata; el Sitio Alterno requiere de soluciones de replicación tanto a nivel de infraestructura como de datos (0- 4 horas).

WarmSide: Recuperación basada en copias de respaldo; el Sitio Alterno debe existir con conectividad, enlaces de terceros y equipos listos para restaurar las copias de respaldo (24 a 48 horas).

ColdSide: Recuperación basada en copias de respaldo; el Sitio Alterno debe existir con por lo menos la conectividad necesaria (1 semana).

A continuación mencionaré las siguientes estrategias de recuperación de TI [16]

Estrategias Propuestas a Nivel de Infraestructura

1.- Seleccionar los posibles sitios alternos para los procesos críticos de TI y que tenga los recursos mínimos que se requieran.

2.-Para el futuro considerar las necesidades de la facultad para la priorización de las aplicaciones, para definir los servidores críticos que albergarán dichas aplicaciones, todo esto para agilizar el proceso de continuidad del negocio.

3.- Asegurar que el sitio alterno tenga salida a internet que cubra con los requerimientos de las aplicaciones requeridas dentro de las primeras horas.

Estrategias Propuestas a Nivel de Personal

1.- Identificar personal primario necesario para la recuperación de los procesos críticos del DST. Adicionalmente identificar los conocimientos mínimos que debe tener este rol así como también las habilidades y competencias técnicas.

2.- Identificar personal alterno para asegurar la continuidad de las operaciones del DST, se debe identificar el personal alterno que posea características similares al personal primario. Además se debe considerar el trabajar desde casa en caso no se pueda contar con algún ambiente de trabajo.

3.- Designar un responsable del plan de contingencia, dicho responsable se encargará de la gestión de la recuperación de los elementos tecnológicos requeridos para establecer el funcionamiento en las aplicaciones que administra el DST.

4.- Gestionar un programa de capacitación sobre planes de continuidad de negocios y planes de contingencia informático, tanto al personal primario como alterno que labora en DST, con el fin de actualizar conocimientos sobre estos temas, y que ambos grupos adquieran conocimientos equitativos.

5.- Efectuar programas de capacitaciones para el personal en general que incluya prevención de emergencia en caso de eventos catastróficos, y como poder manejarlo en caso de que ocurran. Invitar autoridades externas como bomberos, defensa civil o policía nacional para que participen en las capacitaciones.

6.- Establecer un plan de capacitación anual para el área de TIC para el personal que labora en la FIEC, que considere temas técnicos y de procesos de gestión, y la recuperación de equipos e infraestructura tecnológica, con el fin de ampliar los conocimientos.

7.- Asegurar que el área del DST defina un árbol de llamadas integrado, para garantizar la comunicación efectiva entre el personal tanto interno como externo en caso de desastre.

8.- Definir un canal de comunicación entre el mismo personal que labora en DST y demás responsables de la facultad. Este canal puede ser por medios de mensajes telefónicos o tercerizando software como plataforma virtual.

Estrategias Propuestas a Nivel de Recursos

1.- Elaborar un diseño de la ubicación de los equipos de cómputo como impresoras, computadoras, etc. y de comunicaciones como switches, routers y teléfonos que estarán ubicados en el Sitio Alterno de Operaciones.

2.- Asegurar que todo el personal clave de los procesos de recuperación posean en el SAO, computadores de escritorio para el desarrollo de las actividades de recuperación a nivel de configuración, monitoreo, entre otros. Además, se debe considerar como recurso adicional: una laptop para realizar pruebas de interconectividad.

Estrategias Propuestas a Nivel de Proveedores Críticos

1.- Identificar los procedimientos actuales según normas que utiliza el estado para administrar los recursos y/o servicios tecnológicos en caso de desastres.

2.- Identificar proveedores para la reconstrucción/reparación de las instalaciones afectadas ante eventos catastróficos y establecer

contratos que contengan acuerdos de nivel de servicio antes estos eventos.

3.- Revisar los contratos (pasados y actuales) firmados con los proveedores de servicios, para asegurar que existan acuerdos de niveles de servicio (SLA) que definan penalizaciones en caso de incumplimientos, de tal manera que se pueda contar con sus servicios en caso de desastre.

Estrategias Propuestas a Nivel de Registros Vitales (Documentación)

1.- Definir políticas de control de acceso y seguridad para los registros vitales de configuración.

2.- Crear un inventario de los registros vitales, que venga acompañado de un procedimiento de manejo de cambios, en el cual se identifique claramente el responsable, las fechas y los motivos de cada actualización realizada. Además, identificar al custodio responsable de los registros vitales requeridos por cada uno de los procesos/ servicios críticos.

3.- Asegurar el correcto almacenamiento de los registros vitales en un espacio que cuente con las medidas de seguridad necesarias.

4.- Actualización periódica de registros vitales de ser necesario.

5.- Digitalización de documentos por servicio o proceso de sistemas, asegurando su validez e identificando detalles técnicos con archivos de registros vitales que contienen niveles de prioridad para su recuperación y determinar los tiempos mínimos y máximo de almacén de registros vitales.

6.- Identificar al personal afín que puede servir de apoyo en caso de contingencia.

7.- Crear roles adicionales para que personal afín pueda tener acceso a la red solo en caso de contingencia.

4.2 Seleccionar métodos alternos de respaldo y almacenamiento de datos.

Los datos importantes y configuraciones de aplicaciones críticas encontradas en la fase de análisis de riesgos son las que se deben de recuperar y tener en consideración en ciertos aspectos [17] como:

- Confiabilidad: Minimizando probabilidades de error.
- Seguridad: El almacenamiento debe ser en un lugar seguro según requerimiento y normativas actuales en cuanto a humedad, temperatura, y de la seguridad física y lógica.
- Disponibilidad: asegurar que la información almacenada es la correcta, haya sido probada y es íntegra.

Para considerar las posibles eventualidades, se detalla a continuación las posibles actividades que se deben realizar con el objetivo de

prever, mitigar o eliminar los riesgos [17]:

Tabla 8 Almacenamiento de Datos

Fuente: El autor

Actividad	Componentes	Resultado
Realizar copias de seguridad de la información que se encuentra almacenada en los discos duros de los computadores.	Documentos en formatos Word,Excel, PDF, audio y correos electrónicos.	Una copia de seguridad en la nube (opcional). Una copia de seguridad anual obligatoria de todos los documentos importantes. Responsable: Todos los funcionarios del DST.
Realizar copias de seguridad de los sistemas de información y Bases de Datos.	Aplicaciones WEB y de escritorio. Aplicaciones y Bases de Datos de los servicios y archivos de configuraciones.	Copia de seguridad semanal de los sistema de información. Responsable: Asistente Técnico de Redes, Asistente Técnico de Desarrollo, Webmaster.
Contar mínimo con un manual de instalación para restaurar los archivos del sistema operativo y aplicaciones de un computador o servidor en caso de falla física o virus informático.	Sistema operativo (Windows,Linux, etc.) Bases de datos (Sql, MySql, etc.) Drivers y utilitarios de impresoras, redes, computadoras, etc	Una copia u original del instalador en de los programas y sistemas operativos. Copias semanales de configuraciones. Responsable: Asistente Técnico de Redes, Asistente de Soporte Técnico, Asistente Técnico de Desarrollo, Webmaster.
Mantener descentralizados los sistemas de información del DST, de acuerdo a sus necesidades.	Sitios WEB, Base de Datos.	Aplicaciones instaladas en diferentes localizaciones físicas, computadores o servidores. Responsable: Webmaster, Asistente Técnico de Desarrollo.

4.3 Determinar los requerimientos del plan de contingencia informático.

Para este plan de contingencia informático del DST, es importante contar con el apoyo total del Decano de la FIEC, como máxima autoridad, así como de Gerencia de Tecnologías y Sistemas de Información, encargada de la Infraestructura total de la ESPOL, además de contar con una estructura ya definida y planes de acción en caso de que un incidente afecte parcialmente o totalmente los activos de información críticos para la facultad.

En caso de ocurrir una contingencia es muy importante que se conozca las causas del por qué se dieron y los daños que ha causado, de esta manera se podrá actuar rápidamente para restablecer el proceso o servicio dentro de un tiempo prudencial.

A continuación mencionaré los siguientes requerimientos estratégicos para el plan de contingencia:

1.- Establecer y definir el sitio alterno de operación y control.

2.- Gestionar instalaciones alternas de hardware- equipos de cómputo con sistemas más críticos.

3.- Equipamiento del SW-Router Principal de la FIEC

4.-Respaldos disponibles para restauración y documentación de aplicaciones críticas.

5.- Formación de Estructura y Equipos de Recuperación.

Seleccionar posibles Sitios Alternos de Operación y Control

Para la selección de los posibles sitios alternos de operaciones se ha tomado en cuenta la infraestructura tecnológica que actualmente posee el DST, así como los sistemas que administra, la ubicación geográfica, distancia de movilización e infraestructura física disponible por parte de FIEC, y a nivel de toda ESPOL.

La alternativa más óptima es la que nos puede ofrecer Gerencia de Tecnología y Sistemas de Información (GTySI), el cual posee un centro de cómputo muy bien equipado y que administra la parte tecnológica de toda la ESPOL, de hecho dentro de su infraestructura tecnológica podemos contar con servidores virtuales los cuales pueden representar a nuestros servidores físicos, con las debidas configuraciones y accesos de las aplicaciones críticas que posee la FIEC.

4.4 Determinar la estructura del plan

La estructura del Plan de Contingencia Informático que se propone para DST, se basa en su actual funcionamiento así como la relación que se mantiene con entidades internas como externas.

Entidades de Coordinación

Es necesario tener una adecuada comunicación con entidades

internas y externas, los mismos que ante eventos inesperados pueden colaborar y ayudarnos a solventar cualquier incidente para volver a brindar los servicios en los tiempos establecidos.

- Internas
    - Gerencia de Tecnologías y Sistemas de información
    - Personal Administrativo de la FIEC.
    - ESPOL 911 (1911-2004 (interno))
    - Inspector de Servicios Eléctricos.
- Externas
    - Emergencias (911)
    - Bomberos (911).
    - Cruz Roja (04) 256-0674
    - Policía Nacional.
    - Aseguradoras

Organización y conformación del equipo del plan de contingencias

Para la administración, desarrollo e implementación del Plan de Contingencia Informático del DST, se describe la siguiente estructura, la cual está conformada por los diferentes equipos de trabajo los cuales se detallan en la siguiente Figura 4.1.

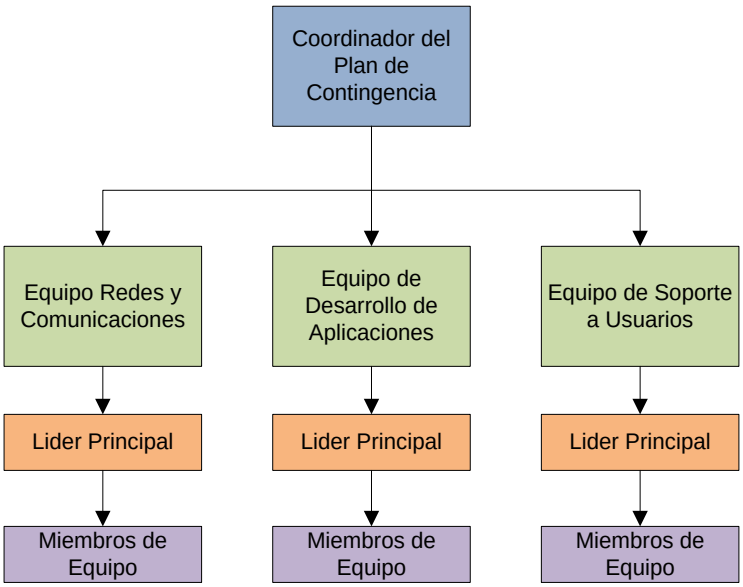


Figura 4.1 Equipo del PCI.

Fuente: El autor

Coordinador del Plan de Contingencia

El Coordinador del Plan de Contingencias Informático deberá ser formalmente designado por la Gerencia Tecnológica o en su efecto por la máxima autoridad de la facultad, a través de este coordinador se analizaran en conjunto con las autoridades toda la estructura y acciones a tomar en torno al plan de contingencia, deberá poseer las siguientes capacidades, conocimientos y responsabilidades [15]:

Capacidades / Conocimientos:

a) Liderazgo.
b) Conocimiento de la organización (FIEC) y de los procesos que se ejecutan.

c) Comunicación fluida y clara con otras áreas y departamentos de la facultad.
d) Capacidad de gestión de proyectos.

Las responsabilidades del Coordinador son:

a) Monitorear y asegurar el cumplimiento del plan.
b) Mantener copias del plan actualizadas y encargarse de que se encuentren disponibles para todos los miembros de los diferentes grupos de trabajo del plan.
c) Mantenimiento adecuado de los canales de comunicación entre los diferentes grupos de trabajo del plan.
d) Dirigir y coordinar las actividades del resto de los equipos que conforman el equipo de trabajo para la recuperación del plan de contingencia.
e) Coordinar las pruebas del plan con el fin de determinar su correcto funcionamiento y entendimiento por parte de los diferentes grupos de trabajo del plan.
f) Aportar en la mejora continua del plan de contingencia.

Coordinador del Plan de Contingencia Informático (CPCI)		
Coordinador del Plan de Contingencia Informático (CPCI)	Cargo:	Analista de Infraestructura Informática 2
	Posición:	Jefe de Laboratorios de Computación
	Fono:	2269937

Figura 4.2 CPCI

Fuente: El autor

A continuación se muestra los tres equipos establecidos para la recuperación, los cuales estarán conformados por personal que labora dentro del Departamento de Soporte Técnico.

Equipo de Redes y Comunicaciones

Este personal se encargará de las actividades de recuperación de redes y comunicaciones, debiendo reportar al CPCI sobre la interrupción del servicio y proceso de recuperación del mismo.

Las Responsabilidades de este equipo son:

1.- Elaborar y documentar las configuraciones de las redes y comunicaciones de datos, poseer el diagrama de la topología de red debidamente actualizado.

2.- Identificar y determinar el problema de la red o elementos de comunicaciones que hayan sido dañados y las posibles causas.

3.-Asegurar la disponibilidad y obtener los partes y piezas a ser remplazados de ser el caso en los equipos de comunicaciones.

4.- Coordinar, instalar y configurar el hardware y software requerido para restablecer las comunicaciones.

5.- Coordinar con el CPCI, los cambios que se deba de realizar en las comunicaciones externas de la FIEC, para que los usuarios puedan seguir usando los servicios que brindamos.

6.- Verificar el correcto funcionamiento de los elementos de comunicaciones y la conectividad en general para el restablecimiento de las mismas.

Equipo de Desarrollo de Aplicaciones

Este equipo se encarga de las acciones de recuperación de las aplicaciones y sistemas críticos de la FIEC, debiendo notificar al CPCI sobre la interrupción de los servicios y progreso de recuperación de los mismos.

Las responsabilidades de este equipo son:

1.- Identificar los procesos, bases de datos y aplicaciones que hayan sido afectados por una contingencia.

2.- Asegurar la disponibilidad de los respaldos tanto de las bases de datos, configuraciones y aplicaciones necesarias para la recuperación de los sistemas informáticos.

3.- Instalar, configurar y ajustar todo el software que haya sido afectado por una contingencia ya sea en el sitio principal como en el alterno.

4.- Restablecer el ambiente adecuado de operación de las aplicaciones que se encuentran en los servidores de la facultad.

Equipo de Soporte a Usuarios

Este equipo se encargará de identificar los equipos de cómputo que estén comprometidos luego de la contingencia además de brindar el debido soporte e instalación de equipos a los usuarios después de la misma, debiendo notificar al CPCI sobre la interrupción del servicio y progreso de recuperación del mismo.

Las responsabilidades de este equipo son:

1.- Reportar e informar de las condiciones (alarmas, sistema de parqueadero sistema de cámaras, computadoras, impresoras, etc) de los equipos informáticos que se vean afectados por una contingencia.

2.- Coordinar con los proveedores de hardware el cumplimiento de las garantías y niveles de soporte de las mismas en caso de poseerlas.

3.- Participar en las instalaciones de los sistemas operativos y demás aplicaciones en los equipos de cómputo.

4.- Verificar el correcto funcionamiento de los elementos de hardware que hayan sido reemplazados o restaurados por los proveedores.

5.- Participar en la generación de comunicaciones oficiales a usuarios internos ante contingencias, recuperación ante desastres, o demoras en el restablecimiento de servicios informáticos.

A continuación se muestra el listado de cómo está conformado los equipos de recuperación. Cabe indicar que solo se muestra los roles de los mismos.

Tabla 9 Listado de Integrantes de los Equipos de Recuperación

Fuente: El autor

Listado de Integrantes de los Equipos		
Equipos de Redes y Comunicaciones		
Rol	**Servicios**	**Responsable**
Líder/Ejecutor	Monitorear el estado de la Red y servidores de la FIEC	Cargo: Asistente Técnico de Redes
	Administrador de Servidores de la Facultad	Fono: 2269941
Miembro del Equipo/ Ejecutor	Monitorear el estado de la Red y servidores de la FIEC	Cargo: Asistente Técnico de Soporte
	Configuración de hardware y software a utilizar en los sistemas	Fono: 2269941
Equipo de Desarrollo de Aplicaciones		
Rol	**Servicios**	**Responsable**
Líder/Ejecutor	Desarrollar, Administrar y monitorear sistemas de la Facultad	Cargo: Asistente Técnico de Desarrollo
	Documentar los cambios realizados en los sistemas	Fono: 2269941
Miembro del Equipo/ Ejecutor	Realizar mantenimiento al sitio web de la FIEC	Cargo: Webmaster
	Documentar los cambios realizados en el sitio web	Fono: 2269941
Equipo de Soporte a Usuarios		
Rol	**Servicios**	**Responsable**
Líder/Ejecutor	Configuración e instalación de equipos de computación	Cargo: Asistente Técnico de Soporte
	Actualizaciones de paquetes de programas, sistemas operativos	Fono: 2269941
Miembro del Equipo/ Ejecutor	Mantenimiento Prevento y correctivo equipos de cómputo	Cargo: Asistente Técnico de Soporte
	Mantener inventario actualizado equipos de computación	Fono: 2269941

4.5 Diseñar el plan de contingencia informático

Para el diseño del plan de contingencia informático es importante establecer los pasos necesarios que permitan minimizar o evitar la

ocurrencia de eventos o incidentes que paralicen parcial o totalmente los servicios críticos que componen los sistemas de información, los cuales son fundamentales para la FIEC, se establece este plan con la finalidad de restablecer los servicios ante los riesgos que a continuación se detallan:

Seguridad [N] Desastres Naturales

Riesgo: [N*.] Desastres Naturales - Terremotos

Activos que afecta: [HW] Equipos Informáticos, [AUX] Equipamiento Auxiliar.

Medidas Organizativas:

- Establecer un plan de evacuación del hardware más importante de acuerdo a las funciones que desempeña dentro del departamento, corresponde a los activos de información que se desean preservar.
- Identificar las áreas más vulnerables del puesto de trabajo que puedan generar riesgo para la integridad física de producirse un incendio, terremoto o inundación, tal como mobiliario que no se encuentre anclado, mamparas, espejos, almacenamiento de materiales en altura, etc.
- Difundir entre docentes, alumnos y personal administrativo, los puntos de encuentro, vías de evacuación y zonas seguras

dentro de la facultad.

- Realizar, mantener y difundir junto con la Unidad de Seguridad y Salud ocupacional el procedimiento pertinente en caso de terremoto o sismo que afecte tanto al Departamento de Soporte Técnico como a toda la ESPOL.

Medidas Técnicas:

- Habilitar los equipos (servidores) dentro del SAO para empezar proceso de recuperación de servicios críticos.

Medidas Humanas:

- Formación del personal para actuar en caso de terremoto o sismo.

Riesgo: [N.1] Fuego

Activos que afecta: [AUX] Equipamiento Auxiliar.

Medida Organizativas:

- Dado que la FIEC y por ende toda la ESPOL, se encuentra dentro de un área verde, es muy posible la prosperación de un incendio forestal, en especial, en verano, por tal motivo se deben difundir las respectivas medidas de seguridad en caso de incendio.
- Si observa un incendio forestal o una columna de humo dentro del monte, es importante avisar lo más rápidamente posible a

alguno de los servicios de emergencia más próximos, como Servicios Forestales, Bomberos, Policía.

- Todo el mundo debe conocer en todo momento rutas de escape. Deben llegar a alguna zona segura en la que se puedan albergar ante una situación comprometida.

Medidas Humanas:

- Mantener una adecuada formación del personal para actuar en caso de incendios forestales.

Seguridad [I] De origen industrial

Riesgo: [I.1] Fuego

Activos que afecta: [HW] Equipos Informáticos, [AUX] Equipamiento Auxiliar, [Media] Soportes de Información

Medidas Técnicas

- DST debe contar con un sistema de incendio tipo C de activación manual, debiendo realizarse inspecciones semestrales de la presión de carga adecuados y deben recargarse mínimo cada 12 meses cuando no han sido utilizados. Deben constar con la etiqueta de registro de carga y fecha de vencimiento.
- Los cuartos de rack, laboratorios de computación, deben contar con un sistema de alarmas, sistema de detección de fuego y extintores.

- La utilización de equipos como: archivadores, racks y sistemas de bandejas de cable deben ser de material ignifugo (proteja contra el fuego), evitando así daños mayores a los activos de información.
- Considerar un plan de mantenimiento eléctrico al menos una vez al año, para detectar e impedir posibles cortocircuitos o sobrecargas eléctricas.

Medidas Organizativas:

- Establecer señalética adecuada basada en políticas de seguridad industrial referentes a la prohibición de fumar en lugares cerrados o cuartos de rack.
- Mantener un stock de repuestos de equipos informáticos para que sean utilizados en el sitio alterno para poder operar de ser el caso.
- Contar con un manual de procedimientos de respaldos de todos los sistemas informáticos críticos de la FIEC.
- Se debe capacitar al personal que labora tanto en el DST como en toda la FIEC sobre el uso y manejo de los extintores mínimo una vez al año.

Medidas Humanas:

- El personal de la organización debe ser capacitado, para el uso adecuado de los equipos de protección contra incendio (utilización de extintores, mascarillas, tanques de oxígeno, etc.).
- Debe establecerse los roles y responsabilidades en la administración de respaldos de información (Bases de datos, configuraciones, etc.).

Riesgo: [I.3] Contaminación mecánica

Activos que afecta: [MEDIA] Soportes de Información, [HW] Equipos Informáticos

Medidas técnicas:

- El responsable de la administración de servidores e infraestructura de la facultad, debe monitorear las condiciones físicas y medioambientales de forma continua en los equipos dentro del cuarto de rack, en caso de alertas físicas dentro de los mismos, así como de revisar mensajes configurados enviados a su mail en caso de interrupciones en el equipo.
- Realizar la planeación del mantenimiento físico respectivo de los equipos que se encuentran dentro del cuarto de rack (cuarto de servidores)
- El cuarto de rack (cuarto de servidores) y los laboratorios de computación deben estar climatizados y mantener los niveles

de temperatura y humedad dentro de los límites requeridos para la infraestructura instalada.

Medidas Organizativas:

- Controlar los filtros de aire de aires acondicionados, los mismos que deben tener un mantenimiento de limpieza o cambio en caso de deterioro, ya que pueden llegar a dañarse.
- Establecer un plan de mantenimiento con respecto a los muros, pisos y paredes así como el aspirado del polvo dentro del cuarto de rack.
- Establecer plan de mantenimiento semestral de equipos de cómputo de los laboratorios de la FIEC, así como de los equipos de comunicaciones ubicados en los cuartos de rack.

Medidas Humanas:

- En caso de que el mismo personal del DST tenga que realizar el mantenimiento físico de equipos informáticos, debe de contar con todos los implementos necesarios de seguridad física para que la salud del personal no se vea perjudicada.

Riesgo: [I.5] Avería de origen físico o lógico.

Activos que afecta: [SW] Software - Aplicaciones Informáticas, [HW] Equipos Informáticos, [AUX] Equipamiento Auxiliar, [Media]

Soportes de Información

Medidas Técnicas:

- Entre las especificaciones de los equipos de comunicaciones, detallar la necesidad de adquirirlos con redundancia es decir, doble fuente de poder, doble ventiladores de enfriamiento, etc.
- Verificar en los contratos de adquisición de equipos informáticos el tiempo de garantía, y que no más cubren las mismas ante desperfectos de fábrica.
- Mantener un adecuado respaldo de las configuraciones de los equipos de comunicaciones e informáticos (servidores críticos).

Medidas Organizativas:

- Establecer políticas de uso adecuado de los equipos informáticos (hardware), que impidan el deterioro de los mismos, en caso de cumplir su tiempo de vida es necesario gestionar su posible reemplazo.
- Establecer un plan de mantenimiento tanto preventivo como correctivo de los equipos de comunicaciones y de cómputo mínimo de 6 meses o cada año.
- Verificar la vigencia de las garantías técnicas de 1 a 3 años de equipos informáticos y de comunicaciones contra daño y deterioro, o desperfectos por parte del fabricante.
- Mantener un stock de repuestos que permita minimizar los

tiempos de inoperatividad de las comunicaciones, así como piezas a reemplazar para equipos de cómputo.

Medidas Humanas:

- Mantener una adecuada formación y capacitación del personal de tal manera, poder interactuar con los equipos cuando sea necesario su mantenimiento en caso de remplazo de piezas o partes y restauración de configuraciones de los mismos.

Riesgo: [I.6] Corte del suministro eléctrico

Activos que afecta: [HW] Equipos Informáticos, [AUX] Equipamiento Auxiliar

Medidas Técnicas:

- El edificio tiene conexión hacia un cuarto de generador eléctrico que alimentan a los sistemas UPS que protegen a los equipos de sobrecargas eléctricas y apagones. Siendo de esta manera protegida las tomas dentro del cuarto de rack (cuarto de servidores) y una parte de los Laboratorios de Computación. Se ha establecido un generador eléctrico en los edificios 15A, 16C, 16AB.
- Evitar la puesta de cables de conexión entre equipos y tomas de corriente eléctrica sobre piso falso.

- Identificación de tomas de corriente exclusivas para los activos dentro del cuarto de rack del 16C así como de los laboratorios del DST.
- Verificar cada semestre el funcionamiento adecuado del Suministro de Energía Ininterrumpible (UPS) en los diferentes laboratorios y cuartos de rack de la FIEC así como los supresores de voltaje que alimentan los diferentes activos que administra el DST.

Medidas Organizativas:

- Verificar que se cumpla el plan de mantenimiento preventivo y correctivo del generador de emergencia y UPS, para garantizar su efectiva operación continua.
- Contar con un manual de procedimiento de operación y puesta en marcha del generador de emergencia eléctrico.

Medidas Humanas:

- Facilitar capacitación referente a la operación y funcionamiento general del generador de emergencia eléctrico en casos de pruebas y operación en producción.

Riesgo: [I.8] Fallo de servicios de comunicaciones

Activos que afecta: [COM] Redes de Comunicaciones

Medidas Técnicas:

- Evitar cables de conexión entre equipos y tomas de corriente eléctrica sobre piso falso en cuartos de rack o comunicaciones, que provoque desconexión accidental de los equipos.
- El DST debe cumplir los procedimientos de seguridad física y control de acceso que aseguren el perímetro de la instalación de los equipos de red y servidores.
- Aplicación de actualizaciones y parches sobre equipos de comunicaciones en ambiente controlado.

Medidas Organizativas:

- Los armarios y racks físicos de acceso a los equipos de información del área de comunicaciones deben siempre estar protegidos con cerraduras o llaves o un sistema de control de acceso que permita el acceso única y exclusivamente al personal autorizado.

Medidas Humanas:

- Mantener una adecuada formación y capacitación del personal de tal manera de evitar acciones accidentales sobre los equipos y configuraciones por exceso de confianza.

Riesgo: [I.10] Degradación de los soportes de almacenamiento de la información

Activos que afecta: [MEDIA] Soportes de Información

Medidas Técnicas:

- Personal del DST, debe asegurarse que los medios de almacenamiento (cintas magnéticas, discos duros) se encuentren en óptimas condiciones para el respaldo de información asegurando de esta manera la integridad de la misma.
- Verificar correcto funcionamiento del equipo que realiza el respaldo de información, en este caso de las cintas magnéticas.
- Los medios de almacenamiento tales como cintas magnéticas, discos duros de respaldo, etc. deben estar ubicados en lugares seguros para evitar que sufran daños ambientales.

Medidas Organizativas:

- El DST, debe tener definido un procedimiento de respaldo de la información, con el fin preservar la integridad y disponibilidad de los mismos.

Medidas Humanas:

- Personal responsable del DST, debe realizar las copias de seguridad, y según el caso, debe transportarlas al lugar seguro.

Seguridad [E] Errores y fallos no intencionados

Riesgo: [E.2] Errores del administrador

Activos que afecta: [D] Datos

Medidas Técnicas:

- El personal del DST, deberá probar que las copias de respaldo que se han realizado, funcionan correctamente, para comprobar la integridad de la información almacenada.
- Un plan de backups debidamente probado y listo para poner en marcha en caso de problemas de administración y configuración.
- El DST, realizará un monitoreo continuamente de la red, servicios, sistemas y demás recursos informáticos, con el objetivo de asegurar que la infraestructura tecnológica funcione correctamente.
- Los servidores deberán generar logs de los sistemas y servicios que alojen, los mismos que deberán ser monitoreados periódicamente para evitar que afecte la disponibilidad e integridad de los mismos.

Medidas Organizativas:

- El personal del DST debe contar con una manual de configuraciones de los servidores que administra dentro de la facultad.

- El personal del DST, debe tener definido un manual de procedimiento o políticas de respaldo de la información y datos críticos, con el fin preservar la integridad y disponibilidad de la misma.
- Llevar una bitácora de los incidentes más comunes que se han presentado y soluciones específicas a los mismos.

Medidas Humanas:

- Realizar capacitaciones continuas del personal del DST en el área de TI y seguridad de la información, para de esta manera proveer de una adecuada instalación y configuración de los equipos informáticos.

Riesgo: [E.8] Difusión de Software Dañino

Activos que afecta: [SW] Software - Aplicaciones Informáticas

Medidas Técnicas:

- Mantener actualiza la base de datos del antivirus empresarial que se esté utilizando en la ESPOL y en todas las facultades, a fin de protegerse de ataques de virus informáticos.
- La versión actual de antivirus se encuentre en todos los servidores que albergan las aplicaciones que se usan en la facultad, en caso de ser Servidores con Linux tener las debidas medidas de seguridad de acuerdo a políticas establecidas o

mediante listas de acceso.

Medidas Organizativas:

- Llevar una bitácora de los incidentes más comunes que se han presentado y soluciones específicas a los mismos.

Medidas Humanas:

- Realizar capacitaciones continuas del personal del DST en el área de TI y seguridad de la información, para de esta manera proveer de una adecuada instalación y configuración de los equipos informáticos.

Riesgo: [E.20] Vulnerabilidades de los programas (software)

Activos que afecta: [SW] Software - Aplicaciones Informáticas

Medidas Técnicas

- El responsable de administrar los servidores debe estar al tanto de parches de seguridad para instalar en los servidores que albergan las aplicaciones que se utilizan en la facultad, adicionalmente, reportar en caso de encontrar bugs en los sistemas y a su vez realizar el respectivo correctivo.
- Realizar el respectivo hardening de los sistemas nuevos por instalar en los servidores y/o equipos que posea la facultad.

Medidas Organizativas

- El DST debe contar con una manual de configuraciones o

políticas de seguridad de los servidores que administra dentro de la facultad.

Medidas Humanas:

- Realizar capacitaciones continuas del personal del DST en el área de TI y seguridad de la información, para de esta manera proveer de una adecuada instalación y configuración de los equipos informáticos.

Riesgo: [E.23] Errores de mantenimiento / actualización de equipos (hardware)

Activos que afecta: [HW] Equipos Informáticos

Medidas Técnicas

- El personal del DST debe realizar mantenimientos preventivos y correctivos de los equipos informáticos de la FIEC para asegurar su disponibilidad e integridad, teniendo en cuenta lo siguiente: se realizarán 2 mantenimientos preventivos en el año en lo que refiere a los Laboratorios de computación de la FIEC. Se realizará 1 mantenimiento preventivo en el año en los cuartos de rack (cuarto de servidores).

Medidas Organizativas:

- El personal del DST, registrarán las fallas supuestas o reales y además llevará un registro de instalación y un registro de la planificación y ejecución del mantenimiento preventivo y

correctivo realizado.

Riesgo: [E.24] Caída del sistema por agotamiento de recursos

Activos que afecta: [S] Servicios, [HW] Equipos Informáticos, [COM] Redes de Comunicaciones

Medidas Técnicas:

- El personal del DST debe estar constantemente monitoreando los equipos informáticos (servidores, equipos de comunicaciones) en caso de fallas físicas o lógicas que perjudiquen el acceso a las aplicaciones que más se utilizan.
- Realizar el Plan de mantenimiento de los equipos de comunicaciones mínimo de 6 meses o cada año.
- Mantener un adecuado respaldo de las configuraciones de los equipos de comunicaciones e informáticos (Servidores críticos).

Medidas Organizativas:

- El personal del DST, registrarán las fallas supuestas o reales y además llevará un registro de instalación y un registro de la planificación y ejecución del mantenimiento preventivo y correctivo realizado.

Medidas Humanas:

- Realizar capacitaciones continuas del personal del DST en el área de TI y seguridad de la información, para de esta manera

proveer de una adecuada instalación y configuración de los equipos informáticos.

Riesgo: [E.25] Pérdida de equipos

Activos que afecta: [Media] Soportes de Información, [AUX] Equipamiento Auxiliar

Medidas Técnicas:

- Los cuartos de rack (cuarto de servidores) deben contar con mecanismos de control de acceso tales como puertas de seguridad, cerradura, sistemas de control de acceso con tarjetas, sistema de alarmas o controles biométricos.

Medidas Organizativas:

- El ingreso de terceros a los cuartos de racks (cuarto de servidores), debe estar debidamente registrado mediante una bitácora ubicada en la entrada de estos lugares de forma visible.

Medidas Humanas:

- Las solicitudes de acceso al cuarto de racks (cuarto de servidores) o a los centros de cableado deben ser notificadas al Jefe del DST para autorizar el acceso y que al menos una persona del DST esté presente durante la visita en los lugares señalados anteriormente.

Seguridad [A] Ataques intencionados

Riesgo: [A.6] Abuso de privilegios de acceso

Activos que afecta: [S] Servicios

Medidas Técnicas:

- Los usuarios de los recursos informáticos y de los sistemas que administra el DST, deberán usarlo adecuadamente de forma responsable, salvaguardando la información a la cual se les ha permitido acceder.
- El DST restringe el acceso a recursos informáticos y sistemas, de acuerdo con el grupo de usuario al que pertenece, necesidad de uso y/o bajo autorización de máxima autoridad o jefe inmediato.
- El DST es responsable de la administración de los sistemas informáticos, por lo tanto velará para que estos sean debidamente protegidos contra accesos no autorizados a través de mecanismos de control de acceso lógico. Además, velará que los desarrolladores, se acojan a buenas prácticas de desarrollo en lo que corresponde al acceso lógico y evitar accesos no autorizados a los sistemas administrados.

Medidas Organizativas:

- Las funciones, roles y responsabilidades del personal del DST deben estar documentadas y apropiadamente segregadas.
- El DST debe contar con un manual de procedimiento para documentar los roles y accesos otorgados al personal

administrativo o docente que accede a las aplicaciones que administra el DST.

Medidas Humanas:

- Los usuarios de los recursos informáticos, servicios de red y los sistemas que administra el DST deben hacerse responsables de las acciones realizadas sobre estos, así como el uso del usuario y contraseña asignados para el acceso de los mismos.

Riesgo: [A.15] Modificación deliberada de la información

Activos que afecta: [COM] Redes de Comunicaciones

Medidas Técnicas:

- El DST deberá asignar derechos de acceso a recursos informáticos, a los usuarios que lo soliciten, previa autorización del Jefe inmediato o máxima autoridad.
- Acceso autorizado a las claves y configuraciones al personal encargado de administrar los equipos de comunicaciones.

Medidas Organizativas:

- El DST debe cumplir las políticas y/o procedimientos de seguridad física y control de acceso que aseguren el perímetro de las instalaciones de los equipos de red y servidores.

Medidas Humanas:

- Capacitar al personal en el área de TI y seguridad de la información para evitar modificaciones accidentales de la data

y configuraciones sobre los equipos informáticos y de comunicación.

Riesgo: [A.18] Destrucción de información

Activos que afecta: [D] Datos

Medidas Técnicas:

- El DST deberá asignar derechos de acceso a recursos informáticos, a los usuarios que lo soliciten, previa autorización del Jefe inmediato o máxima autoridad.
- Los sistemas deberán generar logs de actividades de los usuarios y administradores, los mismos que deberán ser monitoreados en el caso de ocurrir algún evento que afecte los mismos.

Medidas Organizativas

- Establecer política de control de acceso para disminuir baches de seguridad que se pueden producir por el abuso de privilegios de acceso y por accesos no autorizados a fin de proteger la integridad y disponibilidad de la información.
- El DST, debe tener definido un procedimiento de respaldo de la información, con el fin preservar la integridad y disponibilidad de los mismos.

Medidas Humanas:

- El usuario es responsable del acceso que le ha proporcionado, es decir posee un usuario y contraseña, que le permite acceder a los recursos informáticos que administra el DST, por lo cual deberá mantenerlo de forma confidencial.

Riesgo: [A.24] Denegación de servicio

Activos que afecta: [HW] Equipos Informáticos, [COM] Redes de Comunicaciones

Medidas Técnicas:

- Los cuartos de racks (cuarto de servidores) deben contar con mecanismos de control de acceso tales como puertas de seguridad, cerradura, sistemas de control de acceso con tarjetas, sistema de alarmas o controles biométricos.
- Los equipos deben mantenerse ubicados en un buen lugar, aislándolo de amenazas como fuego, agua, vibración, polvo, interferencia electromagnética y vandalismo, etc.
- Monitorear los equipos informáticos, a fin de revisar si los recursos que posee son suficientes, o necesitan ser reemplazados.

Medidas Organizativas:

- Establecer política de control de acceso para disminuir los inconvenientes de seguridad que se pueden producir por el abuso de privilegios de acceso y por accesos no autorizados.

Medidas Humanas:

- El personal del DST es responsable de la administración de los recursos que utilizan los equipos informáticos para establecer su normal funcionamiento.

Riesgo: [A.25] Robo

Activos que afecta: [HW] Equipos Informáticos

Medidas Técnicas:

- El DST debe tener los activos importantes identificados por lo que se debe elaborar y mantener un inventario de los mismos.
- Verificar constantemente mediante inventarios los activos de información distribuidos entre los diferentes laboratorios de la facultad, así como oficinas de docentes, personal administrativo y aulas.
- El DST debe monitorear periódicamente la validez de los usuarios (propietarios/responsables) y sus perfiles de acceso a los activos de información.
- Instalación de nuevas cámaras de seguridad en Cuartos de Racks y en los diferentes laboratorios que no posean estos equipos que se encuentran ubicados en toda la FIEC.

Medidas Organizativas:

- Las respectivas actas de entrega/recepción de los activos que deben estar asociados a una persona responsable, quien hace uso del mismo.
- En caso de pérdida o robo de un equipo informático, se debe reportar al DST para que a su vez se informe al Custodio de los Activos y a la máxima autoridad de la facultad para que se inicie el trámite interno y se ponga la denuncia ante la autoridad competente.

Medidas Humanas:

- Los usuarios finales son los responsables del cuidado y mantenimiento de los activos a ellos asignados como custodios internos de los mismos.

Riesgo: [A.27] Ocupación enemiga

Activos que afecta: [L] Instalaciones

Medidas Organizativas:

- Tanto el personal que labora en el DST como en la FIEC, debe ocupar un área (espacio) u oficina donde desempeñará sus actividades.
- La máxima autoridad de la facultad, debe asignar un espacio disponible con todos los equipos necesarios para desempeñar sus funciones.

Medidas Humanas:

- El personal administrativo y docentes de la facultad son responsables del cuidado y mantenimiento de los equipos asignados para su gestión.

4.6 Definir y Documentar los procedimientos de recuperación

Considerando la plataforma tecnológica de TI que actualmente posee la FIEC, y conociendo la importancia de poseer la documentación necesaria cuando exista un evento que afecte parcialmente o totalmente el funcionamiento de los aplicativos de la facultad, se define los siguientes documentos de recuperación en el Anexo G:

1.- Documentación por Indisponibilidad por Desastre Natural.

2.- Documentación por Indisponibilidad por Suministro Eléctrico.

En estos documentos se debe detallar toda la información pertinente con el fin de recuperar todos los activos de información de los servicios críticos de la FIEC.

El responsable de cada equipo de recuperación es el encargado de elaborar y mantener esta documentación actualizada tomando en consideración el peor escenario posible.

En la Figura 4.3 podemos observar mediante el siguiente diagrama de flujo procedimiento para recuperación establecido para el DST.

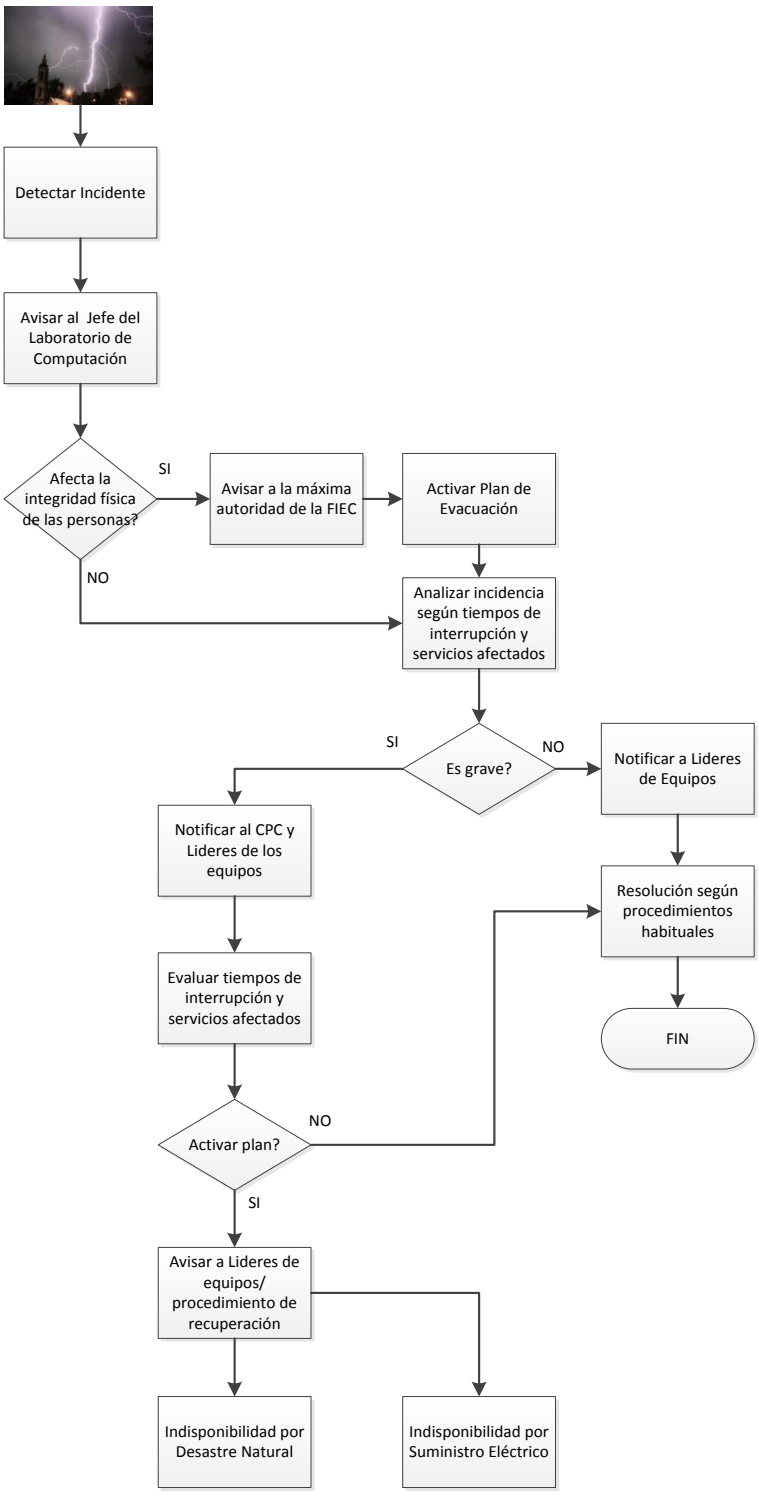


Figura 4.3 Diagrama de Procedimiento de Recuperación

Fuente: El autor

4.7 Determinar los documentos requeridos a utilizar durante y después del desastre

Para seguir con el procedimiento de recuperación ante incidentes, se debe definir los documentos a utilizarse durante y después del desastre. A continuación los detallo:

Durante:

- La Lista del Equipo del Plan de Contingencia Informático por personal del DST.

  Se utilizará este formulario (Anexo E) para obtener información del personal que integra el plan, los mismo que pertenecen a los diferentes equipos de recuperación, de esta manera se podrá localizarlos con mayor facilidad en caso de tener una contingencia [16].

- Información de contactos externos.

  Se utilizará esta lista de información de contactos externos (Anexo F) para registrar los datos de las entidades como la Policía, Bomberos, Proveedores de servicios externos, etc., los mismos que podrán ayudar en caso de requerir su colaboración ya sea de manera directa o con la entrega de equipos o repuestos [16].

- Procedimientos de recuperación

Estos procedimientos de recuperación (Anexo G) establecidos anteriormente se utilizarán cuando se haya activado el plan, esto permitirá a los equipos actuar de manera adecuada para recuperar procesos y servicios críticos [16].

- Lista de Sistemas de Información de Activos

  Se utilizará la documentación [17] (Anexo H) previamente realizada y actualizada de los sistemas críticos del DST, así como requerimientos para la recuperación de su funcionamiento.

- Lista de Control de BACKUPS

  Se muestra el control de los procedimientos [17] (Anexo I) de respaldos diarios que se realizan en los sistemas críticos y el responsable del mismo.

Después:

- Libro de Registro de Contingencias.

  Se utilizará este formulario (Anexo J) para realizar el seguimiento del estado de la contingencia, lo que servirá al CPCI para poder comunicar y brindar información del estado y desarrollo de recuperación de la contingencia [17].

- Evaluar el estado del Activo.

  Se utilizará este formulario (Anexo K) para realizar una evaluación de daños ocasionados por la contingencia, de esta

manera se podrá definir qué acciones tomar sobre dicho activo, ya sea para su reparación o el reemplazo del mismo [16].

- Lista de verificación plan de contingencia.

  Se utilizará este documento [17] (Anexo L) para verificar si los pasos descritos para el plan de contingencia fueron de ayuda al momento de ocurrir la contingencia, o por el contrario se necesita realizar otra revisión para poder corregirlo.

- Evaluación de Resultados después de la Contingencia.

  Se utilizará este formulario [16] (Anexo M) para realizar una evaluación de las acciones que se tomaron después de la contingencia y permitirá obtener una retroalimentación de todo el proceso a fin de conocer en que se ha fallado y como mejorarlo.

CAPÍTULO 5

IMPLEMENTACIÓN DEL PLAN DE CONTINGENCIA INFORMÁTICO

5.1 Antecedentes

Como una parte importante en la mejora continua del plan de contingencia y su efectiva aplicación, se debe definir y proponer pruebas periódicas, como un conjunto de medidas para validar la constante aplicabilidad del plan, poder planear, realizar y documentar los procedimientos que son necesarios ejecutarse para realizar estas

pruebas será de mucha utilidad para validar el diseño del mismo.

El siguiente plan debe ser probado periódicamente en virtud de:

- La ejecución de las pruebas servirá para validar la validez del plan y cuan confiable es, así como para encontrar mejoras que ayuden a que el plan siempre este actualizado.
- La estructura de la facultad y relación con la tecnología podría ocasionar que el plan con el pasar del tiempo quede obsoleto.
- Las pruebas se realizan cuando existen actualizaciones, adquisiciones o modificaciones en el hardware, software, o en cualquier tipo de aplicativos, e infraestructura y también si existen cambios en los procesos del negocio.
- La realización de pruebas de contingencia permiten la posibilidad de evaluar responde la organización ante un determinado desastre o evento desafortunado.
- Las pruebas deben ejecutarse ante eventos muy similares y que puedan ocurrir en la realidad, deben asemejarse loa más posible a la realidad de nuestro país, las mismas que deben ser planificadas de tal manera que no afecte las actividades normales de la organización o su riesgo sea mínimo.
- El responsable de las pruebas del plan de contingencia será el CPCI quién debe gestionar el cumplimiento y actualización del mismo, así como evaluar y realizar el mantenimiento de la

misma.

5.2 Pruebas y Verificación

Simulacro para verificar el Plan de Contingencia

1.- Se inicia el procedimiento de recuperación del plan de contingencia.

2.- Planificar el Simulacro del Plan de Contingencia:

- Se debe realizar la planificación anual del simulacro de recuperación de los sistemas de información.
- Actualización de los planes de prevención y recuperación de sistemas (Indisponibilidad por desastre natural- terremotos, por suministro eléctrico, etc.).
- Capacitación sobre los diferentes procedimientos de prevención y recuperación de los sistemas de información.
- Verificación de disponibilidad de manuales técnicos actualizados para los sistemas de información.
- Verificar la disponibilidad de los recursos informáticos para habilitar los sistemas de información más críticos que se utilizan en la facultad.

3.- Preparar recursos informáticos para el simulacro.

- Disponibilidad de recursos para solventar contingencias tales como: manuales de instalación de los sistemas de

información e instalación de equipos críticos, respaldo de bases de datos, equipos de suministro eléctrico, equipos de comunicaciones.

- Disposición de equipos de cómputo (servidor o computadora) con las características técnicas para la recuperación e instalación del sistema de información.
- Verificar disponibilidad de recursos necesarios con los proveedores en caso de requerirse.

4.- Ejecutar el simulacro del plan de contingencia

- Se ejecuta el procedimiento de recuperación, de acuerdo a cada una de las contingencias: desastre naturales (como terremotos o incendios, etc), o suministro eléctrico.
- En este paso se busca asegurar la continuidad de las aplicaciones críticas de la facultad.

5.- Realizar pruebas

- Se realizan las pruebas del plan de contingencia, correspondientes para valorar el impacto real del mismo ante una posible eventualidad.
- En caso de que los resultados obtenidos sean diferentes de los esperados, se debe verificarlos, e iniciar nuevamente la prueba.
- Una vez finalizada la prueba, se elabora un acta que contenga los resultados de su ejecución, los mismos que servirán para

sacar las conclusiones respectivas sobre las mejoras del plan de contingencia.

Desde la perspectiva de continuidad del negocio el ejercicio se focaliza esencialmente en el personal, en donde se evalúa características especiales como comportamiento de los involucrados, conocimiento de la estructura de recuperación, conocimiento de los estados de la gestión de crisis y de las actividades del Plan de Contingencia Informático (PCI), así como la familiaridad con el supuesto ambiente alterno o estrategia alterna establecida, protocolo para las notificaciones efectivas, entre otros.

El Ejercicio de Escritorio, consiste en realizar un ejercicio en un ambiente “sin estrés”, y para ello cada representante de los equipos de recuperación se sienta alrededor de una mesa de trabajo, y sigue exclusivamente las actividades tal y como están descritas en el rol que representa en sus respectivos equipos según el plan, no se improvisa. Además cualquier necesidad no documentada debe anotarse como una mejora al plan, es útil para validar el uso del documento o plan por parte del personal, para validar incoherencias entre actividades de los diferentes roles y para que el personal se familiarice con la estructura del mismo, sobre todo los miembros suplentes a quienes se recomienda hacer participar de este tipo de ejercicios [16].

Ejecución del Ejercicio de Escritorio

Objetivo del Ejercicio de Escritorio:

- Lograr que las áreas involucradas se familiaricen con la estructura del PCI, reconocer los roles involucrados (antes, durante, después) y sus actividades.
- Ejecutar las acciones de coordinación entre el Líder del Plan y los miembros de recuperación identificados.
- Validar las secciones complementarias del Plan de Continuidad (colaboradores, proveedores, documentos, entre otros).
- Reconocer el Sitio Alterno de Operaciones y los recursos asociados para la recuperación.
- Verificar el correcto funcionamiento del plan de contingencia asociado a este ejercicio, en este caso se utilizará para el simulacro: un daño completo del servidor principal del ControlPC que se encuentra ubicado en el edificio 16C en la FIEC a causa de un incendio.
- Actualizar de acuerdo a requerimientos del simulacro las mejoras y cambios en el plan de contingencia

Escenario y premisas del ejercicio

Para la ejecución del ejercicio se definió como escenario un incendio, que terminó afectando físicamente al servidor principal del ControlPC. El Ejercicio que se está estableciendo corresponde al uso de un

programa de mucha utilidad en los laboratorios de computación de toda la facultad, y también en otras facultades.

El control PC es el programa encargado de controlar el uso de los laboratorios de la FIEC, mediante el uso de un usuario y contraseña asignado por el administrador de redes de la FIEC, el estudiante podrá hacer uso de los laboratorios y el software instalado en las computadoras del mismo. Solo necesita ingresar con sus credenciales en la pcs de los laboratorios.

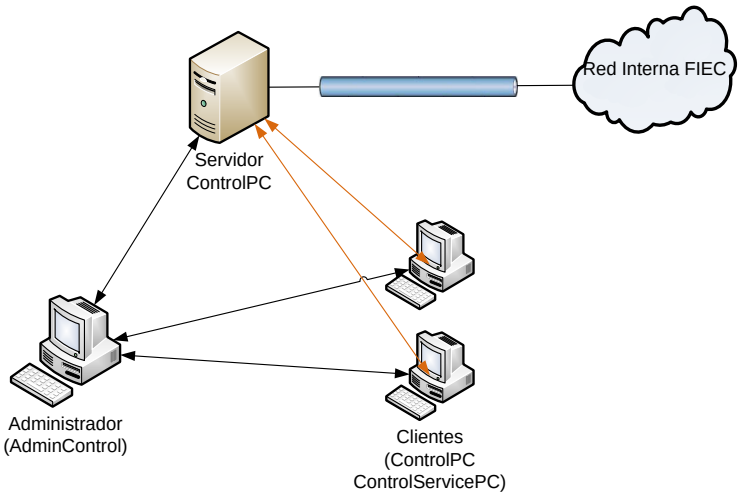


Figura 5.1 Diagrama del ControlPC

Fuente: El autor

Premisas del Ejercicio

1.- El incendió ocurrió a las 10:00 a.m. de un día laborable.

2.- Después de ocurrido el incidente, el Plan de Contingencia Informático fue ejecutado exitosamente en el edificio afectado (los

colaboradores que hubieran podido estar dentro al momento del incidente fueron evacuados sin contratiempos).

3.- Se procede a activar el plan de contingencia, el personal distribuido en los diferentes equipos de recuperación están pendientes de la activación del plan, y del traslado al Sitio Alterno de Operaciones, en donde se procederá a establecer el servicio necesario.

4.- El rol del CPCI, será asumido por el Analista de Infraestructura Informática, la misma persona que debe organizar que todos los recursos necesarios y los equipos estén listos en el SAO.

5.- Las redes de telecomunicaciones deben estar operativas lo más pronto posible en el Sitio Alterno ya que no fueron afectadas por el incidente.

6.- El SAO cuenta con computadores, registros vitales habilitados, recursos de oficina y material de operación; los cuales fueron requeridos por cada área del equipo de recuperación.

7.- El SAO cuenta con los servicios básicos; conectividad, luz, aire acondicionado, alimentos, agua.

8.-Los procedimientos de operación alternos están documentados y listos.

9.-No hubo pérdidas humanas fatales que lamentar.

Planificación de las actividades de logística

Como parte de la planificación se identifica a los participantes del equipo de recuperación de cada área involucrada en el Ejercicio de Escritorio, con los líderes y/o miembros suplentes involucrados en el PCI, quienes deben ser convocados para el desarrollo del ejercicio; se debe realizar una presentación de inducción al ejercicio de escritorio, en donde se logre definir el objetivo, alcance, premisas, escenario del evento y los supuestos del ejercicios.

Como materiales de apoyo para la ejecución del Ejercicio de Escritorio se debe considerar:

- Plan de Contingencia Informático impreso, los cuales deben ser entregados a todos los participantes de cada área.
- Etiquetas para la identificación de cada rol, para identificar, en la mesa de trabajo, a los participantes y a los roles que estarían asumiendo en el momento del ejercicio.
- Definir formatos de “Oportunidades de Mejora”, para poder registrar los comentarios y mejoras que cada involucrado activamente identifique dentro de sus propios roles de recuperación.
- Definir formatos de “Lista de Requerimientos” y “Árbol de Llamadas”, los cuales sirven para mantener documentada las distintas interacciones que se den durante el ejercicio, de tal

manera tenemos evidencia de los ejercicios practicados a las áreas involucradas.

- Una lista para el control de la asistencia de los participantes, la cual debe ser firmada al inicio del taller.

Ejecución del Ejercicio

En este caso, ya definido el escenario del servidor ControlPC que se utiliza en los laboratorios de la FIEC para uso de los estudiantes en los laboratorios de computación, el evento que acontece es un incendio afectando al servidor principal que se encuentra ubicado en el cuarto del rack del edificio 16C, a continuación mostramos el esquema usado para la contingencia, para este servidor en particular.

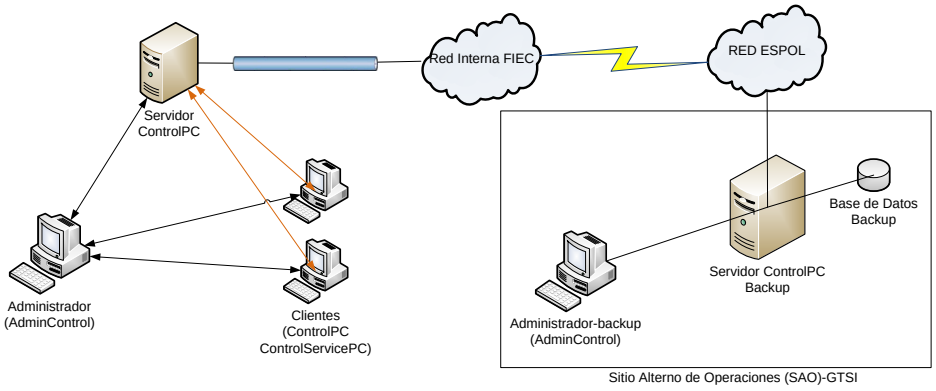


Figura 5.2 Esquema de Funcionamiento con el SAO

Fuente: El autor

En la Figura 5-2 se define el sitio alterno de operaciones ubicado en Gerencia de la Tecnología y Sistemas de Información, si bien es cierto se posee un servidor virtual que almacena el sistema operativo sobre

el cual funciona el servidor del ControlPC, el mismo que se encuentra operativo. Se aplica el PCI consultando al equipo de Desarrollo, el mismo que pone en práctica el Manual de Procedimiento de Recuperación, para poner en marcha el funcionamiento del servidor.

En este caso el Asistente Técnico de Desarrollo es el que posee el manual de configuraciones tanto para cargar la base (con el último respaldo realizado por el mismo), como las configuraciones de funcionamiento. En este simulacro de puesta a prueba, en conjunto con el equipo de Redes y Comunicaciones, que previamente definió permisos de acceso a la dirección ip del servidor de la contingencia para que se pueda comunicar con la red interna de la FIEC, junto con el Equipo de Soporte se despliega la nueva configuración en los equipos clientes de los laboratorios.

Actualización de los Planes de Continuidad

Como paso final y con el fin de cumplir con los objetivos del Ejercicio de Escritorio se requiere llevar un seguimiento y control a los cambios sugeridos a los planes de continuidad realizados (Comunicación, Recuperación de Desastres y Emergencia). Este seguimiento y control será realizado por parte de cada integrante del Equipo de Recuperación; cabe resaltar que la actualización de dichos planes es de responsabilidad exclusiva de cada área.

5.3 Análisis de Resultados

Para el análisis de resultados de la prueba de escritorio, se tomará en cuenta el análisis de riesgos con los activos de información, específicamente, los [HW] Equipos Informáticos, porque estos contienen el hardware de la infraestructura de la facultad, así como los servidores que contienen las aplicaciones más importantes que utilizan tanto personal administrativo, docentes como estudiantes; en este ejercicio, se orienta el caso particular del Servidor del ControlPC para el simulacro.

Analizando el desempeño de los equipos de recuperación en el ejercicio se describe sus funciones: el Equipo de Comunicaciones y Redes de la FIEC, tiene la tarea de asignar accesos y permisos para que la comunicación entre los clientes y servidor pueda darse de manera efectiva, así mismo de revisar el monitoreo del servicio ejecutándose. Y ante cualquier inconveniente que surja en ese momento, revisar los respectivos logs y respaldos en caso de ser necesario.

El Equipo de Soporte, así como en la realización del simulacro y como en el continuo soporte que brinda a sus usuarios, deben estar pendientes de requerimientos adicionales que sean necesarios para el simulacro, como la configuración de todas las pcs-clientes que ahora

se redicecionen al servidor ubicado en el SAO.

El Equipo de Desarrollo, encargado de la administración de las aplicaciones de la FIEC, en el que reporta el inconveniente después de la contingencia, por lo tanto es el responsable, en este simulacro, de la correcta configuración y puesta en producción del servidor ControlPC en el SAO.

Todos los equipos deben seguir los procedimientos previamente revisados de Recuperación de desastres, y siempre estar en comunicación entre ellos.

En la Tabla 10 se muestra el mapa de riesgos del activo [HW] Equipos Informáticos, y como el plan de contingencia se aplica a este y todos los equipos de hardware de la facultad, se pueden observar reducido su impacto, tal como lo muestra la siguiente tabla.

Tabla 10 Análisis de los Activos [HW]

Fuente: El autor

ACTIVOS	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
[HW] Equipos Informáticos	[N.1] Fuego	1- Sería excepcional	5–Catástrofe	Medio
	[N.2] Daños por agua	1- Sería excepcional	5–Catástrofe	Medio
	[N.*] Desastres naturales	2- Es raro que suceda	3–Moderado	Medio
	[I.1] Fuego	2- Es raro que suceda	3–Moderado	Medio
	[I.2] Daños por agua	1- Sería excepcional	4–Grande	Bajo
	[I.*] Desastres industriales	2- Es raro que suceda	4–Grande	Medio
	[I.3] Contaminación mecánica	3- Es posible	3–Moderado	Medio
	[I.4] Contaminación electromagnética	1- Sería excepcional	4–Grande	Bajo
	[I.5] Avería de origen físico o lógico	2- Es raro que suceda	3–Moderado	Medio
	[I.6] Corte del suministro eléctrico	5- Casi seguro que sucede	3–Moderado	**Alto**
	[I.7] Condiciones inadecuadas de temperatura o humedad	2- Es raro que suceda	3–Moderado	Medio
	[E.2] Errores del administrador	1- Sería excepcional	4–Grande	Bajo
	[E.23] Errores de mantenimiento /actualización de equipos (hardware)	2- Es raro que suceda	3–Moderado	Medio
	[E.24] Caída del sistema por agotamiento de recursos	3- Es posible	3–Moderado	Medio
	[E.25] Pérdida de equipos	3- Es posible	3–Moderado	Medio
	[A.6] Abuso de privilegios de acceso	1- Sería excepcional	3–Moderado	Bajo
	[A.7] Uso no previsto	1- Sería excepcional	3–Moderado	Bajo
	[A.11] Acceso no autorizado	2- Es raro que suceda	3–Moderado	Medio
	[A.23] Manipulación de los equipos	1- Sería excepcional	4–Grande	Bajo
	[A.24] Denegación de servicio	3- Es posible	5–Catástrofe	**Alto**
	[A.25] Robo	4- Muy probable	3–Moderado	**Alto**
	[A.26] Ataque destructivo	1- Sería excepcional	5–Catástrofe	Medio

Si bien es cierto aún hay riesgos Altos, pero en general se han reducido muchos riesgos que se consideraban Muy Altos y Altos para este activo en particular. A continuación se presenta la gráfica de Impacto vs Probabilidad de Ocurrencia, en la misma se observa que el Impacto ha disminuido dentro de algunas amenazas lo cual ha favorecido para que el riesgo disminuyera también.

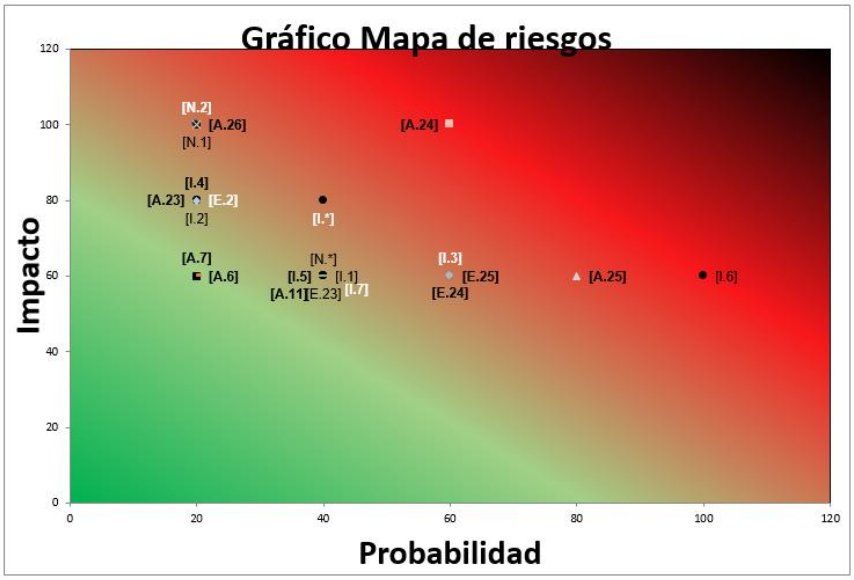


Figura 5.3 Mapa de Riesgos de [HW].

Fuente: El autor.

5.4 Modelo del Acta de Prueba del Plan de Contingencia

Para el modelo del acta de prueba, a continuación se presenta el formulario de Evaluación de Resultados, porque en el mismo se puede observar la descripción de las acciones para la realización del plan que se siguió y adicionalmente si requiere de alguna mejora o actualización por parte del Equipo de Desarrollo.

Tabla 11 Formulario para Evaluar Resultados de la Prueba del PCI

Fuente: El autor

EVALUAR RESULTADOS			
Plan de Contingencia de la FIEC | Área: Departamento de Soporte Técnico| Vigencia: día/mes/año| Versión 1.0			
CÓDIGO	**DST-PCI-PI1**		
TIPO DE INCIDENTE:	Incendio que afecta al Servidor del ControlPC	**LUGAR DEL INCIDENTE:**	Facultad de Ingeniería en Electricidad y Computación
NOMBRE DE QUIÉN LLENA REPORTE:	Asistente Técnico de Desarrollo (ADMDEV)		

Descripción de Acciones	Funcionó (SI/NO)	Como mejorar
El CPCI comunica a cada uno de los líderes de los equipos de recuperación.	SI	
El responsable asignado ejecuta los pasos para recuperación del sistema de acuerdo al nivel de falla.	SI	
Líder del equipo de Comunicación (Admredes) debe estar presente para notificar al personal del centro de cómputo del SAO(GTSI) sobre la contingencia y restablecimiento del servidor.	SI	
Líder del equipo de Desarrollo (Admdev) debe consultar con líder del equipo de Comunicaciones (admredes) para poner en marcha el servidor.	SI	
	SI	

Instalación y puesta a punto de equipo de cómputo y hardware necesario para la instalación del sistema de información.		
Instalación y configuración del sistema de información y el motor de la base de datos, con sus respectivas librerías y niveles de seguridad.	SI	
Realización del procedimiento restauración de la base de datos con la última copia de seguridad disponible.	SI	
Reiniciación del servicio, prueba y afinamiento del Servidor ControlPC.	SI	
Se debe comunicar al Equipo de Soporte para restablecer los equipos clientes de los laboratorios y se redirija al Servidor Alterno (GTySI).	SI	

CONCLUSIONES Y RECOMENDACIONES

Conclusiones

1. En la actualidad, tanto las grandes organizaciones como las empresas medianas y pequeñas, tienen la necesidad de contar entre su planificación y procesos de negocio con un plan de contingencia informático dado que la tecnología avanza cada día y para todas las empresas es imprescindible contar con una infraestructura física tecnológica y que este en continuo funcionamiento, el DST al tratarse de un Departamento dentro de la facultad de una Universidad de renombre, debe estar a la vanguardia de los avances tecnológicos y a su vez de técnicas para prevenir riesgos de TI.

2.- Elaborar un plan de contingencia para el Departamento de Soporte será de mucha utilidad, tanto para el personal que labora en el DST, como en toda la facultad, dado que es una de las más grandes de toda la ESPOL, y debe estar siempre a la vanguardia de la tecnología e información, brindando la continuidad en sus servicios informáticos ante cualquier inconveniente o contingencia.

3.- Debe siempre tener presente que la elaboración de un Plan de contingencia no significa más gastos o reducción de recursos, al contrario es una muy buena inversión que permitirá mantener la entrega del servicio o producto siempre disponible para el acceso de los usuarios.

4.- Es relevante mencionar que el presente diseño del PCI va a generar un valor agregado y una estrategia desarrollada para DST, ya que se busca lograr con él la continuidad del negocio en caso de que ocurra un desastre de origen natural con industrial. Por ello, es de mucha importancia que la FIEC implemente y este en continuo mejoramiento el presente PCI, pues bien se presenta el diseño del mismo, debería ser gestionado permanentemente para su mejora continua.

5.- Mediante el presente trabajo, se pudo analizar y conocer un poco más de los activos que administra el DST, reconocer la infraestructura que posee y las responsabilidades de los funcionarios que laboran en la FIEC.

6.- De nada sirve tener un documento formal de Plan de Contingencia si a este no se lo mantiene, prueba y actualiza de manera continua, tal cual lo indica la norma 22301:2012 y BS 25999-1 y buenas prácticas como ITIL, y MAGERIT.

7.- En base a la prueba de escritorio puedo concluir que los miembros de los diferentes equipos de recuperación, tiene muy en claro sus respectivas funciones y siempre están prestos a colaborar en lo que se necesite, al ser un grupo joven y unido han demostrado que pueden actuar de la mejor manera ante algún evento inesperado que pudiera parar los servicios de la FIEC.

Recomendaciones

1.- La FIEC, así como sus máximas autoridades deben analizar esta propuesta del plan de contingencia informático, para determinar si es factible su incorporación dentro de la facultad en especial para el DST., debido a que en esta propuesta se establecen medidas organizativas , técnicas y humanas con el fin de estar preparados ante una contingencia.

2.- Realizar pruebas y simulacros por lo menos una vez al año para verificar y mantener el continuo mejoramiento del plan de contingencia que aquí se presenta.

3.- Capacitar constantemente al personal involucrado en el DST y al personal tanto administrativo como docente que labora en la FIEC, no solamente en el proceso de recuperación de este plan informático, sino también ante eventos de desastre naturales tales como terremotos o incendios, deberían conocer los debidos protocolos de seguridad en caso de que ocurran estos eventos.

4.- Difundir adecuadamente el plan de contingencia informático a los funcionarios y partes interesadas de la organización que deseen revisarlo.

5.- Actualizar la información de los funcionarios y proveedores de servicios, cargos, funciones, responsabilidades, direcciones, teléfonos lo cual deberá ser actualizada en el plan de contingencia.

BIBLIOGRAFÍA

[1]. Soler de Arespacochaga, Jose. La Seguridad Informática: Planes de Contingencia, Disponible en: http://www.mapfre.com/documentacion/publico/i18n/catalogo_imagenes/grupo.cmd?path=1009130. Fecha de consulta 12-jun-2016, páginas 19-32.

[2]. MSc. Olaya Jorge, Curso “Plan de Contingencia”, BCM, página 14.

[3]. MSc. Olaya Jorge, Curso “Plan de Contingencia”, BCM, página 14, 17

[4]. Solís Montes Gustavo A., COBIT y la administración de riesgos Disponible en: https://www.auditool.org/blog/auditoria-de-ti/827-riesgo-tecnologico-su-medicion-como-prioridad-para-el-aseguramiento-del-negocio. Fecha de consulta: 25-jun-2016.

[5]. BCM Business continuity management, BS 25999. Disponible en: https://auditoriauc20102mivi.wikispaces.com/file/view/BCM_BS+25999_BCI201021700620355.pdf. Fecha de consulta: 25-jun-2016.

[6]. BS 25999, la nueva norma para Sistemas de Gestión de la Continuidad del Negocio. Disponible en: http://www.aec.es/c/document_library/get_file?uuid=99c086c1-9c20-4389-a9db-682ddbedc3c8&groupId=10128. Fecha de consulta: 15-jul-2016.

[7]. Nuevo estándar internacional en continuidad del negocio ISO 22301:2012. Disponible en: http://gestion.com.do/pdf/018/018-nuevo-estandar-internacional.pdf. Fecha de consulta: 15-jul-2016.

[8]. MAGERIT v.3 : Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Disponible en: https://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html#.WHrPr32cR_c. Fecha de consulta: 11-ago-2016.

[9]. MAGERIT: Metodología Práctica para Gestionar Riesgos, WeLiveSecurity, Disponible en: http://www.welivesecurity.com/la-es/2013/05/14/magerit-metodologia-practica-para-gestionar-riesgos/. Fecha de consulta: 15-ago-2016.

[10]. MAGERIT versión 3.0 Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información Libro I – Método Disponible en: https://administracionelectronica.gob.es/pae_Home/dms/pae_Home/documentos/Documentacion/Metodologias-y-guias/Mageritv3/2012_Magerit_v3_libro1_metodo_ES_NIPO_630-12-171-8/2012_Magerit_v3_libro1_metodo_es_NIPO_630-12-171-8.pdf. Fecha de consulta: 15-ago-2016.

[11]. FIEC, Organigrama. Disponible en: https://www.fiec.espol.edu.ec/es/organigrama. Fecha de consulta: 15-ago-2016.

[12]. FIEC, Historia del Departamento de Soporte Técnico (DST-FIEC). Disponible en: https://www.fiec.espol.edu.ec/es/historia-dst. Fecha de consulta: 15-ago-2016.

[13]. PRESIDENCIA / DINASED/FGE, PRESIDENCIA /DINASED, MTT2 (MSP, IESS, Instituto de Seguridad Social de la Policía Nacional, Instituto de Seguridad Disponible en: http://www.eltelegrafo.com.ec/especiales/2016/Lista-de-fallecidos-por-terremoto-en-Ecuador/. Fecha de consulta: 13-ene-2017.

[14]. Filián Gómez Margarita, “Implementación de un Esquema de Seguridad de Informática Aplicado a los Activos de la FIEC, basado en el estándar ISO 27002”, ESPOL, Guayaquil, 2015

[15]. Castro Marquina Laura Daiana, Diseño de un Sistema de Gestión de Continuidad de Negocios (sgcn) para la RENIEC bajo la óptica de la NORMA ISO/IEC 22301. Scribd. Disponible en: https://es.scribd.com/document/209290225/CASTRO-LAURA-DISENO-SISTEMA-GESTION-CONTINUIDAD-NEGOCIOS-RENIEC-NORMA-ISO-IEC-22301. Fecha de consulta: 15-oct-2016.

[16]. Carpio Cobos Alfredo Marcelo, “Elaborar el Plan de Contingencia Informático, de la unidad de negocio Hidropaute CELEC EP, que permita garantizar la continuidad de las actividades ante eventos que podrían alterar el normal funcionamiento de la tecnología de la información y comunicación (TIC).” ESPOL, Guayaquil, 2015.

[17]. COPNIA, Plan de Contingencia y Políticas de Seguridad de Sistemas de Información, Disponible en: https://copnia.gov.co/uploads/filebrowser/DCALIDAD/SI-mp-01%20MANUAL%20DE%20CONTINGENCIA.pdf. Fecha de consulta: 05-ene-2017.

[18]. Castro Marquina Laura Daiana, “Diseño de un Sistema de Gestión de Continuidad de Negocios (SGCN) para la RENIEC bajo la óptica de la Norma ISO/IEC 22301” Anexos, Pontificia Universidad Católica del Perú, Disponible en: http://tesis.pucp.edu.pe/repositorio/handle/123456789/5110 Fecha de consulta 05-ene-2017.

ANEXOS

ANEXO A

ACTIVOS DE LA FIEC		[D] Disponibilidad	[I] Integridad	[C] Confidencialidad
[D] Datos		**5**	**6**	**5**
[bd_crm]	Base de Datos de CRM	1	3	3
[bd_reservar]	Base de Datos de Reservar Salas	3	3	3
[bd_controlac]	Base de Datos de CONTROLAC	5	5	3
[bd_reunion]	Base de Datos de Reuniones	3	4	3
[bd_ara]	Base de Datos de ARA	5	5	5
[bd_satt]	Base de Datos de SATT	5	5	7
[backup]	Copias de Respaldo	7	7	5
[source]	Código Fuente	7	7	5
[files]	Archivos	7	7	6
[bd_controlpc]	Base de Datos de CONTROLPC	5	6	7
[conf]	Datos de Configuración	7	7	7
[log]	Registro de Actividad	7	7	3
[bd_ldap]	LDAP	7	7	9
[bd_sitioFiec]	Base de Datos del Sitio Web de la FIEC	7	7	7
[S] Servicios		**5**	**5**	**4**
[serv_a/v]	Audio y Video	3	1	1
[serv_equi]	Préstamo de Equipos	3	1	1
[serv_support]	Asistencia Técnica	5	5	3
[serv_dev]	Implementación y Administración de sistemas/sitio web para la FIEC	7	7	5
[serv_acco]	Gestión de Identidades (Creación de cuentas)	3	3	2
[serv_wifi]	Red Inalámbrica exclusiva de la FIEC	5	5	5
[email]	Correo Electrónico	9	9	7
[serv_mante]	Mantenimiento a Equipos	5	3	3
[serv_file]	Almacenamiento de archivos y aplicaciones desarrolladas por estudiantes	1	7	5
[serv_labs]	Préstamo de Laboratorios	7	5	3
[SW] Software - Aplicaciones Informáticas		**5**	**5**	**3**

[sis_crm]	Sistema CRM	1	1	3
[sis_controlac]	Sistema CONTROLAC	5	4	3
[sis_creacion]	Sistema Creación de Cuentas	5	4	2
[sis_reunion]	Sistema de Reuniones	3	3	3
[sis_reservar]	Sistema Reservar Salas	3	5	3
[sis_ara]	Sistema ARA	7	5	3
[sis_satt]	Sistema SATT	7	5	3
[pkt]	Repositorio de Software Vario	7	5	5
[sis_controlpc]	Sistema CONTROLPC	5	5	1
[av]	Antivirus	9	9	7
[sis_portal]	Portal Cautivo	5	5	3
[HW] Equipos Informáticos		**5**	**5**	**4**
[print]	Medios de Impresión	3	1	0
[scan]	Escáneres	1	1	1
[cam]	Cámara IP	3	3	3
[mobile]	Laptop	1	1	3
[srv_stmg]	Streaming	1	1	3
[wap]	Punto de Acceso Inalámbrico	3	3	3
[pc]	Computador	7	3	3
[srv_files]	Archivos	5	6	7
[srv_control]	Control-PC	5	5	5
[srv_dhcp]	DHCP	5	5	3
[srv_radius]	Radius	5	5	3
[switch]	Conmutadores	9	9	6
[router]	Ruteadores	9	9	6
[srv_mail]	Correos	7	9	7
[srv_db]	Base de Datos	7	9	8
[srv_web]	Web	7	9	7
[srv_ant]	Antivirus	9	9	7
[COM] Redes de Comunicaciones		**8**	**8**	**7**
[wifi]	Red Inalámbrica	7	7	5
[lan]	Red cableada	9	9	9
[MEDIA] Soportes de Información		**7**	**5**	**4**
[disk]	Discos	7	5	5
[san]	Almacenamiento en red	7	6	3
[tape]	Cinta Magnética	7	5	5
[AUX] Equipamiento Auxiliar		**5**	**3**	**1**
[furniture]	Mobiliario: armarios, racks etc	5	0	0
[tools]	Herramientas de Soporte y Mantenimiento	1	1	0

[tools_network]	Herramientas de Soporte y Mantenimiento redes	1	1	0
[ss]	Sistema de Seguridad	7	3	7
[ups]	Sistema de Alimentación Ininterrumpida	7	6	0
[ac]	Equipos de Climatización	7	7	0
[L] Instalaciones		**9**	**2**	**2**
[building]	Edificio	9	1	0
[local]	Cuarto de rack y servidores	9	3	3
[P] Personal		**7**	**5**	**5**
[adm]	Administradores de la Infraestructura Tecnológica	7	5	5
[com]	Administrador de Redes y Servidores	7	5	5
[ast]	Analista de Soporte Técnico	7	5	5
[des]	Desarrolladores / Programadores	7	5	5
[wm]	Web master	7	5	5

ANEXO B

CRITERIOS DE VALORIZACIÓN DE ACTIVOS DEFINIDOS EN MAGERIT

[pi] Información de carácter Personal		
6	6.pi1	Probablemente afecte gravemente a un grupo de individuos
	6.pi2	Probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
5	5.pi1	Probablemente afecte gravemente a un individuo
	5.pi2	Probablemente quebrante seriamente leyes o regulaciones
4	4.pi1	Probablemente afecte a un grupo de individuos
	4.pi2	Probablemente quebrante leyes o regulaciones
3	3.pi1	Probablemente afecte a un individuo
	3.pi2	Probablemente suponga el incumplimiento de una ley o regulación
2	2.pi1	Pudiera causar molestias a un individuo
	2.pi2	Pudiera quebrantar de forma leve leyes o regulaciones
1	1.pi1	Pudiera causar molestias a un individuo
[lpo] Obligaciones legales		
9	9.lro	Probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7	7.lro	Probablemente cause un incumplimiento grave de una ley o regulación
5	5.lro	Probablemente sea causa de incumplimiento de una ley o regulación
3	3.lro	Probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
1	1.lro	Pudiera causar el incumplimiento leve o técnico de una ley o regulación
[si] Seguridad		
10	10.si	Probablemente sea causa de un incidente excepcionalmente serio de seguridad o dificulte la investigación de incidentes excepcionalmente serios
9	9.si	Probablemente sea causa de un serio incidente de seguridad o dificulte la investigación de incidentes serios
7	7.si	Probablemente sea causa de un grave incidente de seguridad o dificulte la investigación de incidentes graves
3	3.si	Probablemente sea causa de una merma en la seguridad o dificulte la investigación de un incidente
1	1.si	Pudiera causar una merma en la seguridad o dificultar la investigación de un incidente
[cei] Intereses comerciales o económicos		
9	9.cei.a	De enorme interés para la competencia
	9.cei.b	De muy elevado valor comercial
	9.cei.c	Causa de pérdidas económicas excepcionalmente elevadas
	9.cei.d	Causa de muy significativas ganancias o ventajas para individuos u organizaciones

	9.cei.e	Constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
7	7.cei.a	De alto interés para la competencia
	7.cei.b	De elevado valor comercial
	7.cei.c	Causa de graves pérdidas económicas
	7.cei.d	Proporciona ganancias o ventajas desmedidas a individuos u organizaciones
	7.cei.e	Constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
3	3.cei.a	De cierto interés para la competencia
	3.cei.b	De cierto valor comercial
	3.cei.c	Causa de pérdidas financieras o merma de ingresos
	3.cei.d	Facilita ventajas desproporcionadas a individuos u organizaciones
	3.cei.e	Constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
2	2.cei.a	De bajo interés para la competencia
	2.cei.b	De bajo valor comercial
1	1.cei.a	De pequeño interés para la competencia
	1.cei.b	De pequeño valor comercial
0	0.3	Supondría pérdidas económicas mínimas
[da] Interrupción del servicio		
9	9.da	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
	9.da2	Probablemente tenga un serio impacto en otras organizaciones
7	7.da	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
	7.da2	Probablemente tenga un gran impacto en otras organizaciones
5	5.da	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	5.da2	Probablemente cause un cierto impacto en otras organizaciones
3	3.da	Probablemente cause la interrupción de actividades propias de la Organización
1	1.da	Pudiera causar la interrupción de actividades propias de la Organización
[po] Orden público		
9	9.po	Alteración sería del orden público
6	6.po	Probablemente cause manifestaciones, o presiones significativas
3	3.po	Causa de protestas puntuales
1	1.po	Pudiera causar protestas puntuales
[olm] Operaciones		
10	10.olm	Probablemente cause un daño excepcionalmente serio a la eficacia o seguridad de la misión operativa o logística

9	9.olm	Probablemente cause un daño serio a la eficacia o seguridad de la misión operativa o logística
7	7.olm	Probablemente perjudique la eficacia o seguridad de la misión operativa o logística
5	5.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística más allá del ámbito local
3	3.olm	Probablemente merme la eficacia o seguridad de la misión operativa o logística (alcance local)
1	1.olm	Pudiera mermar la eficacia o seguridad de la misión operativa o logística (alcance local)
[adm] Administración y Gestión		
9	9.adm	Probablemente impediría seriamente la operación efectiva de la Organización, pudiendo llegar a su cierre
7	7.adm	Probablemente impediría la operación efectiva de la Organización
5	5.adm	Probablemente impediría la operación efectiva de más de una parte de la Organización
3	3.adm	Probablemente impediría la operación efectiva de una parte de la Organización
1	1.adm	Pudiera impedir la operación efectiva de una parte de la Organización
[lg] Pérdida de confianza (reputación)		
9	9.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
	9.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
7	7.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
	7.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
5	5.lg.a	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones
	5.lg.b	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público
3	3.lg	Probablemente afecte negativamente a las relaciones internas de la Organización
2	2.lg	Probablemente cause una pérdida menor de la confianza dentro de la Organización
1	1.lg	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	0.4	no supondría daño a la reputación o buena imagen de las personas u organizaciones
[crm] Persecución de delitos		
8	8.crm	Impida la investigación de delitos graves o facilite su comisión
4	4.crm	Dificulte la investigación o facilite la comisión de delitos
[rto] Tiempo de recuperación del servicio		

7	7.rto	RTO < 4 horas
4	4.rto	4 horas < RTO < 1 día
1	1.rto	1 día < RTO < 5 días
0	0.rto	5 días < RTO
[lbl.nat] Información clasificada (nacional)		
10	10.lbl	Secreto
9	9.lbl	Reservado
8	8.lbl	Confidencial
7	7.lbl	Confidencial
6	6.lbl	Difusión limitada
5	5.lbl	Difusión limitada
4	4.lbl	Difusión limitada
3	3.lbl	Difusión limitada
2	2.lbl	Sin clasificar
1	1.lbl	Sin clasificar

ANEXO C

ROLES: FUNCIONES Y RESPONSABILIDADES

A continuación se describen las responsabilidades y funciones que requiere casa rol que se ha definido para el esquema de seguridad de informática:

Responsable de servicios e infraestructura tecnológica
El Jefe del DST tendrá el rol de responsable de los servicios informáticos y de los activos que forma la infraestructura tecnológica de la FIEC. Teniendo por funciones las siguientes: • Establecer los requisitos de los servicios en materia de seguridad. • Trabajar con el responsable de seguridad, sistemas y soporte en el mantenimiento y revisión de los servicios, equipos y sistemas alineándolos al esquema de seguridad. • Coordinar las actividades con los demás responsables para lograr la adecuada y oportuna implementación del esquema de seguridad. • Realizar revisiones y estado de las incidencias ocurridas. • Verificar que los sistemas desarrollados no presenten vulnerabilidades, realizando pruebas sobre los mismos.

Responsables de Seguridad
El Jefe del DST y el Asistente Técnico de Redes tienen el rol de responsable de seguridad. • El Jefe del DST tiene por funciones las siguientes: • Mantener la seguridad de la información y los servicios que administra • Realizar revisiones periódicas que permitan verificar el cumplimiento del esquema de seguridad. • Difundir y promover la concienciación de la seguridad informática dentro de su ámbito de responsabilidad.

- Coordinar reuniones con los demás responsables de seguridad para verificar que las medidas y esquema de seguridad establecidas son adecuadas para la protección de los activos.
- Analizar, modificar, y completar la documentación relacionada con el esquema de seguridad.
- Aprobar los procedimientos de seguridad elaborados por los demás responsables.
- Revisar que el sistema de control de acceso y CCTV funcione correctamente.

El Asistente Técnico de Redes tiene por funciones las siguientes:

- Monitorear el estado de la red y servidores.
- Sugerir herramientas o mecanismos que ayuden en el análisis de logs y eventos.
- Investigar a cerca de los incidentes de seguridad desde que son notificados hasta que sean resueltos.
- Llevar una bitácora de los incidentes ocurridos.
- Realizar hardening en los sistemas para reducir vulnerabilidades y posibles amenazas.
- Asegurar que la red inalámbrica ingresen a través del portal cautivo.
- Realizar copias de seguridad de la información de los principales servidores de la FIEC.
- Revisar periódicamente el estado de las bases y sus usuarios.
- Determinar la configuración de hardware y software a utilizar en el sistema,
- Configuración y puesta a punto de las bases de datos.

Responsable de Sistemas

El Asistente Técnico de Desarrollo en el rol de responsable de los sistemas. Tiene por funciones, dentro de sus áreas de trabajo, las siguientes:

- Desarrollar, administrar y mantener los sistemas que desarrollo o se le asignen durante todo su ciclo de vida, realizando tareas de instalación configuración y verificación de su correcto funcionamiento.

- Definir como se conectan los usuarios a los sistemas, ya sea a través de credenciales de la FIEC o ESPOL.
- Sugerir y documentar los cambios que afecten a la seguridad de los sistemas en el modo que operan.
- Sugerir y aplicar las medidas de seguridad al momento de desarrollar los sistemas.
- Considerar todos los escenarios posibles de posibles vulnerabilidades en los sistemas y corregirlos.
- Determinar la configuración de hardware y software a utilizar en el sistema.
- Documentar los cambios realizados en los sistemas.
- Definir perfiles de acceso para cada sistema.
- Investigar acerca de incidentes de seguridad que afecten los sistemas en lo relacionado con versiones de software, sistema operativo y código; documentarlos y comunicarlo a las personas responsables de seguridad.
- Realizar las pruebas necesarias de los sistemas desarrollados con el fin de evitar posibles vulnerabilidades.
- Revisar que los sistemas que desarrolle no presenten información de dirección ip, versión de base de datos o sistema operativo donde es alojado, es decir información del servidor.

Responsables de Soporte

Los Asistentes Técnico de Soporte en el rol de responsable de soporte. Tienen por funciones, dentro de sus áreas de trabajo, las siguientes:

- Realizar mantenimiento preventivo y correctivos al finalizar un semestre.
- Deben mantener y actualizar el inventario de los equipos a su cargo.
- Instalar antivirus en todos los equipos con inventario ESPOL.
- Realiza configuraciones necesarias para evitar que ejecución de código malicioso mediante el autorun.
- Los equipos a su cargo deben tener configuradas contraseñas.
- Deben sugerir y realizar actualizaciones de paquetes de programas, sistemas operativos y parches.

Responsable del sitio web
El Webmaster en el rol de responsable de sitio web, Tienen por funciones, dentro de sus áreas de trabajo, las siguientes: • Realizar mantenimiento al sitio web de la FIEC. • Sugerir y realizar cambios en los componentes o plugins que presenten vulnerabilidades. • Sugerir el cambio de versión del administrador de contenido. • Revisar que el sitio web no presente información de dirección ip, versión de base de datos o sistema operativo.

ANEXO D

ANÁLISIS DE RIESGOS				
ACTIVOS	**AMENAZA**	**PROBABILIDAD**	**IMPACTO**	**RIESGO**
[D] Datos	[E.1] Errores de los usuarios	4- Muy probable	2–Pequeño	Medio
	[E.2] Errores del administrador	3- Es posible	4–Grande	**Alto**
	[E.3] Errores de monitorización (log)	2- Es raro que suceda	4–Grande	Medio
	[E.4] Errores de Configuración	2- Es raro que suceda	4–Grande	Medio
	[E.14] Escapes de información	1- Sería excepcional	3–Moderado	Bajo
	[E.15] Alteración accidental de la información	1- Sería excepcional	4–Grande	Bajo
	[E.18] Destrucción de información	1- Sería excepcional	5–Catástrofe	Medio
	[E.19] Fugas de información	1- Sería excepcional	4–Grande	Bajo
	[A.4] Manipulación de la configuración	1- Sería excepcional	4–Grande	Bajo
	[A.5] Suplantación de la identidad del usuario	2- Es raro que suceda	3–Moderado	Medio
	[A.6] Abuso de privilegios de acceso	1- Sería excepcional	4–Grande	Bajo
	[A.11] Acceso no autorizado	1- Sería excepcional	3–Moderado	Bajo
	[A.13] Repudio	2- Es raro que suceda	3–Moderado	Medio
	[A.15] Modificación deliberada de la información	1- Sería excepcional	5–Catástrofe	Medio
	[A.18] Destrucción de información	3- Es posible	4–Grande	**Alto**
	[A.19] Divulgación de información	2- Es raro que suceda	4–Grande	Medio

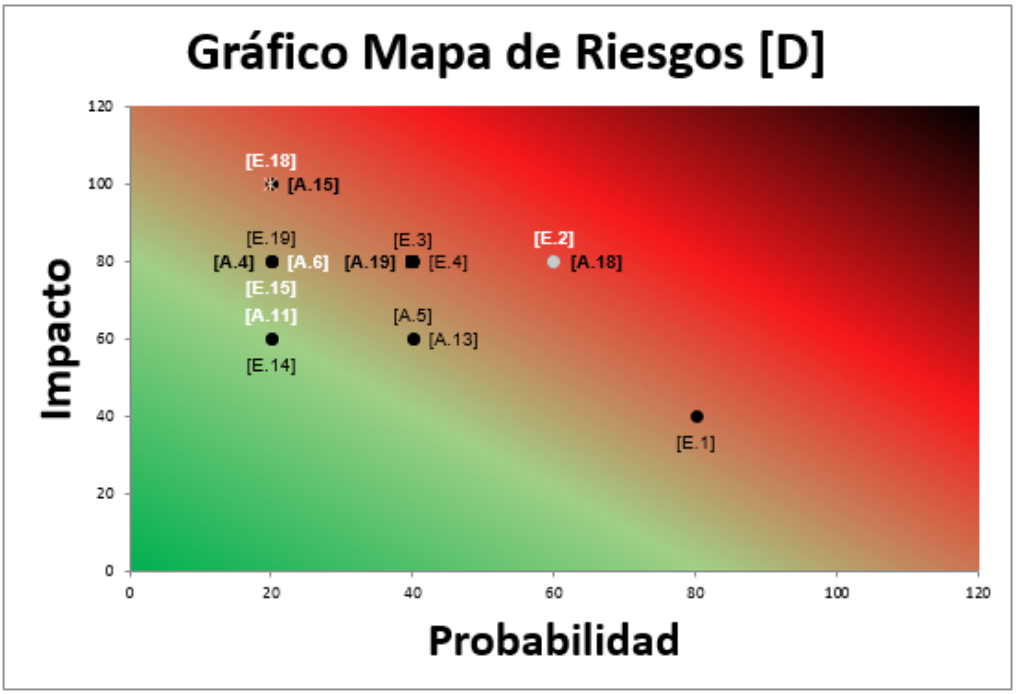


Gráfico Mapa de Riesgos [D]
Impacto
Probabilidad
120
100
80
60
40
20
0
0
20
40
60
80
100
120
[E.18]
[A.15]
[E.19]
[A.4]
[A.6]
[E.15]
[A.11]
[E.14]
[E.3]
[A.19]
[E.4]
[A.5]
[A.13]
[E.2]
[A.18]
[E.1]

ACTIVOS	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
[S] Servicios	[E.1] Errores de los usuarios	4- Muy probable	1– Insignificante	Bajo
	[E.2] Errores del administrador	3- Es posible	2–Pequeño	Medio
	[E.9] Errores de [re]encaminamiento	1- Sería excepcional	4–Grande	Bajo
	[E.10] Errores de secuencia	2- Es raro que suceda	2–Pequeño	Bajo
	[E.15] Alteración accidental de la información	2- Es raro que suceda	4–Grande	Medio
	[E.18] Destrucción de información	1- Sería excepcional	5–Catástrofe	Medio
	[E.19] Fugas de información	1- Sería excepcional	1– Insignificante	Bajo
	[E.24] Caída del sistema por agotamiento de recursos	3- Es posible	4–Grande	**Alto**
	[A.5] Suplantación de la identidad del usuario	1- Sería excepcional	4–Grande	Bajo
	[A.6] Abuso de privilegios de acceso	3- Es posible	4–Grande	**Alto**
	[A.7] Uso no previsto	3- Es posible	2–Pequeño	Medio
	[A.9] [Re-] encaminamiento de mensajes	1- Sería excepcional	3–Moderado	Bajo
	[A.10] Alteración de secuencia	2- Es raro que suceda	2–Pequeño	Bajo
	[A.11] Acceso no autorizado	1- Sería excepcional	4–Grande	Bajo
	[A.13] Repudio	1- Sería excepcional	2–Pequeño	Bajo
	[A.15] Modificación deliberada de la información	1- Sería excepcional	4–Grande	Bajo
	[A.18] Destrucción de información	1- Sería excepcional	5–Catástrofe	Medio
	[A.19] Divulgación de información	2- Es raro que suceda	2–Pequeño	Bajo
	[A.24] Denegación de servicio	1- Sería excepcional	4–Grande	Bajo

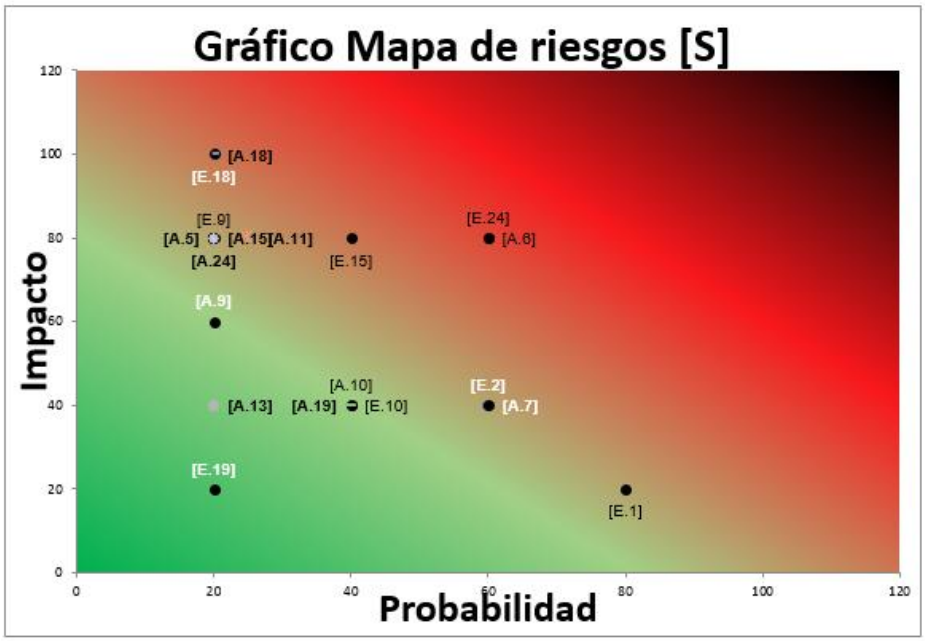


Gráfico Mapa de riesgos [S]
Impacto
Probabilidad
0
20
40
60
80
100
120
[A.18]
[E.18]
[E.9]
[A.5]
[A.15][A.11]
[A.24]
[E.15]
[E.24]
[A.6]
[A.9]
[A.10]
[A.13]
[A.19]
[E.10]
[E.2]
[A.7]
[E.19]
[E.1]

ACTIVOS	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
[SW] Software - Aplicaciones Informáticas	[I.5] Avería de origen físico o lógico	2- Es raro que suceda	5–Catástrofe	**Alto**
	[E.1] Errores de los usuarios	3- Es posible	3–Moderado	Medio
	[E.2] Errores del administrador	2- Es raro que suceda	4–Grande	Medio
	[E.8] Difusión de software dañino	3- Es posible	5–Catástrofe	**Alto**
	[E.9] Errores de [re]encaminamiento	1- Sería excepcional	4–Grande	Bajo
	[E.10] Errores de secuencia	1- Sería excepcional	3–Moderado	Bajo
	[E.15] Alteración accidental de la información	2- Es raro que suceda	3–Moderado	Medio
	[E.18] Destrucción de información	1- Sería excepcional	5–Catástrofe	Medio
	[E.19] Fugas de información	1- Sería excepcional	4–Grande	Bajo
	[E.20] Vulnerabilidades de los programas (software)	2- Es raro que suceda	5–Catástrofe	**Alto**
	[E.21] Errores de mantenimiento/actualización de programas (software)	2- Es raro que suceda	4–Grande	Medio
	[A.5] Suplantación de la identidad del usuario	1- Sería excepcional	4–Grande	Bajo
	[A.6] Abuso de privilegios de acceso	2- Es raro que suceda	4–Grande	Medio
	[A.7] Uso no previsto	1- Sería excepcional	1– Insignificante	Bajo
	[A.8] Difusión de software dañino	1- Sería excepcional	4–Grande	Bajo
	[A.9] [Re-] encaminamiento de mensajes	1- Sería excepcional	3–Moderado	Bajo
	[A.10] Alteración de secuencia	1- Sería excepcional	2–Pequeño	Bajo
	[A.11] Acceso no autorizado	1- Sería excepcional	3–Moderado	Bajo
	[A.15] Modificación deliberada de la información	1- Sería excepcional	4–Grande	Bajo
	[A.18] Destrucción de información	1- Sería excepcional	5–Catástrofe	Medio
	[A.19] Divulgación de información	2- Es raro que suceda	3–Moderado	Medio
	[A.22] Manipulación de programas	1- Sería excepcional	5–Catástrofe	Medio

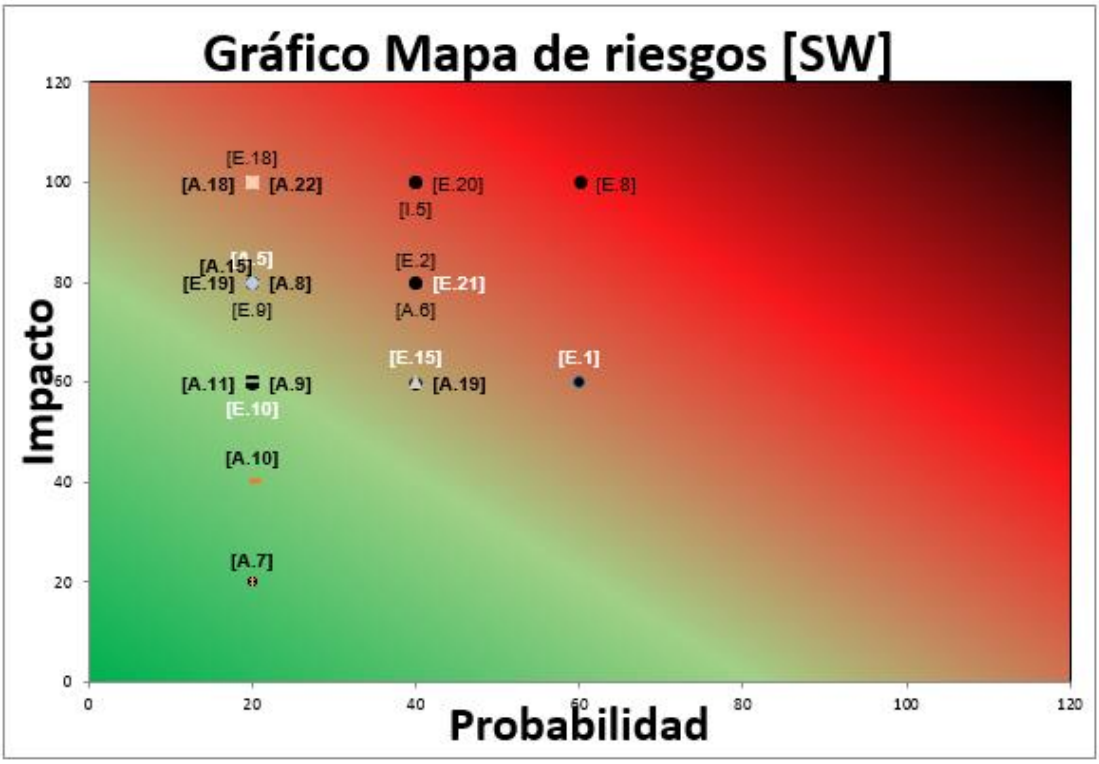
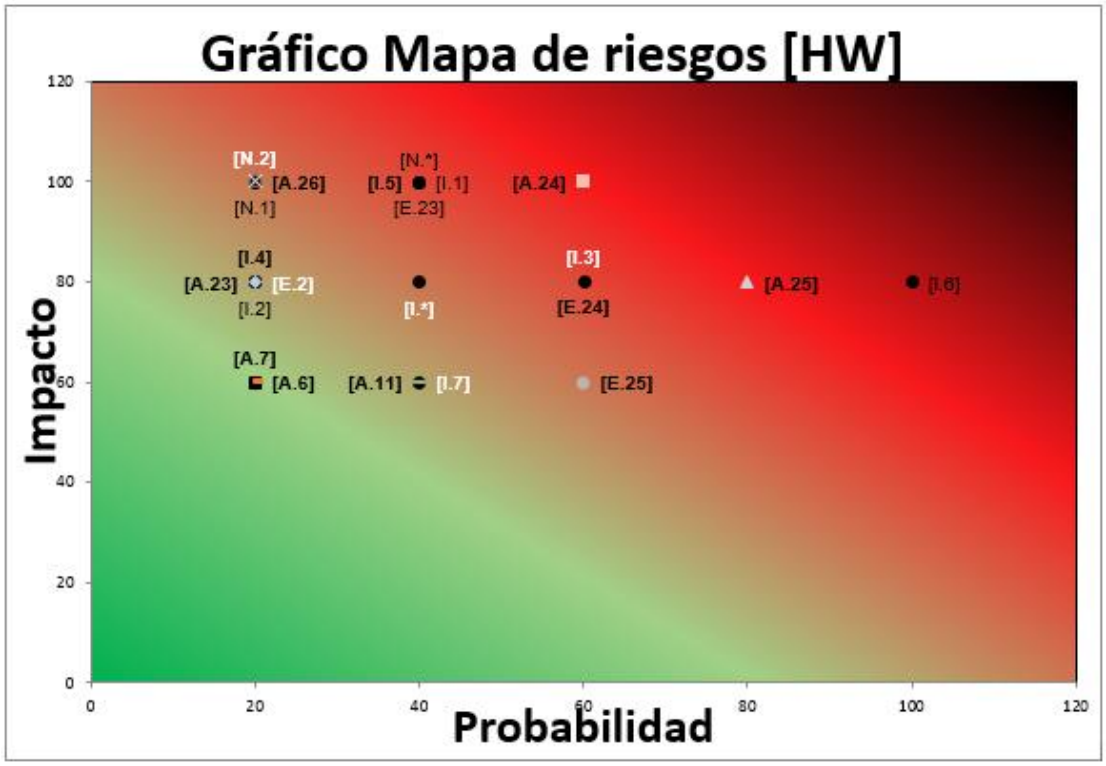


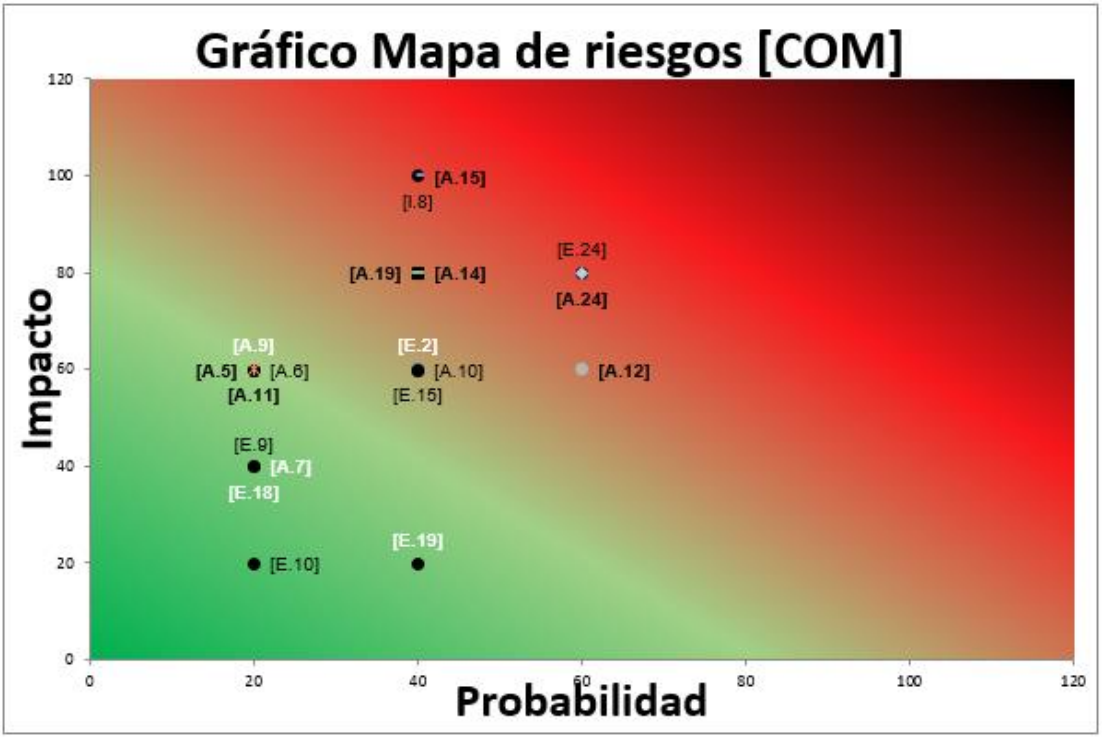
Gráfico Mapa de riesgos [SW]
Impacto
Probabilidad
120
100
80
60
40
20
0
0
20
40
60
80
100
120
[E.18]
[A.18]
[A.22]
[E.20]
[E.8]
[I.5]
[A.15]
[E.19]
[A.8]
[E.9]
[E.2]
[E.21]
[A.6]
[E.15]
[E.1]
[A.11]
[A.9]
[A.19]
[E.10]
[A.10]
[A.7]

ACTIVOS	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
[HW] Equipos Informáticos	[N.1] Fuego	1- Sería excepcional	5–Catástrofe	Medio
	[N.2] Daños por agua	1- Sería excepcional	5–Catástrofe	Medio
	[N.*] Desastres naturales-Terremotos	2- Es raro que suceda	5–Catástrofe	**Alto**
	[I.1] Fuego	2- Es raro que suceda	5–Catástrofe	**Alto**
	[I.2] Daños por agua	1- Sería excepcional	4–Grande	Bajo
	[I.*] Desastres industriales	2- Es raro que suceda	4–Grande	Medio
	[I.3] Contaminación mecánica	3- Es posible	4–Grande	**Alto**
	[I.4] Contaminación electromagnética	1- Sería excepcional	4–Grande	Bajo
	[I.5] Avería de origen físico o lógico	2- Es raro que suceda	5–Catástrofe	**Alto**
	[I.6] Corte del suministro eléctrico	5- Casi seguro que sucede	4–Grande	**Muy alto**
	[I.7] Condiciones inadecuadas de temperatura o humedad	2- Es raro que suceda	3–Moderado	Medio
	[E.2] Errores del administrador	1- Sería excepcional	4–Grande	Bajo
	[E.23] Errores de mantenimiento /actualización de equipos (hardware)	2- Es raro que suceda	5–Catástrofe	**Alto**
	[E.24] Caída del sistema por agotamiento de recursos	3- Es posible	4–Grande	**Alto**
	[E.25] Pérdida de equipos	3- Es posible	3–Moderado	Medio
	[A.6] Abuso de privilegios de acceso	1- Sería excepcional	3–Moderado	Bajo
	[A.7] Uso no previsto	1- Sería excepcional	3–Moderado	Bajo
	[A.11] Acceso no autorizado	2- Es raro que suceda	3–Moderado	Medio
	[A.23] Manipulación de los equipos	1- Sería excepcional	4–Grande	Bajo
	[A.24] Denegación de servicio	3- Es posible	5–Catástrofe	**Alto**
	[A.25] Robo	4- Muy probable	4–Grande	**Alto**
	[A.26] Ataque destructivo	1- Sería excepcional	5–Catástrofe	Medio



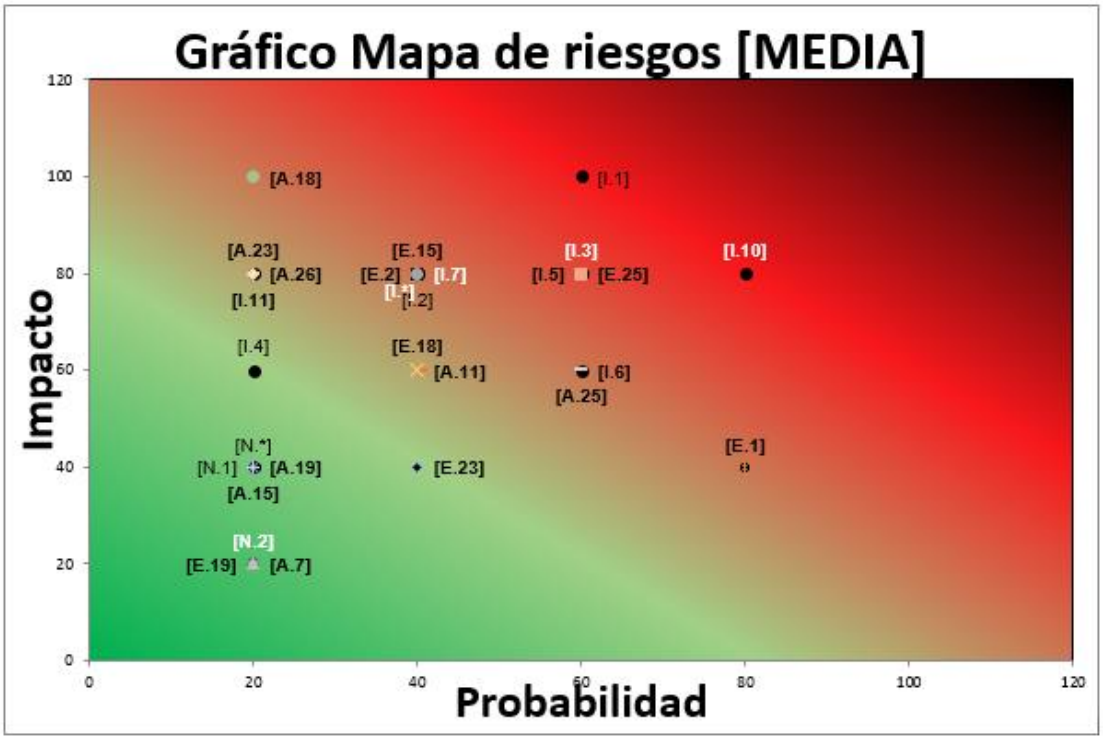
ACTIVOS	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
[COM] Redes de Comunicaciones	[I.8] Fallo de servicios de comunicaciones	2- Es raro que suceda	5–Catástrofe	**Alto**
	[E.2] Errores del administrador	2- Es raro que suceda	3–Moderado	Medio
	[E.9] Errores de [re]encaminamiento	1- Sería excepcional	2–Pequeño	Bajo
	[E.10] Errores de secuencia	1- Sería excepcional	1–Insignificante	Bajo
	[E.15] Alteración accidental de la información	2- Es raro que suceda	3–Moderado	Medio
	[E.18] Destrucción de información	1- Sería excepcional	2–Pequeño	Bajo
	[E.19] Fugas de información	2- Es raro que suceda	1–Insignificante	Bajo
	[E.24] Caída del sistema por agotamiento de recursos	3- Es posible	4–Grande	**Alto**

	[A.5] Suplantación de la identidad del usuario	1- Sería excepcional	3–Moderado	Bajo
	[A.6] Abuso de privilegios de acceso	1- Sería excepcional	3–Moderado	Bajo
	[A.7] Uso no previsto	1- Sería excepcional	2–Pequeño	Bajo
	[A.9] [Re-] encaminamiento de mensajes	1- Sería excepcional	3–Moderado	Bajo
	[A.10] Alteración de secuencia	2- Es raro que suceda	3–Moderado	Medio
	[A.11] Acceso no autorizado	1- Sería excepcional	3–Moderado	Bajo
	[A.12] Análisis de tráfico	3- Es posible	3–Moderado	Medio
	[A.14] Interceptación de información (escucha)	2- Es raro que suceda	4–Grande	Medio
	[A.15] Modificación deliberada de la información	2- Es raro que suceda	5–Catástrofe	**Alto**
	[A.19] Divulgación de información	2- Es raro que suceda	4–Grande	Medio
	[A.24] Denegación de servicio	3- Es posible	4–Grande	**Alto**



ACTIVOS	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
[MEDIA] Soportes de Información	[N.1] Fuego	1- Sería excepcional	2–Pequeño	Bajo
	[N.2] Daños por agua	1- Sería excepcional	1–Insignificante	Bajo
	[N.*] Desastres naturales-Terremotos	1- Sería excepcional	2–Pequeño	Bajo
	[I.1] Fuego	3- Es posible	5–Catástrofe	**Alto**
	[I.2] Daños por agua	2- Es raro que suceda	4–Grande	Medio
	[I.*] Desastres industriales	2- Es raro que suceda	4–Grande	Medio
	[I.3] Contaminación mecánica	3- Es posible	4–Grande	**Alto**
	[I.4] Contaminación electromagnética	1- Sería excepcional	3–Moderado	Bajo
	[I.5] Avería de origen físico o lógico	3- Es posible	4–Grande	**Alto**
	[I.6] Corte del suministro eléctrico	3- Es posible	3–Moderado	Medio
	[I.7] Condiciones inadecuadas de temperatura o humedad	2- Es raro que suceda	4–Grande	Medio
	[I.10] Degradación de los soportes de almacenamiento de la información	4- Muy probable	4–Grande	**Alto**
	[I.11] Emanaciones electromagnéticas	1- Sería excepcional	4–Grande	Bajo
	[E.1] Errores de los usuarios	4- Muy probable	2–Pequeño	Medio
	[E.2] Errores del administrador	2- Es raro que suceda	4–Grande	Medio
	[E.15] Alteración accidental de la información	2- Es raro que suceda	4–Grande	Medio
	[E.18] Destrucción de información	2- Es raro que suceda	3–Moderado	Medio
	[E.19] Fugas de información	1- Sería excepcional	1–Insignificante	Bajo
	[E.23] Errores de mantenimiento/ actualización de equipos (hardware)	2- Es raro que suceda	2–Pequeño	Bajo
	[E.25] Pérdida de equipos	3- Es posible	4–Grande	**Alto**
	[A.7] Uso no previsto	1- Sería excepcional	1–Insignificante	Bajo
	[A.11] Acceso no autorizado	2- Es raro que suceda	3–Moderado	Medio
	[A.15] Modificación deliberada de la información	1- Sería excepcional	2–Pequeño	Bajo
	[A.18] Destrucción de información	1- Sería excepcional	5–Catástrofe	Medio

[A.19] Divulgación de información	1- Sería excepcional	2–Pequeño	Bajo
[A.23] Manipulación de los equipos	1- Sería excepcional	4–Grande	Bajo
[A.25] Robo	3- Es posible	3–Moderado	Medio
[A.26] Ataque destructivo	1- Sería excepcional	4–Grande	Bajo



ACTIVOS	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
[AUX] Equipamiento Auxiliar	[N.1] Fuego	2- Es raro que suceda	5–Catástrofe	**Alto**
	[N.2] Daños por agua	1- Sería excepcional	4–Grande	Bajo
	[N.*] Desastres naturales-Terremotos	3- Es posible	5–Catástrofe	**Alto**
	[I.1] Fuego	3- Es posible	4–Grande	**Alto**
	[I.2] Daños por agua	2- Es raro que suceda	3–Moderado	Medio
	[I.*] Desastres industriales	3- Es posible	3–Moderado	Medio
	[I.3] Contaminación mecánica	3- Es posible	3–Moderado	Medio
	[I.4] Contaminación electromagnética	1- Sería excepcional	2–Pequeño	Bajo
	[I.5] Avería de origen físico o lógico	3- Es posible	4–Grande	**Alto**
	[I.6] Corte del suministro eléctrico	5- Casi seguro que sucede	5–Catástrofe	**Muy alto**
	[I.7] Condiciones inadecuadas de temperatura o humedad	2- Es raro que suceda	3–Moderado	Medio
	[I.9] Interrupción de otros servicios y suministros esenciales	1- Sería excepcional	3–Moderado	Bajo
	[E.23] Errores de mantenimiento/ actualización de equipos (hardware)	1- Sería excepcional	3–Moderado	Bajo
	[E.25] Pérdida de equipos	4- Muy probable	4–Grande	**Alto**
	[A.7] Uso no previsto	1- Sería excepcional	3–Moderado	Bajo
	[A.11] Acceso no autorizado	2- Es raro que suceda	3–Moderado	Medio
	[A.23] Manipulación de los equipos	1- Sería excepcional	2–Pequeño	Bajo
	[A.25] Robo	1- Sería excepcional	4–Grande	Bajo
	[A.26] Ataque destructivo	1- Sería excepcional	4–Grande	Bajo

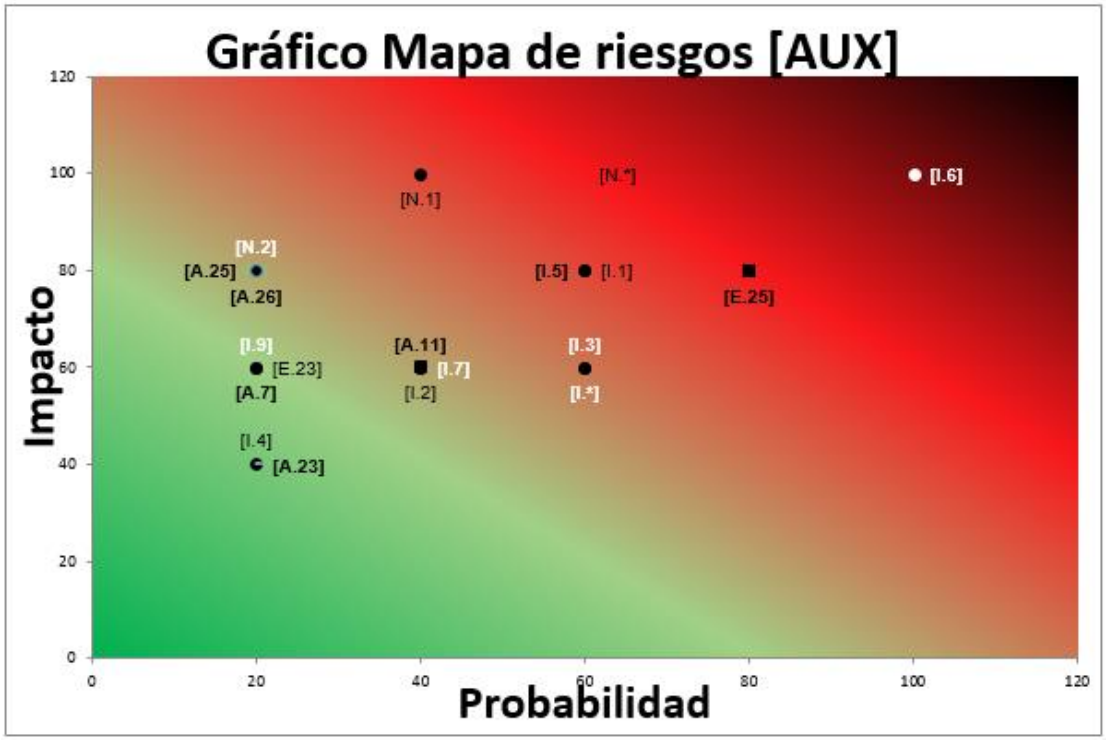


Gráfico Mapa de riesgos [AUX]
Impacto
Probabilidad
120
100
80
60
40
20
0
0
20
40
60
80
100
120
[N.1]
[N.*]
[I.6]
[N.2]
[A.25]
[A.26]
[I.5]
[I.1]
[E.25]
[I.9]
[E.23]
[A.7]
[A.11]
[I.7]
[I.2]
[I.3]
[I.*]
[I.4]
[A.23]

ACTIVOS	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
[L] Instalaciones	[N.1] Fuego	1- Sería excepcional	5–Catástrofe	Medio
	[N.2] Daños por agua	1- Sería excepcional	4–Grande	Bajo
	[N.*] Desastres naturales-Terremotos	1- Sería excepcional	5–Catástrofe	Medio
	[I.1] Fuego	2- Es raro que suceda	4–Grande	Medio
	[I.2] Daños por agua	2- Es raro que suceda	3–Moderado	Medio
	[I.*] Desastres industriales	1- Sería excepcional	4–Grande	Bajo
	[I.11] Emanaciones electromagnéticas	1- Sería excepcional	3–Moderado	Bajo
	[E.15] Alteración accidental de la información	1- Sería excepcional	3–Moderado	Bajo
	[E.18] Destrucción de información	1- Sería excepcional	3–Moderado	Bajo
	[E.19] Fugas de información	1- Sería excepcional	3–Moderado	Bajo
	[A.7] Uso no previsto	1- Sería excepcional	4–Grande	Bajo
	[A.11] Acceso no autorizado	1- Sería excepcional	5–Catástrofe	Medio
	[A.15] Modificación deliberada de la información	1- Sería excepcional	3–Moderado	Bajo
	[A.18] Destrucción de información	1- Sería excepcional	4–Grande	Bajo
	[A.19] Divulgación de información	1- Sería excepcional	2–Pequeño	Bajo
	[A.26] Ataque destructivo	1- Sería excepcional	5–Catástrofe	Medio
	[A.27] Ocupación enemiga	3- Es posible	4–Grande	**Alto**

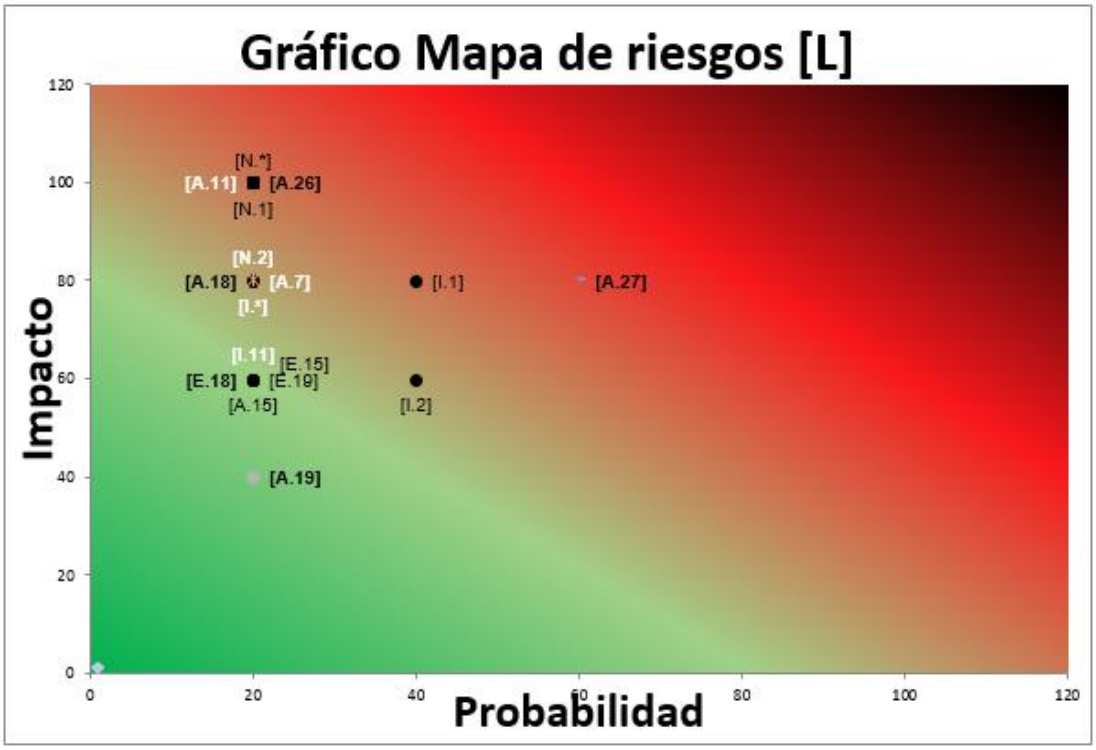
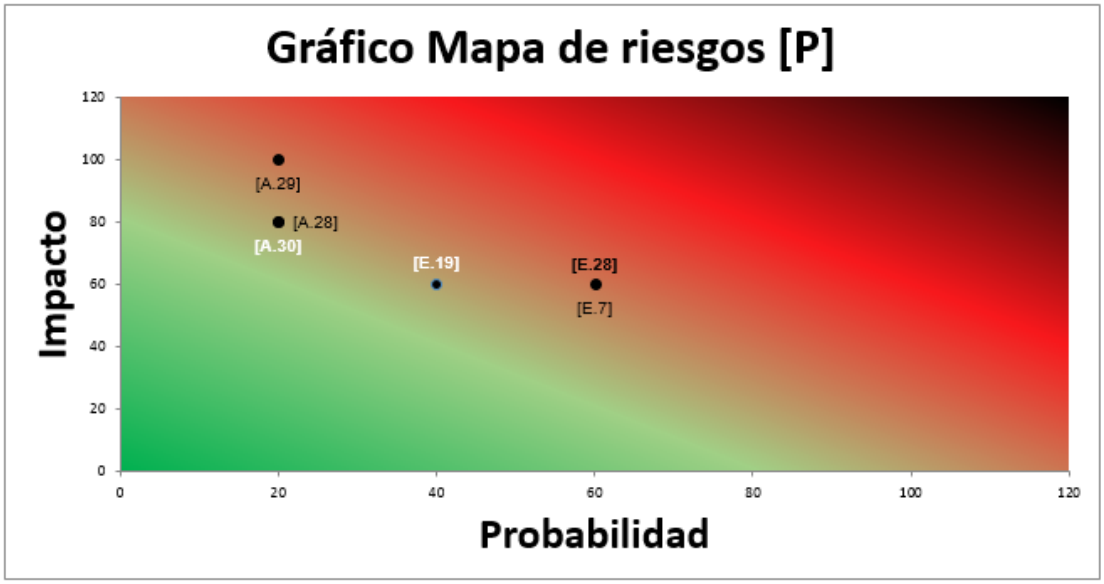


Gráfico Mapa de riesgos [L]
Impacto
Probabilidad
120
100
80
60
40
20
0
0
20
40
60
80
100
120
[N.*]
[A.11]
[A.26]
[N.1]
[N.2]
[A.18]
[A.7]
[I.1]
[A.27]
[I.*]
[I.11]
[E.15]
[E.18]
[E.19]
[A.15]
[I.2]
[A.19]

ACTIVOS	AMENAZA	PROBABILIDAD	IMPACTO	RIESGO
[P] Personal	[E.7] Deficiencias en la organización	3- Es posible	3–Moderado	Medio
	[E.19] Fugas de información	2- Es raro que suceda	3–Moderado	Medio
	[E.28] Indisponibilidad del personal	3- Es posible	3–Moderado	Medio
	[A.28] Indisponibilidad del personal	1- Sería excepcional	4–Grande	Bajo
	[A.29] Extorsión	1- Sería excepcional	5–Catástrofe	Medio
	[A.30] Ingeniería Social (picaresca)	1- Sería excepcional	4–Grande	Bajo



ANEXO E

LISTA DE PERSONAL QUE LABORA EN DST

Plan de Contingencia de la FIEC |Área: Departamento de Soporte Técnico| Vigencia: día/mes/año| Versión 1.0

EQUIPO DEL PLAN DE CONTINGENCIA INFORMÁTICO					
CÓDIGO:					
COORDINADOR DEL PLAN INFORMÁTICO					
Cargo del Funcionario		**ROL del Funcionario (PCI)**	**Teléfono**	**Celular**	**Dirección**
Analista de Infraestructura Informático 2		Coordinador			
MIEMBROS DEL EQUIPO					
Equipos	**Cargo del Funcionario**	**ROL del Funcionario (PCI)**	**Teléfono**	**Celular**	**Dirección**
Equipos de Redes y Comunicaciones	Asistente Técnico de Redes	Líder del Equipo			
	Asistente Técnico de Soporte	Ejecutor del Equipo			
Equipo de Desarrollo de Aplicaciones	Asistente Técnico de Desarrollo	Líder del Equipo			
	Webmaster	Ejecutor del Equipo			
Equipo de Soporte a Usuarios	Asistente Técnico de Soporte 2	Líder del Equipo			
	Asistente Técnico de Soporte 1	Ejecutor del Equipo			

ANEXO F

FIEC FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN	**INFORMACIÓN DE CONTACTOS EXTERNOS**	DST FIEC Nuestras Soluciones son Innovadoras
Plan de Contingencia de la FIEC | Área: Departamento de Soporte Técnico| Vigencia: día/mes/año| Versión 1.0		

CÓDIGO	**DST-PCI**		
Empresa	GTySI	**Servicio**	Infraestructura y Tecnologías de la Información
Teléfono	+593 4 2269 246		
Dirección	Km 30,5 Vía Perimetral		
Nombre del Contacto	**EMAIL**	**Teléfono**	**Celular**

ANEXO G

PROCEDIMIENTO PARA RECUPERACIÓN EN CASO DE INTERRUPCIÓN DEL SERVICIO		
Plan de Contingencia de la FIEC |Área: Departamento de Soporte Técnico|Vigencia: día/mes/año|Versión 10		
INFORMACIÓN RELEVANTE		
CÓDIGO		
NOMBRE DE LA CONTINGENCIA		
FUENTES DE RIESGO	**ESTIMACIÓN DE RIESGO**	
Hardware Software Equipos Auxiliares Instalaciones		
EQUIPO DE RECUPERACIÓN		
Nombre del Equipo		
MIEMBROS DEL EQUIPO		
No.	**Principal**	**Suplente**
1		
2		
DESCRIPCIÓN DE ACTIVIDADES		
1.- Aviso de activación del plan de contingencia por parte del CPCI.		
2.- El CPCI comunica a cada uno de los lideres de los equipos de recuperación.		
3.- Si el sistema se encuentra funcionando parcialmente se procede a suspender el servicio y se realiza las respectivas copias de seguridad.		
4.- El líder de los equipos de recuperación ejecuta los pasos para recuperación del sistema de información o equipos informáticos.		
5.- Líderes de los equipos deben consultar con personal de centro de cómputo del sitio alterno para ponerlo en marcha.		
6.- Instalación y configuración de los equipos de cómputo y hardware necesario para poner en marcha los equipos de comunicaciones para que de esta manera los sistemas de información puedan funcionar.		
7.- Instalación y configuración de los sistemas de información y el motor de la base de datos, con sus respectivas librerías y niveles de seguridad para las aplicaciones críticas.		
8.- Realizar configuraciones adicionales necesarias para el funcionamiento de los sistemas de información.		
9.- Proceder con la restauración de las base de datos con la última copia de seguridad disponible.		
10.- Reiniciación del servicio, prueba y afinamiento del sistema de información antes de la puesta en producción.		
11.- Si el equipo de cómputo no requiere cambiarse por fallas técnicas de hardware y se cuenta con una copia del disco duro, es necesario restaurar la copia de seguridad, para verificar funcionamiento de los sistemas de información.		
OBSERVACIONES		

ANEXO H

LISTA DE SISTEMAS DE INFORMACIÓN ACTIVOS

Nivel	Nombre del Sistema	Lenguaje de Desarrollo	Procesos y Áreas	Equipamiento	Equipamiento Mínimo	Actividades de Restauración

ANEXO I

LIBRO DE CONTROL DE BACKUPS

No.	Fecha	Sistema de Información	Período	Responsable que lo realizó
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				

ANEXO J

LIBRO DE REGISTRO DE CONTINGENCIAS

No.	Fecha de Ocurrencia	Hora de Ocurrencia	Tipo de Incidente	Sistema de Información	Procedimiento Aplicado	Resultado/ Estado	Fecha de Solución	Hora de Solución	Funcionario que lo Reporta

ANEXO K

FIEC FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN	**ESTADO DEL ACTIVO INFORMÁTICO**	DST FIEC Nuestras Soluciones son Innovadoras
Plan de Contingencia de la FIEC |Área: Departamento de Soporte Técnico| Vigencia: día/mes/año| Versión 1.0		

CÓDIGO			
TIPO DE INCIDENTE:		**LUGAR DEL INCIDENTE:**	
NOMBRE DE QUIÉN LLENA REPORTE:			

ESTADO	*CONDICIÓN	TIEMPO RECUPERACIÓN	COMENTARIOS

***CONDICIÓN**	ND -> No dañado DPU-> Dañado pero utilizable DR-> Dañado requiere reparación antes de usar D-> Dañado

_____

FIRMA

ANEXO L

LISTA DE VERIFICACION PLAN DE CONTINGENCIA

N°	ACTIVIDAD	RESULTADO	SI	NO	OBSERVACIONES
1	Realizar copias de seguridad de la información y documentos de los discos duros de los computadores del personal del DST. (Documentos en formatos Word, Excel, PDF y correos electrónicos)	Se encuentra disponible una copia de seguridad anual de los archivos en un dispositivo portable de alta capacidad. Cierta información del personal se encuentra disponible en la nube.			
2	Realizar copias de seguridad de los sistemas de información y bases de datos de los Servidores Críticos que albergan las aplicaciones web que administra el DST.	Se encuentra disponible una copia de seguridad semanal en cinta o disco duro o en la nube de los siguientes sistemas. 1. Controlac 2. Página Web de la FIEC 3. Aplicación para la Recepción de Artículos (ARA) 4. Sistema de Reuniones FIEC 5. Correos FIEC 6. ControlPC, etc.			
3	Contar mínimo con manuales de instalación para restaurar los archivos del sistema operativo y aplicaciones de un de servidores en caso de falla o virus.	Se encuentra disponible manuales de instalación para cada uno de los siguientes equipos del DST. Revisar inventarios de equipos informáticos disponibles y listos para su uso. El área de sistema tiene disponible una copia o el original del CD de instalación.			

4	Mantener descentralizados los sistemas de información del DST.	El DST mantiene las aplicaciones instaladas en diferentes localizaciones físicas, computadores o servidores.			
5	Mantener garantías vigentes de equipos críticos, asegurándolos contra incendios, robo o daños de fábrica	La FIEC cuenta con garantías vigentes contra todo riesgo de daño y/o pérdida física por cualquier causa.			
6	Mantenimientos, revisiones preventivas y correctivas de equipos de computación y comunicación, extintores, alarmas y sistemas contra incendio, para mantenerlos en óptimas condiciones.	EL DST cuenta con un plan de mantenimiento y contratos de mantenimientos vigentes para los equipos de cómputo y sistemas contra incendios de la FIEC.			
7	Actualizar las claves o contraseña de acceso a las aplicaciones y bases de datos de la FIEC, de acuerdo a revisión previa por parte del personal del DST.	Verificación de las políticas de acceso sobre la actualización anual de claves para todos los sistemas de información de la facultad.			
8	Mantener actualizados los sistemas operativos, antivirus y aplicaciones de la FIEC.	Verificación de las últimas actualizaciones de los sistemas operativos y antivirus en los sistemas de información.			
9	Mantener los equipos en condiciones ambientales óptimas de tal forma que no se deterioren por uso inadecuado.	Verificación de los equipos que se encuentran en los cuartos de rack que posean un lugar con condiciones ambientales adecuadas para su normal funcionamiento y cuente con sistemas de seguridad de acceso.			
10	Mantener como respaldo un inventario adicional con equipos de cómputo, repuestos, consumibles, para su reemplazo inmediato en	Verificación que equipos y repuestos de respaldo en bodega.			

	caso de falla.				
11	Disponibilidad de redundancia de recursos para evitar la interrupción de la prestación del servicio en los sistemas de información de la facultad	Verificación de equipos de infraestructura que cumplan con el concepto de redundancia n+1.			

NOTA: El presente modelo es un ejemplo, y se pueden modificar o adicionar actividades de ser necesario.

ANEXO M

FIEC FACULTAD DE INGENIERÍA EN ELECTRICIDAD Y COMPUTACIÓN	**EVALUAR RESULTADOS DEL PCI**	DST FIEC Nuestras Soluciones son Innovadoras
Plan de Contingencia de la FIEC | Área: Departamento de Soporte Técnico| Vigencia: día/mes/año| Versión 1.0		

CÓDIGO	**DST-PCI-001**		
TIPO DE INCIDENTE:		**LUGAR DEL INCIDENTE:**	
NOMBRE DE QUIÉN LLENA REPORTE:			

Descripción de Acciones	Funcionó (SI/NO)	Como mejorar