ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"DESARROLLO E IMPLANTACIÓN DE UN PLAN DE CONTINGENCIA INFORMÁTICA PARA LA DIRECCIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN DE LA PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR SEDE SANTO DOMINGO"

TESIS DE GRADO

Previo a la obtención del título de

MAGISTER EN SEGURIDAD INFORMÁTICA APLICADA

Franklin Andrés Carrasco Ramírez

Guayaquil – Ecuador

2015

AGRADECIMIENTO

A Dios, por ayudarme a pensar con claridad, cuando las esperanzas se quieren derrumbar ante los obstáculos que llegan a la vida, y por aquellas bendiciones recibidas que cambiaron mi horizonte.

A mi familia, sin su apoyo incondicional no llegaría tan lejos.

A mi Director Mg. Fausto Correa, y profesionales que estuvieron presentes con su guía, tiempo, y conocimiento. A la Pontificia Universidad Católica del Ecuador Sede Santo Domingo, por brindarme las facilidades para el desarrollo del proyecto.

DEDICATORIA

Para mi hijo, quien desde su llegada al mundo me ha entregado su alegría y me ha enseñado que su compañía la tendré hasta el infinito y más allá.

A mi esposa, por su amor, dedicación y compañía en la lucha de cada día al caminar juntos en esta larga vía de la superación.

A mi bebé, ya te quiero conocer.

TRIBUNAL DE SUSTENTACIÓN

Ing. Lenin Freire

DIRECTOR MSIA

Mg. Fausto Correa

DIRECTOR

Mg. Rocky Barbosa

MIEMBRO PRINCIPAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis, me corresponde exclusivamente; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral“

Franklin Carraco Ramírez

RESUMEN

En el presente proyecto se desarrolla un Plan de Contingencia Informática para la Dirección de Tecnología de la Información de la Pontificia Universidad Católica del Ecuador Sede Santo Domingo. El primer capítulo describe la naturaleza de la universidad, y la problemática o riesgos informáticos que pueden ser controlados con soluciones preventivas/correctivas; determinando así el objetivo general y objetivos específicos para el alcance del proyecto.

El segundo capítulo, explica las referencias bibliográficas que sustentan el desarrollo del proyecto, generando un conocimiento previo de las temáticas expuestas. En el tercer capítulo se describen las unidades que conforman el Departamento de Tecnología de la Información, así como el inventario tecnológico que posee la Universidad, presentando el levantamiento inicial de la información.

En el cuarto capítulo se realiza el análisis informático de la Sede, que define el alcance tecnológico del Plan, desarrollado bajo la metodología Magerit. En el quinto capítulo se desarrolla el Plan de Contingencia Informática, de acuerdo a las especificaciones indicadas en la metodología Magerit y la herramienta PILAR, determinando los principales activos tecnológicos, sus dependencias, amenazas, riesgo, niveles de impacto y salvaguardas que se deben aplicar, terminando con las actividades de contingencia para situaciones de alto riesgo.

El sexto capítulo termina con la propuesta de capacitación, pruebas, e implantación del Plan de Contingencia Informática en la universidad, con la finalidad de implantar un esquema de seguridad, y generando una conciencia informática entre los integrantes de la comunidad universitaria.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

AP	Access Point (Punto de Acceso)
BCP	Business Continuity Plan (Plan de Continuidad del Negocio)
BIA	Business Impact Analysis (Análisis de Impacto al Negocio)
CITIC	Centro de Investigación de Tecnologías de la Información y Comunicación
COOP	Continuity Of Operations Planning (Plan de Continuidad de Operaciones)
DHCP	Dynamic Host Configuration Protocol (Protocolo de Configuración Dinámica de Host)
DNS	Domain Name System (Sistema de Nombres de Dominio)
DRP	Disaster Recovery Plan (Plan de Recuperación ante Desastres)
DTI	Dirección de Tecnologías de la Información
HW	Hardware
IDS	Intrusion Detection System (Sistema de Detección de Intrusos)
IEC	International Electrotechnical Commission (Comisión Electrotécnica Internacional)
IPS	Intrusion Prevention System (Sistema de prevención de intrusos)

ISACA	Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información)
ISO	International Organization for Standardization (Organización Internacional de Normalización)
LAN	Local Area Network (Red de Área Local)
NAT	Network Address Translation (Traducción de Direcciones de Red)
NIST	National Institute of Standards and Technology (Instituto Nacional de Estándares y Tecnología)
PAT	Port Address Translation (Traducción de Puertos de Red)
PILAR	Procedimiento Informático Lógico para el Análisis de Riesgos
PUCE SD	Pontificia Universidad Católica del Ecuador Sede Santo Domingo
RPO	Recovery Point objective (Punto Objetivo de Recuperación)
RTO	Recovery time objective (Tiempo Objetivo de Recuperación)
SAI	Sistema de Alimentación ininterrumpida
SW	Software - Aplicaciones
TI	Tecnologías de la Información
UTP	Unshielded Twisted Pair (Par trenzado sin blindaje)
VLAN	Virtual LAN (Red de Área Local Virtual)
WLAN	Wireless Local Area Network (Red de Área Local Inalámbrica)

ÍNDICE DE FIGURAS

ÍNDICE TABLAS

INTRODUCCIÓN

La tecnología es un complemento necesario para el rápido desarrollo de tareas o actividades en una institución; y aunque con su implantación se trate de reemplazar el trabajo humano, estas estarán siempre expuestas a incidentes que afectarán su desempeño, provocando daños que pueden perjudicar a las empresas. El empleo de servicios y sistemas informáticos condiciona a las compañías a disponer de equipos tecnológicos con altas capacidades de procesamiento, almacenamiento y comunicación, manteniendo su funcionalidad bajo la demanda requerida por los usuarios.

Las instituciones de educación como las universidades, aprovechan la tecnología para automatizar sus procesos tanto en el ámbito administrativo, como el académico; es así, que para mantener la disponibilidad de los servicios informáticos, se emplean sistemas de monitoreo que arrojan alertas informativas permitiendo a los técnicos de Tecnologías de la Información ejecutar un conjunto de actividades preventivas, o correctivas, dependiendo de la amenaza. Y cuando la materialización de una amenaza supera los controles preventivos, llegando a presentar altos niveles de daños, es

necesaria la aplicación de procedimientos de contingencia que permitan reestablecer la continuidad de los servicios en cortos lapsos de tiempo.

Los procedimientos de contingencia son un recurso significativo para resguardar los activos más importantes de una institución, entre estos la información. Para asegurar que estos procedimientos se ejecuten correctamente, se requiere de un Plan de Contingencia Informático, cuyo objetivo es el disponer de un conjunto de actividades que permitan restaurar los procesos y servicios de la entidad, sin afectar gravemente la continuidad de sus operaciones. La ejecución del plan será exitosa, si de forma anticipada se realizan pruebas rigurosas, en las cuales el personal de tecnologías de la información logre alcanzar el conocimiento y la experiencia previa, para actuar frente a posibles riesgos.

El Plan de Contingencia Informática es una solución significativa y multidisciplinaria, que permite a las empresas mantener o recuperar las actividades del negocio en cortos lapsos de tiempo, resguardando la información y los activos tecnológicos primordiales.

CAPÍTULO 1

GENERALIDADES

1.1. Antecedentes

La Pontificia Universidad Católica del Ecuador Sede Santo Domingo (PUCESD) es una institución de Educación Superior, fundada en el año de 1996 en la ciudad de Santo Domingo, provincia Santo Domingo de los Tsáchilas; forma parte del Sistema Nacional PUCE, conformado también por las Sedes en Quito, Ibarra, Esmeraldas, Ambato y Manabí, los cuales buscan extender los servicios de educación superior en el país, con el fin de atender con calidad las demandas de formación superior.

Desde sus inicios la Sede Santo Domingo se mantiene en constante desarrollo, lo cual ha generado considerables cambios administrativos, académicos y tecnológicos, este último afectado constantemente por la automatización de procesos, creación de servicios y movimiento del personal técnico. La universidad inicialmente sostuvo sus recursos informáticos a través del Departamento de Computación, el cual cumplía con la tarea de dar soporte técnico a usuarios, mantenimiento en equipos de cómputo, mantenimiento a sistemas informáticos y apoyo a eventos o actividades especiales.

Con el crecimiento de la institución y la demanda de estudiantes, este departamento cambió su alcance al de Centro de Investigación de Tecnologías de la Información y Comunicación (CITIC), conformado con las subunidades de Soporte Técnico, Programación y Redes (telecomunicaciones), cuyas funciones eran las de mantener y dar soporte a la infraestructura tecnológica de la universidad como son: equipos de comunicación, computadores, servicios y sistemas informáticos.

La investigación y el vínculo con la comunidad a través de servicios de TI, eran dos de las principales actividades que realizaba el CITIC, sin embargo ante las nuevas exigencias sobre la educación superior, además de la organización y definición de funciones en el personal administrativo y académico de la universidad, este departamento nuevamente cambió su alcance al de Dirección de Tecnologías de la Información (DTI).

La DTI reestructura sus actividades de gestión con la finalidad de generar Gobernanza en TI, fomentando la disponibilidad, integridad, y confidencialidad de los servicios y sistemas informáticos, ante la demanda de usuarios, vulnerabilidades informáticas y nuevas tendencias en tecnología de la información y comunicación.

El departamento mantiene las mismas subunidades del CITIC, pero con funciones asociadas a la seguridad de los datos, así como la estabilidad en los procesos de negocio de la institución; y por tales motivos se ha

autorizado la propuesta para la creación de un Plan de Contingencia Informática, cuyas actividades a corto plazo permitan la sostenibilidad de los procesos más críticos de la universidad. El organigrama actual de la DTI se presenta en la Figura 1.1.

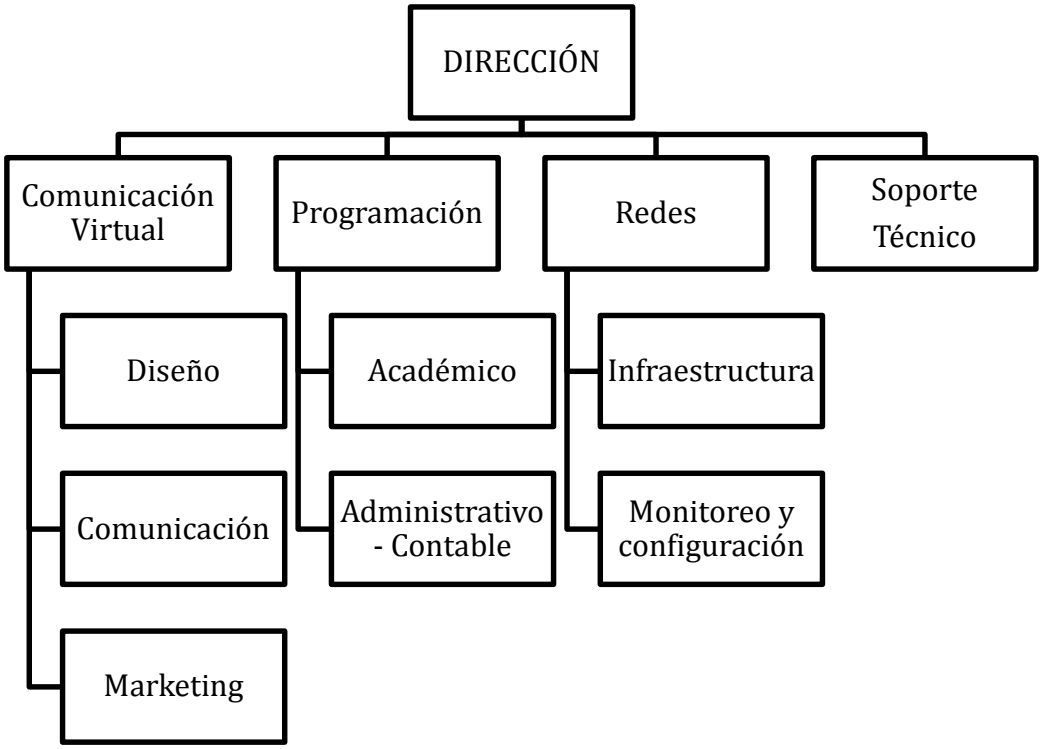

Figura 1.1: Organigrama Dirección de Tecnologías de la Información
Elaborado: Ing. Franklin Carrasco

1.2. Descripción del problema

En la actualidad la universidad se expone a riesgos informáticos que causan la pérdida de información, especialmente en los servicios de comunicación y sistemas informáticos. Los sistemas de información que posee la institución como son: servidores, equipos de comunicación, sistemas y servicios informáticos, servicios de comunicación, entre otros, son administrados por la Dirección de Tecnologías de la Información, cuyo personal no cuenta con procesos formales que eviten la paralización de sus operaciones y puedan activarse sin generar en la mayoría de casos conflictos o retrasos.

En ciertas ocasiones, fenómenos atmosféricos y eléctricos tales como, lluvias, tormentas, y rayos, han provocado situaciones críticas en la institución que involucraron pérdida de equipos de comunicación, computadores de escritorio, reguladores de energía, y puntos de acceso inalámbrico, creando un corte en los servicios de tecnología, afectando a las diversas áreas de la universidad.

En dichas situaciones críticas se ha logrado habilitar los principales servicios informáticos mediante la redistribución de los equipos que no se vieron afectaron con el incidente. Estos hechos han generado retrasos laborales en varias unidades, hasta concretar la adquisición, configuración e implantación de los activos siniestrados. Ante esto se pueden evidenciar varias problemáticas que generan pérdida económica y de tiempo en la actividad de la universidad, tales como:

- Frecuentes cortes de energía eléctrica que afectan a la tanto en los servidores de los sistemas informáticos académico y financiero, como en los equipos que interconectan la LAN de la Sede, entre ellos switches y router.

- Problemas de inconsistencia de datos por cambios realizados en los procesos programados sobre el código fuente de los sistemas informáticos financiero y académico, requeridos durante periodos de mayor afluencia de clientes.

- Detención de operaciones en los sistemas informáticos financiero y académico por:

    - Pérdida de conexión Cliente/Servidor a causa de fallas en equipos activos de comunicación o red de datos cableada.

- Retraso y dificultad en el levantamiento de los servidores de producción por inexistencia de servidores de respaldo y falta de procedimientos para su reactivación.

- Capacidad de almacenamiento y procesamiento limitado en los servidores de producción.

- Inexistencia de procedimientos o políticas que resguarden y aseguren el manejo de la información.

- Personal no capacitado en la instalación, configuración y manejo de la infraestructura tecnológica que posee la universidad.

- Pérdida de energía eléctrica en el Campus de la Universidad.

- Falta de procedimientos formales y asignación de responsabilidades para el personal de TI durante una eventualidad crítica.

- Acceso no autorizado de usuarios en la red LAN de la universidad, provocando retardo en la comunicación, robo de información y colapso en los equipos de comunicación.

La problemática expuesta afecta de forma directa a la continuidad de los servicios informáticos de la universidad, además presenta riesgos como la pérdida de información que es un activo irreparable.

1.3. Solución propuesta

Para garantizar la disponibilidad de los servicios informáticos que requiere la universidad, es necesario contar con un plan de contingencia informática ante eventualidades. El Plan de Contingencia Informática es una herramienta programada para actuar ante eventos inesperados, que afectan la continuidad de los procesos de la empresa. Para su desarrollo se emplea la metodología Magerit versión 3.0, que está asociada a los estándares ISO/IEC 27002:2005, e ISO/IEC 27002:2005:2013 asociados con la seguridad de la información y técnicas de seguridad.

Al desarrollar e implantar un Plan de Contingencia Informática en la Dirección de Tecnologías de la Información de la Pontificia Universidad Católica del Ecuador Sede Santo Domingo, se determinarán estratégicamente los procesos a seguir y sus responsables directos, quienes actuarán ante riesgos claramente identificados que afectan directamente a la infraestructura tecnológica y la gestión de la institución; dejando sentado un precepto que permita contemplar un marco de trabajo periódico, bajo las buenas prácticas establecidas por la metodología Magerit. En la Tabla 1 se identifican los servicios informáticos que mantienen las unidades que conforman la DTI, los cuales permiten automatizar ciertos procesos de la institución:

Tabla 1: Catálogo de servicios básicos de la Dirección de Tecnologías de la Información

NO.	SERVICIO	DESCRIPCIÓN	RESPONSABLE OPERACIONAL
1	Sistema Académico	Servicio utilizado por Dirección Académica para la gestión en los procesos de tipo académico	Programación
2	Sistema Financiero	Servicio utilizado por Dirección Financiera para la gestión en los procesos de tipo financiero – contable	Programación
3	Sistema Nómina	Servicio utilizado por Recursos Humanos para la gestión en los procesos de nómina y administración del personal	Programación

4	Servicios Web	Servicio de comunicación para la publicación de información de la universidad a través de portales web y redes sociales	Comunicación Virtual
5	Soporte a Usuarios	Servicio de atención y apoyo a los usuarios ante eventualidades ocurridas durante su gestión en sus estaciones de trabajo	Soporte Técnico
6	Salas de Cómputo	Servicio utilizado por los estudiantes y docentes para el desarrollo de las clases de grado, posgrado y formación continua	Soporte Técnico
7	Internet	Servicio para acceso a páginas web y correo electrónico institucional, restringido al personal administrativo y limitado al personal docente y estudiantil de la universidad	Redes
8	Comunicaciones	Servicio de comunicación para enlaces de voz, video y datos a través de Internet	Redes
9	Data Center o Centro de Datos	Habitación para protección de hardware crítico de la universidad	Redes
10	Seguridad de Red	Sistema de protección ante acceso no restringidos y ataques contra la integridad informática de la universidad	Redes

Elaborado: Ing. Franklin Carrasco

El establecer actividades de corto plazo dentro del plan de contingencia, permitirá activar procesos inmediatos ante incidencias graves, evitando el riesgo del colapso de la universidad; además de intensificar y asegurar las operaciones, evitando retrasos en los procesos contable y académico, fortaleciendo el servicio al cliente y la rentabilidad económica.

A través del plan de contingencia se realizará un respectivo Análisis del Negocio, en este caso, la Pontificia Universidad Católica del Ecuador Sede Santo Domingo, enfocándose en aquellos aspectos que comprometen sus funciones; levantando información objetiva y completa permitiendo el desarrollo de un conocimiento profuso, para así poder determinar sus potenciales amenazas.

En el plan se identificarán los objetivos del negocio, así como aquellos procesos o actividades críticos que pueden interrumpirse al estar asociados a riesgos. Además se analizará su correspondiente impacto económico, y plazos máximos para la activación de la operatividad, para lo cual se realizará un Análisis de Riesgos, que permita identificar y analizar los diferentes factores de riesgo (amenazas) que podrían afectar a las actividades, activos y procesos de la institución. Los factores de riesgo se priorizarán de acuerdo a su nivel de vulnerabilidad, impacto, importancia y coste, logrando continuidad o minimizando el tiempo de interrupción de la universidad.

Ante el resultado obtenido se determinarán procesos o mecanismos de salvaguarda del tipo preventivo, para reducir una posible materialización de las amenazas. También se determinarán mecanismos restablecedores, que actuarán ante la activación de las amenazas. El Plan de Contingencia permitirá evaluar la frecuente ocurrencia de amenazas, su impacto y los costos que genera. Además de determinar el tiempo de recuperación para cada aplicación o servicio de acuerdo a su nivel de importancia para la universidad. Definidos los riesgos, su impacto y determinada la prioridad de activación de los sistemas informáticos o servicios de la universidad, se levantará una documentación referencial, que permitirá al personal técnico conocer su rol, procedimientos a seguir, y las unidades que deba necesariamente contactar.

Para verificar que el plan de contingencia posee la integridad funcional al poner en marcha una pronta recuperación, se realizarán pruebas ante los ambientes de riesgo previamente revisados, determinando posibles errores que deban corregirse.

Definido el plan, se realizarán reuniones de capacitación para el personal de TI y el personal administrativo. La universidad posee en su infraestructura tecnológica un conjunto de servidores, sistemas informáticos y equipos de comunicación, entre los cuales se identifica un grupo con un considerable nivel de criticidad, pues mantienen servicios académicos y administrativos, como se puede observar en la tabla 2.

Tabla 2: Inventario base de infraestructura Tecnológica de la Dirección de Tecnologías de la Información

INFRAESTRUCTURA	CANTIDAD
Servidores de Producción	16
Sistemas y Servicios Informáticos de Producción	11
Base de Datos	1 Oracle 1 SQL 8 MySQL 1 PostgreSQL
Equipos de comunicación en la red Interna (LAN)	33

Datos recogidos el 10 de enero del 2014
Elaborado: Ing. Franklin Carrasco

En el desarrollo del plan se determinará la capacidad tecnológica de la universidad frente a los procesos administrativos y académicos, permitiendo definir el nivel de riesgo e impactos de forma cualitativa. Se identificarán procesos y normas de seguridad a seguir, ante requerimientos que afectan directamente el manejo y almacenamiento de la información, ya sea en los sistemas informáticos de producción o en sus respectivas bases de datos. También presentará procesos inmediatos de constante actualización para mantener activa la red LAN y WLAN para comunicación de datos.

La implantación del plan de contingencia informática presentará una solución ordenada e inmediata sobre los riesgos internos y externos ocurridos en la universidad, permitiendo la pronta disponibilidad de los servicios, reduciendo así los costos de operación. Otros beneficios que el plan surtirá a la institución son: asegurar la continuidad y estabilidad de la universidad, proteger activos e información, definir responsabilidades del recurso humano de gestión, minimizar posibles pérdidas económicas, clasificar la infraestructura tecnológica, identificar los activos de mayor protección, y presentar respuestas inmediatas ante eventos inesperados.

El desarrollo del presente proyecto tiene la aceptación de la PhD. Margalida Font Roig, Prorrectora de la Pontificia Universidad Católica del Ecuador Sede Santo Domingo (Anexo 1).

1.4. Objetivo General

Desarrollar e implantar un Plan de Contingencia Informática para la Dirección de Tecnologías de la Información de la Pontificia Universidad Católica del Ecuador Sede Santo Domingo.

1.5. Objetivos Específicos

- Identificar la naturaleza del negocio y la metodología aplicable al desarrollo del Plan de Contingencia Informática
- Identificar los principales procesos de negocio, la infraestructura tecnológica implicada y los riegos asociados
- Desarrollar el Plan de Contingencia Informática

- Definir un marco de trabajo interdisciplinario, para la constante actualización del Plan de Contingencia Informática
- Verificar la aplicabilidad del Plan de Contingencia Informática mediante pruebas y análisis de resultados

CAPÍTULO 2

MARCO TEÓRICO

2.1. Seguridad Informática

Al mencionar "*seguridad*" y relacionarla con las operaciones de una empresa o institución, lleva a un común entendimiento en situaciones como: robo, daños físicos, privacidad (accesos a departamentos por personas no autorizadas), entre otros; dejando en ocasiones fuera de alcance el aseguramiento de la infraestructura tecnológica (hardware y software) y su bien de mayor importancia, la información.

Es evidente que definir un concepto para la seguridad de los recursos informáticos, requiere de un amplio alcance por los diversos recursos que le conforman; ante lo cual se puede definir como, “un conjunto de procedimientos, métodos, herramientas y técnicas, implementados para asegurar la integridad, confidencialidad y disponibilidad de la información, y por ende de los sistemas informáticos ante cualquier amenaza”. [1]

La seguridad informática no es un bien medible, en cambio se pueden emplear herramientas para cuantificar de alguna forma nuestra inseguridad informática. Cabe recalcar, aunque se apliquen las mayores medidas de seguridad a un sistema de información, este no dejará de tener un margen de riesgo. Al establecer medidas de seguridad es necesario determinar los elementos que conforman el sistema, los peligros que le afectan y las medidas que se deben adoptar para prevenir, reducir o controlar los riesgos potenciales. Al definir seguridad informática es necesario conocer los elementos que esta resguarda, como son los sistemas de información y los sistemas informáticos.

2.1.1. Sistemas de Información

Se define como un conjunto de elementos organizados, relacionados y coordinados entre sí, encargados de facilitar el funcionamiento global y cumplimiento de los objetivos de una empresa. [2].

Los elementos que componen un sistema de información se identifican como: Recursos, ya sean físicos (computadores, conexiones, periféricos) o lógicos (sistemas operativos, aplicaciones de software); Humanos, conformado por las personas que laboran en la institución; Información, conjunto de datos organizados y generados para el desenvolvimiento del negocio; y las Actividades, propias de la empresa relacionadas o no con la informática. [1]

2.1.2. Sistemas Informáticos

Se constituyen también como un conjunto de recursos físicos y lógicos, manipulados en la mayoría de ocasiones por entes humanos, quienes

se encargan de su manejo para la generación y resguardo de la información. Un Sistema Informático puede ser parte de un Sistema de Información, sin embargo, un Sistema de Información no necesariamente debe contener elementos informáticos.

2.1.3. Tipos de Seguridad

De acuerdo a las medidas de seguridad que pueden establecer las organizaciones, se identifican dos, el primero de tipo Activo, comprende las defensas en tiempo real para evitar o reducir riesgos (ataques o virus informáticos); y de tipo Pasivo, que es el conjunto de medidas o procedimientos a seguir una vez que se activa un incidente.

2.2. ¿Qué es un plan de contingencia?

En la década de los setenta Norman L. Harris, Edward S. Devlin y Judith Robey buscaban la manera de encontrar un método que evitara la

atención continua de los problemas inesperados (“apagar fuegos”), dando lugar al conocido Disaster Recovery Planning, que busca recuperar las operaciones de la empresa de desastres ya sean naturales o humanos. Esta planificación mantiene su aplicación, sin embargo esta actividad cambió su denominación a Contigency Plannning, que agrupa a más procesos que permiten a mitigar amenazas y la recuperación parcial o total de las operaciones del negocio.

El Instituto Nacional de Estándares y Tecnología de los Estados Unidos, define a un plan de contingencia como “una estrategia coordinada que involucra planes, procedimientos, y medidas técnicas que permiten la recuperación de los datos, las operaciones del negocio, y los sistemas de información, después de una interrupción:

- Restableciendo los sistemas de información empleando equipos de respaldo.
- Levantando todos o varios de los procesos de negocio afectados, usando procedimientos alternos (manuales - aceptables en interrupciones a corto plazo).

- Restableciendo las operaciones de los sistemas de información en una ubicación alterna (normalmente aceptables en interrupciones de larga duración o si se afectan físicamente las instalaciones).
- Implementado los controles apropiados de un plan de contingencia basados en el nivel de seguridad de los sistemas de información." [3].

Un similar concepto menciona el Instituto Nacional de Tecnologías de la Comunicación de España (INTECO): "Son servicios destinados a la realización de acciones y gestiones encaminadas a la recuperación de la actividad del negocio, en casos de que se produzcan incidentes de seguridad que afecten a la información y las tecnologías que los soportan, así como la continuidad de los mismos. Estos servicios persiguen reducir las consecuencias de un incidente de seguridad, incluso aquellos que ocasionen la interrupción de la actividad de la empresa con la consiguiente reducción de la incidencia en el negocio." [4].

Consolidando las mencionadas denominaciones se afirma al Plan de Contingencia como un conjunto de procedimientos y actividades validadas para restablecer las actividades de un negocio, que cuando al verse afectados los Sistemas de Información, su planificación se enfoca sobre la infraestructura y sistemas informáticos.

2.3. Otros tipos de planes

Para evitar confusiones respecto al alcance real y el propósito con otros tipos de planes, además de proporcionar una base de entendimiento común en relación a los Planes de contingencia y los Sistemas de Información, se definen otros planes con su propósito y alcance (puede variar de acuerdo al estándar).

2.3.1. Plan de Continuidad del Negocio (BCP)

El BCP permite a la empresa planificar con anticipación las actividades o procesos a seguir para asegurar que sus productos o servicios se siguen ofreciendo luego de un desastre. [5].

BCP se centra en el mantenimiento de los procesos o misión de la organización durante y después de una interrupción, estos pueden estar dirigidos para una unidad específica o para toda la organización e identificados de mayor a menor prioridad, por ejemplo, en un proceso para generación de nómina o procesos de servicio al cliente.

2.3.2. Plan de Continuidad de Operaciones (COOP)

COOP se centra en la restauración de las funciones esenciales basadas en la misión de la organización, en sitios alternos por un tiempo máximo de treinta días hasta recuperar sus operaciones normales. Funciones adicionales a nivel de oficina, pueden estar direccionados por un BCP.

Aquellas amenazas leves o interrupciones en las cuales no se requiera el traslado a un sitio alterno para la restauración de procesos no se abordan en el COOP. [3].

2.3.3. Plan de Comunicaciones Críticas

Es desarrollado por la organización encargada de la difusión pública, en este se designa al personal que se encargará de responder preguntas sobre la emergencia expuesta, como: estado del incidente, o reportes a prensa, sin enfocarse específicamente a información de los Sistemas de Información.

2.3.4. Plan de Recuperación de Desastres (DRP)

Para lograr la máxima recuperación del negocio en el menor tiempo posible, es necesario crear una guía que dirija a detalle las acciones a realizar antes, durante y después de un desastre. A esa guía se la

conoce como Plan de Recuperación de Desastres, un conjunto completo de declaraciones creadas para hacer frente a cualquier desastre que pudiera afectar al negocio, asegurando la continuidad de sus operaciones. [6].

2.4. Riesgos

Al nombrar la palabra “Riesgo”, lleva al entendimiento de la posibilidad de que se origine un contratiempo donde algo o alguien sufren un prejuicio o daño; asociando este concepto con la Tecnología informática de una organización – “Conjunto de los instrumentos y procedimientos industriales de un determinado sector o producto” [7] - se puede precisar lo siguiente: “Los riesgos de TI son un componente del universo de riesgos a los que está sometida una organización. Otro de los riesgos a los que una organización se enfrenta pueden ser riesgos estratégicos, riesgos ambientales, riesgos de mercado, riesgos de crédito, riesgos operativos y riesgos de cumplimiento. En muchas organizaciones, los riesgos relacionados con TI se consideran un componente de riesgo operativo” [8].

“Un riesgo de TI es también un riesgo del negocio, riesgos del negocio asociados con el uso, propiedad, operación, participación, la influencia y la adopción de las TI en una organización. Se compone de los eventos relacionados con TI que potencialmente podrían afectar el negocio. Este hecho puede ocurrir con una frecuencia y magnitud inciertas, y supone dificultades para alcanzar las metas y objetivos estratégicos” [8].

2.4.1. Riesgo Inherente

La dependencia de las empresas al uso (o falta de uso) de las tecnologías de la información han generado un nivel alto de riesgos que invaden a la intranquilidad de quienes mantienen la seguridad informática. ISACA haciendo mención de riesgos inherentes lo define como: “Nivel o exposición al riesgo sin tomar en cuenta las acciones que la dirección ha tomado o podría tomar (por ej., implementar controles)” [9]. Es decir el riesgo que se expone la empresa cuando no se han definido las medidas de control que reduzcan el impacto de su materialización.

2.4.2. Riesgo Residual

A pesar que una empresa mantenga los mayores procesos de control sobre sus operaciones bajo estándares internacionales y marcos de referencia, siempre quedarán expuestos riesgos mínimos que no se logran cubrir.

Estos riesgos son aquellos que aún persisten después de haberse aplicado los controles, mecanismos o estrategias de salvaguarda al riesgo inherente. La metodología Magerit define al riesgo residual: “Aquello que puede pasar, tomando en consideración las salvaguardas desplegadas; el riesgo se reduce a un nivel residual que la Dirección asume” [10].

Cada riesgo agrupa a una o varias amenazas ante las cuales se exponen los activos. Gestionar los riesgos es el punto inicial para la guía de un buen gobierno de TI, con el fin de afrontarlos y controlarlos,

minimizando su impacto hasta niveles aceptables, mediante mecanismos o estrategias de salvaguarda.

2.4.3. Gestión del Riesgo

Se lo define como “un proceso que incluye la prevención, detección y respuesta a los incidentes mantenimiento continuo, revisión y auditoria en cada una de las fases de Planear, Hacer, Chequear, y Actuar”. [11]. Gestionar al riesgo permite crear procedimientos coordinados para controlar y minimizar los efectos dañinos de una posible materialización de las amenazas, dejando a consideración de las autoridades de una institución la toma de decisiones para la aceptación del riesgo.

2.5. Amenazas

Se conoce a una amenaza del tipo informático, como aquella que de forma directa o indirecta afecta a los sistemas de información, generando

daños materiales o inmateriales a través de la explotación de sus vulnerabilidades. Los actores o causantes de las amenazas pueden ser internos o externos a la organización y pueden ser humanos o no humanos, también existen causantes como fallas naturales ocurridas por efectos de la naturaleza; ante esto se define a la amenaza como “Una causa potencial de un incidente no-deseado, el cual puede resultar en daño a un sistema y organización” [8].

La metodología Magerit versión tres, cataloga a las amenazas en cuatro grupos que son: desastres naturales, de origen industrial, errores y fallos no intencionados, y ataques intencionados. [10]. Cada activo tiene asociado un grupo de posibles amenazas las cuales se valoran por la probabilidad de ocurrencia y la degradación de la Disponibilidad, Integridad, y Confidencialidad, permitiendo el análisis para la gestión y determinación de las salvaguardas preventivas y correctivas identificadas dentro del plan de contingencia informática.

2.5.1. Impacto

Magerit denomina al Impacto como “la medida del daño sobre el activo, derivado de la materialización de una amenaza.” [10]. Es decir, el factor que da a conocer la capacidad de inversión económica que debe soportar una empresa para mantener sus actividades luego de una incidencia.

2.6. Análisis de Impacto de Negocios

El análisis de riesgos (y amenazas) es el punto de partida para determinar los procesos de mayor importancia en el funcionamiento del negocio, que da paso al análisis de impacto de negocio; IBM lo define como la identificación de procesos de negocio críticos que más afectan a los ingresos, activos y clientes, para ayudarle a asignar prioridades a las estrategias de recuperación que pudieran ser necesarias durante una interrupción prolongada de la actividad [12].

ITIL en su tercera versión, la denomina como “la actividad de la Gestión de la Continuidad del Negocio que identifica Funciones Vitales del Negocio y sus dependencias. Estas dependencias pueden incluir proveedores, personas, otros procesos del negocio, servicios TI, entre otros. BIA (Business Impact Analysis) define los requerimientos de recuperación para los servicios de TI. Dichos requerimientos incluyen Objetivos de Tiempo de Recuperación, Objetivos del Punto de Recuperación y los Objetos de Nivel de Servicio mínimos para cada Servicio de TI” [13].

Ante lo indicado se puede argumentar que a través del Análisis de Impacto de Negocio se identificarán los procesos, funciones y sistemas de información más críticos, evaluando a su vez el impacto económico de los incidentes y desastres resultantes de la pérdida de los sistemas, servicios, o instalaciones, como también se determina el tiempo máximo que puede la empresa mantenerse sin tener los sistemas, servicios o instalaciones activos.

2.7. Mecanismos o estrategias de salvaguarda

Las salvaguardas son medidas de protección que se aplican para reducir o evitar el impacto de la materialización de las amenazas. Se clasifican de acuerdo a la función que realizan, es decir preventivas y correctivas/restablecedoras. Las salvaguardas preventivas actúan sobre las vulnerabilidades de los activos, monitoreando o previniendo que las consecuencias de la materialización de una amenaza no afecten en un alto porcentaje a los procesos del negocio.

Las salvaguardas correctivas/restablecedoras se ejecutan durante la incidencia para reducir la gravedad de daños y poder restablecer los activos afectados. Estas salvaguardas son importantes para la realización del plan de contingencia informática. En definitiva las salvaguardas se definen como “todo control (política, procedimiento, norma, proceso o mecanismo) que contribuye a reducir las vulnerabilidades de los activos, reducir la probabilidad de que las amenazas puedan explotar vulnerabilidades, reducir el impacto producido en el negocio por la materialización de las amenazas.” [14].

CAPÍTULO 3

LEVANTAMIENTO DE INFORMACIÓN DE LA INFRAESTRUCTURA TECNOLÓGICA

3.1. Situación actual de la institución universitaria

Para dar inicio con el desarrollo del Plan de Contingencia Informática, es fundamental conocer la infraestructura tecnológica que soporta la universidad, así como las unidades que conforman la Dirección de Tecnología. A partir de esta visión inicial tecnológica, se podrán identificar a aquellos equipos expuestos a riesgos y que puedan afectar al desarrollo de los procesos del negocio.

La universidad mantiene la administración de su infraestructura tecnológica física y lógica a través de las unidades de Soporte Técnico, Programación y Redes, las mismas que conforman la Dirección de Tecnologías de la Información. Cada unidad sostiene los servicios como se describe en la Tabla 3:

Tabla 3: Unidades técnicas de la Dirección de Tecnologías de la Información y actividades de gestión

UNIDAD	ACTIVIDADES DE GESTIÓN
Soporte Técnico	• Soporte a Usuarios • Mantenimiento de computadoras • Mantenimiento y control en Salas de Cómputo • Instalación de Software • Inventario físico de computadoras • Control de Transferencias de computadoras
Programación	• Soporte y mantenimiento en Bases de datos y Sistemas Informáticos Institucionales • Desarrollo de Servicios y Sistemas Informáticos • Respaldo de Bases de Datos y Sistemas Informáticos Institucionales • Control de Usuarios en Sistemas Informáticos
Redes	• Control y administración de servidores • Soporte y mantenimiento a redes LAN y WLAN • Monitoreo de las redes LAN y WLAN • Control de accesos a la red • Inventario físico de equipos de comunicación en redes LAN y WLAN • Distribución de infraestructura de comunicación en redes LAN y WLAN

Datos recogidos el 15 de marzo del 2014
Elaborado: Ing. Franklin Carrasco

Los Sistemas Informáticos que sostiene la institución se mantienen en actividad de producción por un tiempo no mayor a diez años, llevando sobre estos, cambios concurrentes en su código fuente, alterando de manera continua sus procesos. Estos sistemas funcionan bajo el modelo Cliente – Servidor, centralizando la aplicación y los datos.

Cada sistema informático funciona sobre un equipo físico, ya sea con la infraestructura para servidor o computador de escritorio. Cuando se solicita el acceso de un usuario a los sistemas informáticos y su respectivo servidor, debe tener la aprobación de la dirección correspondiente; actualmente se mantienen los accesos como se presenta en la Tabla 4:

Tabla 4: Acceso de usuarios a Servidores de Producción

USUARIO	ACCESO
Técnico Programador	• Sistema Operativo • Base de Datos • Código Fuente • Respaldos de Base de Datos y Código Fuente • Sistemas Informáticos Institucionales
Técnico Redes	• Sistema Operativo
Secretarias	• Sistema Informático Institucional • Base de Datos (limitado)
Directores	• Sistema Informático Institucional • Base de Datos (limitado)

Fuente: PUCESD – Dirección de Tecnologías de la Información – Dirección
Elaborado: Ing. Franklin Carrasco

Los equipos servidores se encuentran alojados en un “Cuarto de datos y comunicación” que no mantiene el resguardo tecnológico requerido, su espacio se aclimata en frío con un aire acondicionado de fabricación para el hogar; la energía eléctrica alimenta directamente a todos los equipos activos, excepto al servidor que sostiene los sistemas informáticos de producción de mayor importancia, puesto que este se respalda mediante un Sistema de Alimentación ininterrumpida (SAI o UPS), en caso de existir un corte de la energía eléctrica, todos los equipos sin respaldo eléctrico se apagarán inmediatamente.

El acceso al cuarto frío es permitido únicamente para el personal técnico de la Dirección de Tecnologías de la Información y la Dirección de Recursos Físicos, estos últimos por la administración de la Central Telefónica.

El sitio también contiene equipos de comunicación de red para los niveles de Núcleo, Distribución y Acceso, como son: router, switch, controladora de la Wireless LAN, servidor proxy, servidor DHCP, Servidor Firewall, entre otros.

En la universidad existen tres medios para la comunicación de los datos, como son: enlaces de fibra óptica extendida desde el Cuarto de datos y comunicación hacia los edificios Administrativo, Académico y Salas de Cómputo; enlaces de cable UTP categoría 5e, 6 y 6a distribuidos en cada piso de los mencionados edificios; y el acceso inalámbrico a las redes abiertas para estudiantes, docentes e invitados. Cada piso de los edificios cuenta con un switch administrable simple o

en stack de acuerdo al número de usuarios de la zona. En la Figura 3.1 se presenta el mapa físico de la actual red LAN:

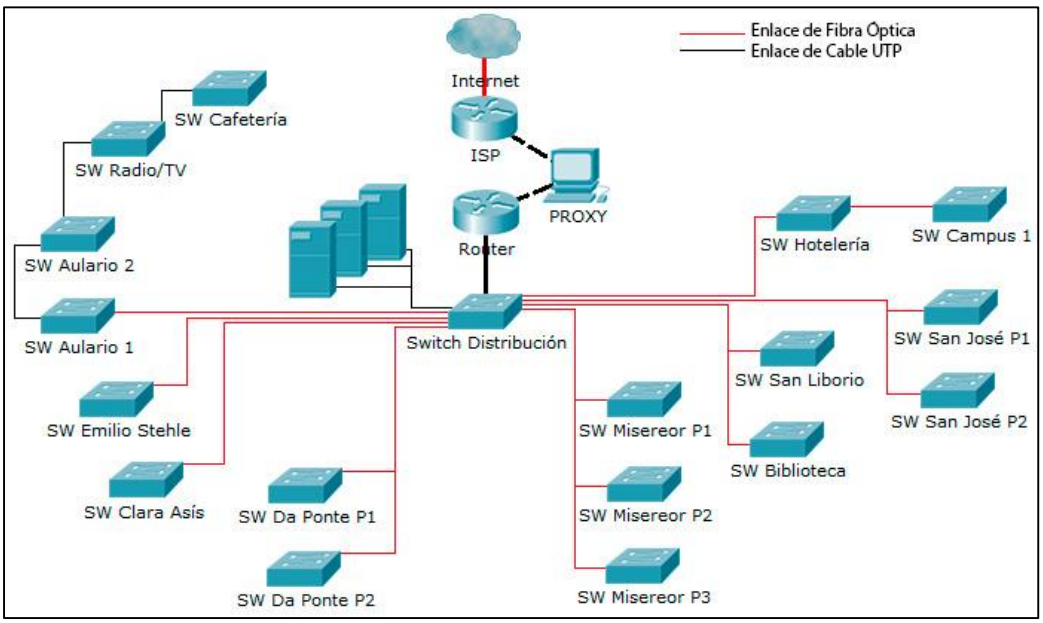

Figura 3.1: Distribución de red LAN - Campus 2 PUCESD
Fuente: PUCESD – Dirección de Tecnologías de la Información – Unidad de Redes
Elaborado: Ing. Franklin Carrasco

La comunidad universitaria la conforman: personal administrativo, académico y estudiantes, distribuidos en direcciones, coordinaciones, y equipos de apoyo, quienes acceden a la red de datos e internet de acuerdo a la función que desempeñan, dispuestos a un segmento de red mediante la implantación de VLANs (Redes de Área Local Virtual),

mencionando las siguientes: Administrativos, Docentes, Internet, Salas de cómputo, Estudiantes, Invitados, Biblioteca. En la Figura 3.2, se identifica el Organigrama Estructural de la PUCESD:

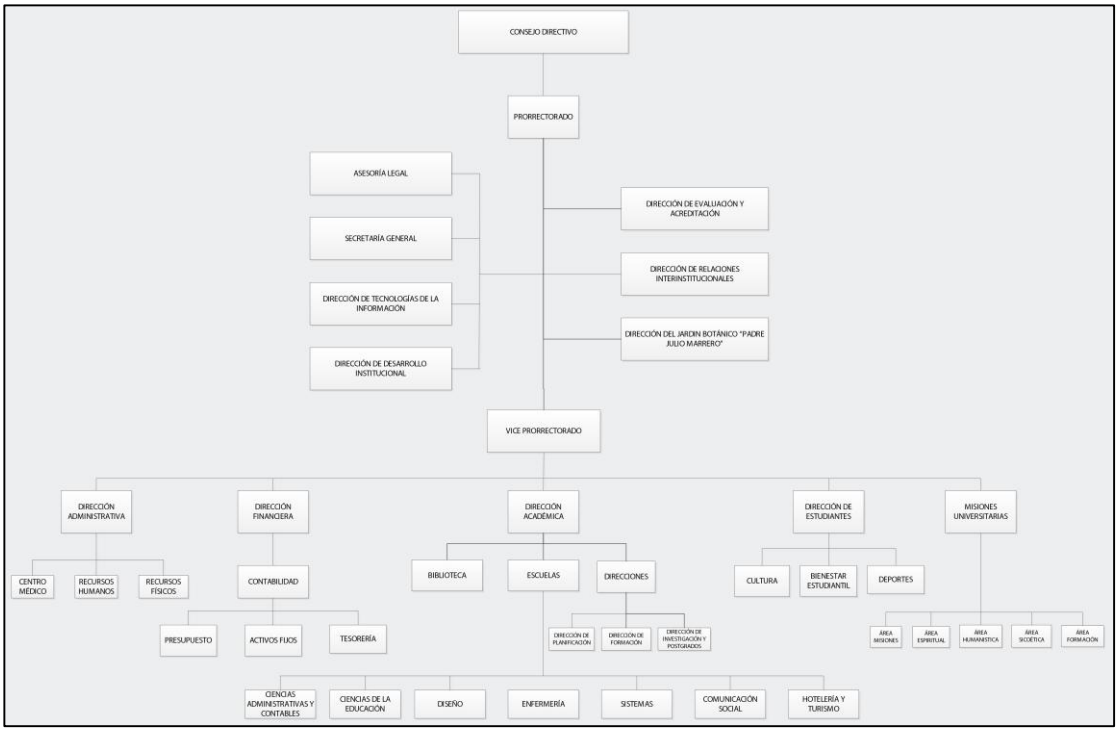

Figura 3.2: Organigrama Estructural
Fuente: Página web PUCESD – http://www.pucesd.edu.ec/index.php/organigrama_estructural.html

3.2. Objetivos institucionales vinculados a la tecnología

Dentro de los Objetivos del Plan Estratégico de Desarrollo Institucional que impulsa la universidad, procura mejorar la calidad de los procesos

administrativos y capacidad cognoscitiva en la academia, mediante la aplicación constante de tecnologías de la información; los objetivos que demuestran esta vinculación son:

Tabla 5: Objetivos PEDI PUCESD vinculados a la tecnología de la información

Objetivo 2	Capacitar a la Comunidad Universitaria en competencias específicas
Objetivo 4	Actualizar Tecnológicamente las Herramientas de Gestión Académica y Administrativa
Objetivo 5	Implementar una infraestructura especializada para el mejoramiento de la gestión e investigación en la Sede

Fuente: Página web PUCESD
http://www.pucesd.edu.ec/images/files/normativas_legislacion/PEDI_2011_2014.pdf

La base de la institución es la educación formada desde los valores del Evangelio bajo el aval del Pontificado, dando la importancia de describir la Misión y Visión que posee la universidad:

VISIÓN

- Formadora, desde el Evangelio, de personas con un profundo sentido ético y profesional

- Una Sede universitaria sólida y posicionada en la Provincia
- Promotora del desarrollo económico-social y cultural de la Provincia

MISIÓN

La Pontificia Universidad Católica del Ecuador, Sede Santo Domingo (PUCE SD), es una sede universitaria integrante del SINAPUCE, que desarrolla el conocimiento con aperturidad, veracidad, rigurosidad y sentido crítico, en sus diferentes expresiones y disciplinas, desde la vivencia de la fe católica como auténtica comunidad caracterizada por los más altos valores, para promover la formación integral de la persona y una sociedad plenamente humana.

3.3. Inventario de infraestructura tecnológica custodiada por la unidad redes

La unidad de redes mantiene la disponibilidad, integridad y confidencialidad de los datos que viajan a través de las redes LAN y WLAN de la

universidad, como también brindan soporte a los departamentos que informen problemas de conexión ya sea física o lógica, entre las actividades que poseen se mencionan:

- Instalación, actualización y administración de Servidores
- Instalación, administración y monitoreo de redes LAN y WLAN
- Aseguramiento de accesos en las redes LAN y WLAN
- Segmentación de red mediante VLAN
- Distribución de ancho de banda
- Control de acceso a redes inalámbricas mediante autenticación
- Implantación e instalación de servicios e infraestructura de red
- Seguridad perimetral
- Soporte a usuarios
- Mantenimiento de equipos activos de red, y servidores
- Control de incidencias sobre equipos activos de red y servidores
- Desarrollo de proyectos para seguridad y soporte de la red

La infraestructura tecnológica empleada en la universidad para la comunicación de datos está conformada por switches, routers, puntos de acceso inalámbrico, y servidores, establecidos para la comunicación de la red. En las Tablas 6, 7, y 8 se observa la distribución de los equipos activos en cada edificio y la función que desempeñan.

Tabla 6: Inventario de equipos para comunicación de red LAN, edificios San José, Misereor, San Liborio

EDIFICIO	UBICACIÓN/ CANTIDAD	EQUIPO ACTIVO	ENLACE	SERVICIO DEL ACTIVO	DEPARTAMENTOS / UNIDADES
San José	Piso 1 2 equipos	Switch CISCO Catalyst 2960	UTP FIBRA	Académico/Contable Internet Vigilancia	Información Secretarías de Escuela, Formación Continua, de Investigación Secretaría General Tesorería Direcciones de Escuela Salas de Profesores
	Piso 2 1 equipo	Switch CISCO Catalyst 2960	UTP FIBRA	Académico/Contable Internet Vigilancia	Dirección Académica Dirección Planificación Dirección Investigación Dirección Formación continua Dirección Jardín Botánico
Misereor	Piso 1 1 equipo	Switch CISCO Catalyst 2960	UTP FIBRA	Internet	Centro Médico Sala de Profesores
	Piso 2 1 equipo		UTP FIBRA	Académico/Contable Internet	Dirección Administrativa Recursos Humanos
	Piso 3 1 equipo		UTP FIBRA	Académico/Contable Internet Vigilancia	Dirección Financiera

San Liborio	Piso 1 2 equipos	Switch CISCO Catalyst 2960	UTP	Internet	Biblioteca
		Switch PoE Dlink 1008P	UTP	Vigilancia	

Fuente: PUCESD – Dirección de Tecnologías de la Información – Unidad de Redes
Elaborado: Ing. Franklin Carrasco

Tabla 7: Inventario de equipos para comunicación de red LAN, edificios San Liborio, Clara de Asís, Da Ponte

EDIFICIO	UBICACIÓN/ CANTIDAD	EQUIPO ACTIVO	ENLACE	SERVICIO DEL ACTIVO	DEPARTAMENTOS / UNIDADES
San Liborio	Piso 2 7 equipos	Switch CISCO Catalyst 2960	UTP FIBRA	Internet	Prorrectorado Viceprorrectorado Relaciones Interinstitucionales Evaluación y Acreditación Desarrollo Institucional Asesoría Legal Psicoética Sala Docentes
		Switch CISCO Catalyst 2960	UTP FIBRA	Conexión red LAN hacia edificios Wireless LAN Controler Servidores	DTI - Cuarto de Control
		Switch TRENDNET	UTP	Servidores Router ISP	DTI - Cuarto de Control
		ROUTER CISCO 2800	UTP	Enrutamiento de datos Segmentación de Red Control de acceso	DTI - Cuarto de Control
		Switch CISCO Catalyst 2960	UTP	Wireless LAN Controler Servidores	DTI - Cuarto de Control
		Wireless LAN Controler CISCO 5500	UTP FIBRA	Conexión de la red WLAN	DTI - Cuarto de Control
		Conversores Single- Mode Fibra a UTP	1000Base-TX (RJ45 UTP) a 1000Base-LX	Conectar enlaces de fibra hacia las redes externas	DTI - Cuarto de Control
		ROUTER CISCO 7604	FIBRA UTP	Internet	Proveedor de Servicios de Internet

Clara de Asís	Piso 1 5 equipos	Switch CISCO Catalyst 2960	UTP FIBRA	Internet Académico/Contable Vigilancia Servidores	Dirección de Tecnologías de la Información Salas de Cómputo
Da Ponte	Piso 1 2 equipos	Switch CISCO Catalyst 2960	UTP	Internet	Sala de Cómputo IV
		TRENDNET	UTP	Internet	Sala de Cómputo IV
	Piso 2 3 equipos	Switch CISCO Catalyst 2960	UTP FIBRA	Internet	Sala de Cómputo V
		TRENDNET	UTP	Internet	Sala de Cómputo V
		Switch CISCO Catalyst 2960	UTP FIBRA	Internet	Sala de Cómputo VI

Fuente: PUCESD – Dirección de Tecnologías de la Información – Unidad de Redes
Elaborado: Ing. Franklin Carrasco

Tabla 8: Inventario de equipos para comunicación de red LAN, edificios Mariana de Jesús, Emilio Lorenzo Stehle Aulario1, Aulario 2, Estudio de Radio, Cafetería, Hotelería.

EDIFICIO	UBICACIÓN/ CANTIDAD	EQUIPO ACTIVO	ENLACE	SERVICIO DEL ACTIVO	DEPARTAMENTOS / UNIDADES
Mariana de Jesús	Piso 1 1 equipo	Switch CISCO Catalyst 2960	UTP	Internet Académico	Dirección Estudiantes Misiones Universitarias Sala de Profesores
Emilio Lorenzo Stehle	Piso 1 1 equipo	Switch CISCO Catalyst 2960	UTP FIBRA	Internet	Sala de Eventos
Aulario 1	Piso 1 1 equipo	Switch CISCO Catalyst 2960	UTP FIBRA	Internet	NO APLICA
Aulario 2	Piso 1 2 equipos	Switch CISCO Catalyst 2960	UTP FIBRA	Internet	NO APLICA
		Switch PoE Dlink 1008P	UTP	Vigilancia	
Estudio de Radio	Piso 1 1 equipo	Switch CISCO Catalyst 2960	UTP FIBRA	Internet	DTI - Estudio de Radio
Cafetería	Piso 1 1 equipo	Switch CISCO Catalyst 2960	UTP FIBRA	Internet	NO APLICA
Hotelería	Piso 1 1 equipo	Switch CISCO Catalyst 2960	UTP FIBRA	Internet	NO APLICA

Fuente: PUCESD – Dirección de Tecnologías de la Información – Unidad de Redes
Elaborado: Ing. Franklin Carrasco

Además del mantenimiento, monitoreo y configuración de los equipos activos, la unidad de redes resguarda el correcto funcionamiento de las conexiones físicas y lógicas de la red LAN, ya sean enlaces de fibra óptica o de cable UTP, sin dejar de lado las asignaciones de direcciones IP que correspondan.

La red WLAN juega un papel importante en el servicio de internet inalámbrico que cubre el campus universitario, se puede considerar que soportan hasta 600 conexiones simultáneas en la red Estudiantes y 200 conexiones en la red Docente.; aunque no es aplicada en procesos de producción, también es empleada por profesores cuya gestión en ciertas ocasiones se conjuga con la gestión administrativa. La Tabla 9 presenta los equipos empleados como Puntos de Acceso inalámbrico en la universidad.

Tabla 9: Inventario de equipos de acceso inalámbrico

Nº	EDIFICIO	UBICACIÓN	MODELO ACCESS POINT
1	San José	Interior - Piso 1	Cisco 3602
2		Interior - Piso 2	Cisco 3602
3		Exterior Frontal	Cisco 1552

4	Misereor	Interior - Sala de reuniones Dirección Financiera	Cisco 1262
5		Exterior - Frontal Piso 2	Cisco 1552
6	San Liborio	Exterior - Lateral Derecho Piso 2	Cisco 1552
7		Interior - Pasillo Piso 2	Cisco 3602
8		Interior - Biblioteca Sala de Lectura	Cisco 1242
9			Cisco 1262
10	Clara de Asís	Pasillo - Salas de Cómputo	Cisco 1262
11		Pasillo DTI	Cisco 3602
12	Da Ponte	Interior - Sala de Cómputo 4	Cisco 3602
13	Da Ponte	Exterior - Frontal Derecha Piso 2	Cisco 1552
14		Exterior - Posterior Derecha Piso 2	Cisco 1552
15		Interior - Sala de Cómputo 6	Cisco 3602
16	Emilio Lorenzo Stehle	Exterior - Posterior Centro	Cisco 1242
17		Salón Alfa	Cisco 1262
18		Salón Omega	
19	Aulario 1	Interior - Pasillo Piso 1	Cisco 1242
20		Interior - Pasillo Piso 2	
21		Exterior - Pasillo Escaleras	Cisco 1262
22		Exterior - Frontal Izquierdo Piso 1	
23		Exterior - Lateral Derecho Piso 1	
24	Aulario 2	Interior - Pasillo Piso 1	Cisco 1242
25		Interior - Pasillo Piso 2	
26		Interior - Pasillo Aula 8	Cisco 3602
27	Estudio de Radio	Exterior - Estudio de Radio	Cisco 1242
28	Hotelería	Exterior - Posterior Izquierdo	Cisco 1242
29	Aula Magna	Interior - Lateral izquierdo	Cisco 1242
30	Bar	Bar	Cisco 3602

Fuente: PUCESD – Dirección de Tecnologías de la Información – Unidad de Redes
Elaborado: Ing. Franklin Carrasco

Una de las funciones más importantes que posee esta unidad es la de mantener en funcionamiento y bajo el debido resguardo los equipos servidores; toda la información digital de la Universidad se encuentran almacenada en estos dispositivos. En la Tabla 10, se presentan los equipos servidores dentro de un marco de mayor a menor prioridad; cabe recalcar que estos equipos son también monitoreados y revisados por la unidad de programación.

Tabla 10: Inventario de Servidores

Nº	SERVIDOR	SERVICIO
1	Producción	Sistemas Informáticos de producción Base de Datos para Sistemas Informáticos de producción
2	Pruebas Producción	Sistemas Informáticos de producción para pruebas Base de Datos para Sistemas Informáticos de producción para pruebas
3	Web	Página Web Servicio para revisión de calificaciones Servicio para Heteroevaluación docentes Base de Datos para portal web y servicio para revisión de calificaciones
4	Biblioteca	Sistema Biblioteca Base de Datos para Sistema de Biblioteca
5	Biométrico	Sistema de control de ingreso del personal Base de Datos para sistema de control de ingreso del personal
6	Docentes	Sistema Administrador de Personal Docente Base de datos para sistema administrador de personal docente
7	Archivos	Servidor de archivos Producción
8	Archivos Respaldo	Servidor de archivos Backup
9	Proxy	Proxy

10	Proxy Respaldo	Proxy Respaldo
11	DHCP	Servidor DHCP
12	Antivirus	Antivirus
13	OCS	Inventario OCS - Inventario CPUs
14	CACTI	Monitoreo CACTI
15	MicroPC	Servicio Micro-PC Biblioteca
16	Cámaras	Servidor Cámaras IP

Fuente: PUCESD – Dirección de Tecnologías de la Información – Unidad de Redes
Elaborado: Ing. Franklin Carrasco

3.4. Inventario de soluciones informáticas soportadas por la unidad de programación

La unidad de programación se encarga de mantener la funcionalidad de los Sistemas Informáticos institucionales como son: Académico, Nómina y Financiero, de los cuales posee sus respectivos códigos fuentes. Estos sistemas tienen un tiempo no mayor a diez años en producción, han pasado por constantes cambios en sus procesos, así como por el mantenimiento de diferentes programadores.

A medida que la universidad ha ido creciendo, se han desarrollado o adquirido nuevas soluciones, actualmente los sistemas informáticos en funcionamiento se presentan en la Tabla 11:

Tabla 11: Inventario Sistemas Informáticos Institucionales

Nº	SOFTWARE	CÓDIGOS FUENTE	ARQUITECTURA	BASE DE DATOS
1	Sistema Académico	SI	32 bits	Oracle 10g
2	Sistema Financiero	SI	32 bits	
3	Sistema Nómina	SI	32 bits	
4	Portal web institucional	SI	32 bits	MySQL
5	Servicio web para revisión de calificaciones	SI	32 bits	MySQL
6	Servicio web para heteroevaluación docente	SI	32 bits	MySQL
7	Sistema Administrador de Personal Docente	SI	32 bits	MySQL
8	Sistema Biblioteca	NO	64 bits	PostgreSQL
9	Sistema para control de ingreso de personal	NO	32 bits	SQL Server 2008
10	ALUMNI	SI	32 bits	MySQL
11	Proyectos de desarrollo web	SI	64 bits	MySQL

Fuente: PUCESD – Dirección de Tecnologías de la Información – Unidad de Programación
Elaborado: Ing. Franklin Carrasco

CAPÍTULO 4

ANÁLISIS Y DISEÑO DEL PLAN DE CONTINGENCIA

4.1. Análisis informático de la institución

Para iniciar con la Gestión de Riesgos informáticos de la universidad, se aplicaron los formatos presentados en el Catálogo de Elementos de la metodología Magerit para la identificación de los activos tecnológicos que permiten el cumplimiento de los objetivos del negocio (Anexo 3). Al vincularlo con el Plan de Contingencia se lo considera como “un componente o funcionalidad de un sistema de información susceptible a ser atacado deliberada o accidentalmente con consecuencias para la organización.

Incluye: información, datos, servicios, aplicaciones (software), equipos (hardware), comunicaciones, recursos administrativos, recursos físicos y recursos humanos". [15].

Para determinar los activos que presentan un alto nivel de riesgo, también se deben reconocer los servicios informáticos empleados en cada departamento, y el acceso a estos en los diferentes edificios. Como es el caso del Cuarto de Control donde se disponen los equipos activos de núcleo, distribución y acceso, así también los servidores, sistemas informáticos y bases de datos; el mismo que se sitúa en el segundo piso del edificio San Liborio. Desde este punto los enlaces de fibra óptica se interconectan con el resto de edificios.

El edificio San José representa la actividad netamente académica de la institución, donde los sistemas informáticos institucionales académico y financiero responden ante la automatización de los procesos para

estudios de grado, posgrado y formación continua, dando acceso a una conexión simultánea de 20 usuarios.

La gestión de tipo administrativo-financiero se realiza específicamente en el edificio Misereor; las direcciones de Recursos Humanos y Financiera emplean los sistemas institucionales de nómina, y financiero respectivamente. Adjunto a este edificio se encuentra San Liborio, que a más de centralizar los sistemas de información, incluye también departamentos específicos para cubrir los requisitos estatales en la educación superior, y unidades directivas de la universidad como Prorrectorado, Viceprorrectorado.

El equipo técnico de la Dirección de Tecnologías de la Información se encuentra en el edificio Clara de Asís, sitio determinado para centralizar el desarrollo tecnológico, la infraestructura tecnológica y progresivamente un Gobierno de TI. En el edificio Mariana de Jesús funcionan la dirección de estudiantes y la dirección de misiones

universitarias, vinculadas al ámbito académico y espiritual, de igual importancia que las unidades en el edificio académico.

Los edificios como Da Ponte, Emilio Lorenzo Stehle, Aularios 1 y 2, Estudio de Radio, Cafetería, y Hotelería están dispuestos para el servicio de internet, actividades formativas, eventos culturales o clases. Con esta referencia se identifican a continuación los activos (lógicos y físicos) utilizados en cada edificio, seleccionados de acuerdo a su confidencialidad, integridad, y disponibilidad. Para esta selección se toma la relación presentada en la Figura 4.1.

Figura 4.1: Orden para selección de activos de la PUCESD
Fuente: PUCESD – Dirección de Tecnologías de la Información – Unidad de Redes
Elaborado: Ing. Franklin Carrasco

Es fundamental empezar por el activo de mayor importancia para la universidad como son los datos, los sistemas informáticos, y los servidores donde se alojan. En las Tablas 12 y 13, se identifican aquellos cuyas posibles fallas representan un alto nivel de riesgo.

Tabla 12: Sistemas informáticos, bases de datos y servidores seleccionados para contingencia

Nº	SISTEMA INFORMÁTICO	BASE DE DATOS	SERVIDOR
1	Sistema Académico	Oracle 10g	Producción
2	Sistema Financiero		
3	Sistema Nómina		
4	Sistema Académico, Nómina, Financiero – Pruebas	Oracle 10g	Pruebas Producción
5	Portal web institucional	MySQL	Web
6	Servicio web para revisión de calificaciones		
7	Servicio web para heteroevaluación docente		
8	Sistema Biblioteca	PostgreSQL	Biblioteca
9	Sistema para control de ingreso de personal	SQL Server 2008	Biométrico
10	Sistema Administrador de Personal Docente	MySQL	Docentes

Elaborado: Ing. Franklin Carrasco

Tabla 13: Servicios para la red LAN seleccionados para contingencia

Nº	SERVICIO	SISTEMA OPERATIVO	SERVIDOR
1	Servidor de archivos Producción	LINUX – CentOS	Archivos
2	Servidor de archivos Backup	LINUX – CentOS	Archivos Respaldo
3	Proxy	LINUX – CentOS	Proxy
4	Proxy Respaldo	LINUX – CentOS	Proxy Respaldo
5	DHCP	Windows Server 2008	DHCP

Elaborado: Ing. Franklin Carrasco

De manera similar se han determinado los equipos de comunicación de la red LAN susceptibles a daños, su importancia radica en la comunicación, su correcto funcionamiento y la seguridad de acceso. En la Tabla 14 se presentan los equipos relacionados al lugar donde se generan los principales procesos de negocio de la institución.

Tabla 14: Equipos activos de comunicación seleccionados para contingencia

EDIFICIO	UBICACIÓN	EQUIPO ACTIVO	CONEXIÓN EXTERNA	RED INTERNA	SERVICIO
San José	Piso 1: 2 equipos Piso 2: 1 equipo	Switch CISCO Catalyst 2960	FIBRA	UTP	- Académico - Contable - Internet - Vigilancia

Elaborado: Ing. Franklin Carrasco

Misereor	Piso 1: 1 equipo	Switch CISCO Catalyst 2960	FIBRA	UTP	- Internet
	Piso 2: 1 equipo		FIBRA	UTP	- Académico - Contable - Nómina - Internet - Vigilancia
	Piso 3: 1 equipo		FIBRA	UTP	
San Liborio	Piso 1: 2 equipo	Switch CISCO Catalyst 2960	UTP	UTP	- Internet - Biblioteca - Vigilancia
	Piso 2 *	1 Switch CISCO Catalyst 2960	UTP	UTP	- Internet
		1 Switch CISCO Catalyst 2960	FIBRA	UTP	- Conexión LAN hacia los edificios - Wireless LAN Controler - Servidores
		1 Switch TRENDNET 448WS	UTP	UTP	- Servidores. - Router ISP
		ROUTER CISCO 2800	UTP		- Enrutamiento de datos - Segmentación de Red - Control de acceso
		1 Switch CISCO Catalyst 2960	UTP	UTP	- Wireless LAN Controler - Servidores
		Wireless LAN Controler CISCO 5500	UTP	UTP	- Conexión red WLAN en el Campus
		10 conversores Single- Mode Fibra a UTP	No aplica	No aplica	Conectar enlaces de fibra hacia las redes externas
		ROUTER CISCO 7604 ISP	UTP	UTP	Internet
Clara de Asís	Piso 1: 5 equipos	Switch CISCO Catalyst 2960	FIBRA	UTP	Internet Académico Contable Nómina Internet Vigilancia Wireless LAN Servidores
Mariana de Jesús	Piso 1: 1 equipo	Switch CISCO Catalyst 2960	UTP	UTP	Internet Académico

Los equipos activos del Cuarto de Control respaldan su funcionalidad bajo el apoyo de activos de tipo eléctrico y climático, como se indican en la Tabla 15.

Tabla 15: Activos para respaldo eléctrico y climatización

Nº	ACTIVO	RESPALDO
1	Sistema de alimentación ininterrumpida (SAI/UPS) Tripp-lite Omnvis 1500	Servidor Producción
		Web
2	Aire Acondicionado FRIGOSTAR ELITE	Climatización Cuarto de Control

Elaborado: Ing. Franklin Carrasco

Mantener una comunicación activa requiere que los medios empleados para la conmutación de los datos se mantengan seguros, por tal razón se consideran también los enlaces de fibra óptica que conectan a cada uno de los edificios seleccionados.

Los últimos activos seleccionados para la contingencia son aquellos que pueden verse afectados por riesgos naturales o humanos, son

importantes puesto que dan la estabilidad a los procesos del negocio. En la Tabla 16, se presentan los edificios que necesitan de un mayor resguardo por la gestión que desempeñan los departamentos administrativos y académicos, como también por el rol asignado a las personas.

Tabla 16: Edificios, departamentos y personal administrativo significativo

EDIFICIO	UBICACIÓN	DEPARTAMENTOS / UNIDADES	PERSONAL
San José	Piso 1	Información Secretarías de Escuela, Formación Continua, Investigación Secretaría General Tesorería Direcciones de Escuela Sala de Profesores	Directores Secretarias Auxiliares Profesores
	Piso 2	Dirección Académica Dirección de Planificación Dirección de Investigación Dirección de Formación continua Dirección de Jardín Botánico	Directores Secretarias Auxiliares Profesores
Misereor	Piso 1	Centro Médico Sala de Profesores	Doctor Enfermera Profesores
	Piso 2	Dirección Administrativa Recursos Humanos	Directores Secretarias Auxiliares
	Piso 3	Dirección Financiera	Directores Secretarias Auxiliares

San Liborio	Piso 1	Biblioteca	Bibliotecarias
	Piso 2	Prorrectorado Viceprorrectorado Relaciones Interinstitucionales Evaluación y Acreditación Desarrollo Institucional Asesoría Legal Psicoética Sala Docentes	Directores Secretarias Auxiliares Abogados Psicólogos Profesores
		DTI - Cuarto de Control	Técnicos de Redes
Clara de Asís	Piso 1	Dirección de Tecnologías de la Información Salas de Cómputo	Directores Coordinadores Técnicos de Soporte Técnicos de Programación Técnicos de Redes Diseñadores Comunicador Social
Mariana de Jesús	Piso 1	Dirección de Estudiantes Misiones Universitarias Sala de Profesores	Directores Secretarias Auxiliares Profesores

Elaborado: Ing. Franklin Carrasco

4.2. Objetivo y alcance del Plan de Contingencia Informática

El objetivo del plan de contingencia es el de disponer de una estrategia que permita a corto plazo responder ante incidencias graves, bajo guías organizadas y dispuestas entre el personal técnico de la Dirección de

Tecnologías de la Información, buscando resguardar y poner en marcha los sistemas de información de la universidad.

Conociendo la infraestructura tecnológica que posee la universidad, así como los principales departamentos que le conforman para la continuidad de sus operaciones. Se determina el alcance del plan de contingencia informática para la Dirección de Tecnologías de la Información, expresamente empleando estrategias para el levantamiento y puesta en marcha de los activos definidos como: bases de datos, servidores, sistemas informáticos y equipos de comunicación de datos; así también se hace referencia al personal técnico especializado, encargado de llevar las funciones técnicas dentro de la universidad.

4.3. Metodología aplicada

Para el desarrollo del plan de contingencia y el análisis de riesgos se aplicará la Metodología Magerit (acrónimo de “Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información”) en su versión 3.0, la misma que ha sido creada por el Consejo Superior de Administración y Electrónica (CSAE), que estima que “la gestión de riesgos es la piedra angular en la guías de buen gobierno público o privado, donde se considera un principio fundamental que las decisiones de gobierno se fundamenten en el conocimiento de los riesgos” [16].

Esta metodología cubre los riesgos de TI en particular, estableciendo principios para el empleo eficaz, eficiente y aceptable de las tecnologías de la información. Magerit basa sus procesos de gestión de riesgos en la normativa ISO 31000, los cuales se presentan dentro de un marco de trabajo, permitiendo a los órganos de gobierno o autoridades de la empresa, tomar decisiones basándose en los riesgos que se generan por el uso de tecnologías. En la Figura 4.2 se puede observar el Marco de Trabajo para la gestión de riesgo, y cuando se aplica esta metodología.

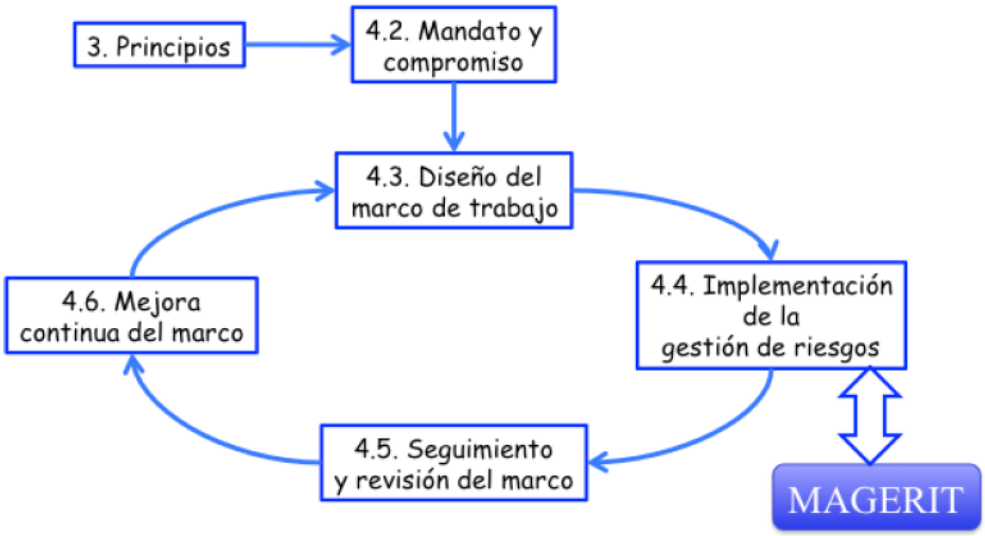

Figura 4.2: ISO 31000 - Marco de trabajo para la gestión de riesgos
Fuente: Libro I Método, Magerit versión 3

Al emplear Magerit nos sumamos a los objetivos que persigue, como son:

Objetivos Directos:

1. Concienciar a los responsables de las organizaciones de información de la existencia de riesgos y de la necesidad de gestionarlos
2. Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC)

3. Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control

Objetivos Indirectos:

1. Preparar a la Organización para procesos de evaluación, auditoría, certificación o acreditación, según corresponda en cada caso [10]

Con los resultados del análisis de riesgos en los sistemas de información de la institución, se establecerá un nivel de seguridad y confianza en redes de datos o sistemas informáticos para resistir incidencias directas o indirectas que comprometan la disponibilidad, integridad, confidencialidad de los datos almacenados o transmitidos por la red; de igual forma se complementará con la autenticidad y trazabilidad de los usuarios que la frecuentan.

El proceso dispuesto por la metodología para la gestión de riesgos se compone de dos procesos importantes, como es el análisis de riesgos, y el tratamiento de estos, tal como se presenta en la Figura 4.3.

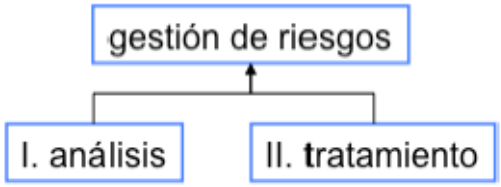

Figura 4.3: Gestión de Riesgos
Fuente: Libro I Método, Magerit versión 3

4.3.1. Análisis de Riesgos

En este apartado se determina que activos posee la universidad y la estimación de los posibles incidentes que le puedan afectar; en su desarrollo se consideran:

a) Activos, sistemas de información que soportan los procesos de negocio de la institución.

b) Amenazas, situaciones o incidencias que pueden afectar a los activos, perjudicando la estabilidad de la empresa.
c) Salvaguardas o contramedidas, creadas como medidas de protección ante la materialización de las amenazas.

Con los resultados obtenidos se estimará el impacto (lo que podría pasar), y el riesgo (lo que probablemente pase), permitiendo desplegar conclusiones que faciliten el tratamiento de los riesgos.

4.3.1.1. Activos

En este primer proceso se debe identificar, clasificar, definir dependencias y valorar los activos de mayor importancia en la universidad ya sea por la información que maneja o por los servicios que presta, pues son el eje de los requisitos de seguridad para el soporte de la institución. Entre los activos de mayor relevancia se identifican:

- Datos, información lógica
- Sistemas o aplicaciones Informáticas que sostienen a los datos (software)
- Equipos informáticos que mantienen o procesan datos, aplicaciones y servicios
- Servicios, contratados o internos, que apoyan al desempeño de la organización
- Dispositivos de almacenamiento de datos
- Redes de comunicaciones para el intercambio de datos
- Instalaciones físicas, donde se ubican los sistemas de información
- Personas, que operan los activos antes mencionados, y
- Equipamiento auxiliar de apoyo a la infraestructura informática

Con esta referencia Magerit clasifica los activos dentro de una jerarquía, identificándolos con un código, un nombre y una breve descripción de sus características, en la Tabla 17 se presenta la clasificación de los activos:

Tabla 17: Tipos de Activos

[D] Datos/Información
[keys] claves criptográficas
[S] Servicios
[SW] Aplicaciones (software)
[HW] Equipamiento Informático (hardware)
[COM] Redes de Comunicaciones
[Media] Soportes de Información
[AUX] Equipamiento auxiliar
[L] Instalaciones
[P] Personal

Fuente: Libro II Catálogo, Magerit versión 3

Una vez identificados y clasificados los activos, se realiza la vinculación de estos de acuerdo a sus dependencias. Como se ha indicado anteriormente la información y los servicios son los activos esenciales en una institución, pero también dependen de otros activos, como son: equipos de comunicación, medios de red, equipos servidores, instalaciones físicas, personal técnico entre otros.

Por lo tanto es importante determinar las dependencias de activos para así conocer sus necesidades de seguridad, es decir, cuando se materializa una amenaza en un activo de nivel inferior, tendrá como consecuencia un perjuicio sobre el activo superior, los activos inferiores

son los pilares en los que se apoya la seguridad de los activos superiores.

En la Figura 4.4 se observa un grafo con la dependencia del servicio de Internet para el constante funcionamiento del servicio de correo electrónico [EMAIL_DTI] y portal web de la universidad [EMAIL_DTI], como también se observan los equipos activos de comunicación y personal de la unidad de redes que permiten mantener activo los servicios antes mencionados.

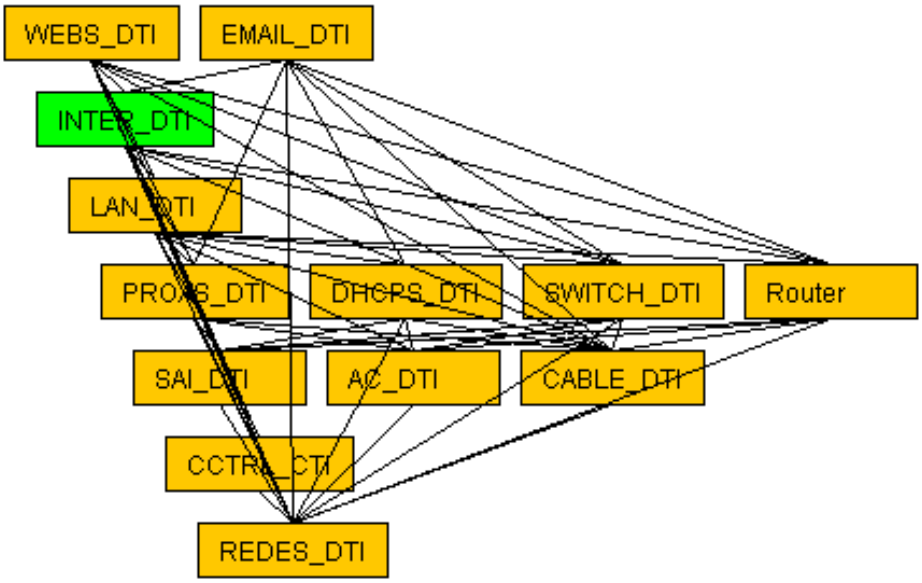

Figura 4.4: Dependencia de servicio de Internet
Fuente: Análisis de riesgos Plan de Contingencia Informática PUCESD - PILAR
Elaborado: Ing. Franklin Carrasco

Para terminar con este análisis de activos, realizamos su valoración de acuerdo a un dimensionamiento establecido. La valoración del activo se realiza de acuerdo a su valor como apoyo en los procesos del negocio, más no por el valor comercial, es decir, desde la perspectiva del nivel de protección que requiere; la valoración puede ser cualitativa (escala de niveles o rango numérico de 0 a 10) o cuantitativa (escala numérica).

Para realizar la valoración es necesaria la participación del equipo técnico, directores y personal administrativo, que conocen a mejor detalle la realidad e importancia de los activos de la institución (servicios e información). La valoración del activo se considera según las consecuencias que podría tener la materialización de una amenaza, para esto es necesario tomar como referencia las dimensiones de:

a) [D] Disponibilidad: ¿Qué perjuicio podría tener la institución si un activo o servicio no estuviera disponible a causa de una amenaza?

b) [I] Integridad: ¿Qué mal podría causar a la institución la alteración de la información de forma no autorizada?
c) [C] Confidencialidad: ¿Qué daño podría ocurrir si personas no autorizadas acceden a la información?
d) [A] Autenticidad: ¿Qué consecuencias se podrían desatar si el usuario que accede al servicio no es quién uno cree?
e) [T] Trazabilidad: ¿Qué daño causaría no saber todas las actividades que realiza un usuario con el acceso a un servicio o a datos?

Definidas las dimensiones de seguridad para los activos, se procede a su estimación de valoración, que por lo general es cualitativo, dejando a criterio del usuario el resultado seleccionado a partir de una escala de valor. Magerit aplica una escala estándar de diez valores, dejando en 0 como valor despreciable y 10 como un evento de afección extremadamente grave, tal como se muestra en la tabla 18.

Tabla 18: Escala de Valoración para cada dimensión

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

Fuente: Libro II Catálogo, Magerit versión 3

Con la finalidad de mantener homogeneidad en la valoración, la metodología presenta un conjunto de criterios que permitirán al usuario determinar con una realidad más exacta los efectos negativos que pueden tener los activos; los cuales se describen en las siguientes tablas:

Tabla 19: Valoración Información de carácter personal

[pi] Información de carácter personal		
6	6.pi1	probablemente afecte gravemente a un grupo de individuos
	6.pi2	probablemente quebrante seriamente la ley o algún reglamento de protección de información personal
5	5.pi1	probablemente afecte gravemente a un individuo
	5.pi2	probablemente quebrante seriamente leyes o regulaciones
4	4.pi1	probablemente afecte a un grupo de individuos
	4.pi2	probablemente quebrante leyes o regulaciones

3	3.pi1	probablemente afecte a un individuo
	3.pi2	probablemente suponga el incumplimiento de una ley o regulación
2	2.pi1	pudiera causar molestias a un individuo
	2.pi2	pudiera quebrantar de forma leve leyes o regulaciones
1	1.pi1	pudiera causar molestias a un individuo

Fuente: Libro II Catálogo, Magerit versión 3

Tabla 20: Valoración Obligaciones legales

[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

Fuente: Libro II Catálogo, Magerit versión 3

Tabla 21: Valoración Seguridad

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

Fuente: Libro II Catálogo, Magerit versión 3

Tabla 22: Valoración Intereses comerciales o económicos

[cei] Intereses comerciales o económicos		
9	9.cei.a	de enorme interés para la competencia
	9.cei.b	de muy elevado valor comercial
	9.cei.c	causa de pérdidas económicas excepcionalmente elevadas
	9.cei.d	causa de muy significativas ganancias o ventajas para individuos u organizaciones
	9.cei.e	constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
7	7.cei.a	de alto interés para la competencia
	7.cei.b	de elevado valor comercial
	7.cei.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

Fuente: Libro II Catálogo, Magerit versión 3

Tabla 23: Valoración Interrupción del servicio

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

7	7.da	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
	7.da2	Probablemente tenga un gran impacto en otras organizaciones
5	5.da	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	5.da2	Probablemente cause un cierto impacto en otras organizaciones
3	3.da	Probablemente cause la interrupción de actividades propias de la Organización
1	1.da	Pudiera causar la interrupción de actividades propias de la Organización

Fuente: Libro II Catálogo, Magerit versión 3

Tabla 24: Valoración Orden público

[po] Orden público		
9	9.po	alteración seria 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

Fuente: Libro II Catálogo, Magerit versión 3

Tabla 25: Valoración Operaciones

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

Fuente: Libro II Catálogo, Magerit versión 3

Tabla 26: Valoración Administración y gestión

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

Fuente: Libro II Catálogo, Magerit versión 3

Tabla 27: Valoración Pérdida de confianza (reputación)

[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

Fuente: Libro II Catálogo, Magerit versión 3

Tabla 28: Valoración Persecución de delitos

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

Fuente: Libro II Catálogo, Magerit versión 3

Tabla 29: Valoración Tiempo de recuperación del servicio

[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

Fuente: Libro II Catálogo, Magerit versión 3

Tabla 30: Valoración Información clasificada (nacional)

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

Fuente: Libro II Catálogo, Magerit versión 3

4.3.1.2. Amenazas

Una vez establecida la valoración los activos, el paso siguiente es la identificación de las amenazas que les podrían causar daños graves e irreversibles. Como se ha indicado anteriormente, una amenaza es la causa generadora de un incidente cuya materialización afecta de forma directa e indirecta a los sistemas de información y procesos de una organización. Magerit cataloga a las amenazas en cuatro grupos, que son:

a) [N] Desastres Naturales: Sucesos ocurridos por efectos propios de la naturaleza sin intervención de los seres humanos, como: Incendios, Perjuicios ocasionados por el agua, Fenómenos climáticos, Fenómenos sísmicos, Fenómenos de origen volcánico, Fenómenos meteorológico, inundaciones, entre otros.

b) [I] De origen industrial: Sucesos ocurridos de forma accidental, derivados de la actividad humana de tipo industrial, y que pueden darse de forma accidental o deliberada, como: Incendios, Fallas o interrupciones eléctricas, Interrupción de operaciones, Ruido electromagnético, Avería o falla de

funcionamiento del hardware, Fallas en la climatización, Pérdida en medios de comunicación, entre otros.

c) [E] Errores y fallos no intencionados: Fallos causados por acciones no malintencionadas de las personas, como: errores de los usuarios, errores de los administradores, errores de monitoreo, errores de configuración, incorrecta asignación de funciones, propagación inocente de virus, escape de información de forma accidental, destrucción de información almacenada en soportes informático, errores de actualización de programas, indisponibilidad del personal, entre otros.

d) [A] Ataques Intencionados: Fallos causados por acciones malintencionadas de las personas, como: manipulación de los registros de actividad (log), manipulación de configuración, suplantación de identidad del usuario, abuso de privilegios de acceso, uso de recursos del sistema para fines no previstos, difusión de software dañino, re-encaminamiento de mensajes, acceso no autorizado a recursos informáticos, interceptación, modificación y destrucción de información, ataques informáticos, robo, ingeniería social, entre otros.

No todos los activos son afectados en una misma dimensión de daño por una amenaza, por lo tanto se debe identificar la relación entre el tipo de activo y lo que podría ocurrir, valorando la influencia de la amenaza sobre el activo, la misma que se define en dos sentidos:

- El nivel de Degradación de valor que causa la amenaza sobre el activo en caso de materializarse, y
- La Probabilidad de ocurrencia de cada amenaza sobre el activo

La metodología permite aplicar un modelo cualitativo por medio de una escala nominal para valorar las amenazas de cada activo de acuerdo a la probabilidad de ocurrencia y degradación de valor, presentadas en las Tablas 31 y 32 respectivamente. Es habitual tomar como referencia un año como medida de la probabilidad de ocurrencia.

Tabla 31: Probabilidad de Ocurrencia

MA	100	muy frecuente	a diario
A	10	frecuente	Mensualmente
M	1	normal	una vez al año
B	1/10 = 0.1	poco frecuente	cada varios años
MB	1/100 =0.01	muy poco frecuente	Siglos

Fuente: Libro II Catálogo, Magerit versión 3

La degradación permite definir el nivel de daño o perjuicio en caso de una posible materialización de la amenaza.

Tabla 32: Degradación del valor

MA	muy alta	casi seguro	Fácil
A	Alta	muy alto	Medio
M	Media	posible	Difícil
B	Baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

Fuente: Libro II Catálogo, Magerit versión 3

4.3.1.3. Impacto potencial

El impacto es la medida de daño que una amenaza puede generar sobre un sistema; Magerit presenta dos resultados sobre el cálculo del impacto, el impacto acumulado, y el impacto repercutido.

El Impacto Acumulado de un activo es el resultado del cálculo del impacto del propio activo y los activos que dependen de él, con las amenazas que está expuesto. El resultado de su cálculo permite determinar que salvaguardas se deben dotar a los medios de trabajo, por ejemplo, copias de respaldos, protección de equipos, entro otros.

El impacto repercutido del activo es el resultado del cálculo del impacto del propio activo, y de las amenazas que están expuestos lo activos que depende. El resultado de su cálculo permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información, es decir, permite a la empresa decidir si tomar la decisión de aceptar de manera gerencial un cierto nivel de riesgo sobre

el activo. Con los cálculos anteriormente indicados, se obtendrá el valor del impacto potencial, el cual se debe minimizar con la aplicación de las salvaguardas correspondientes.

4.3.1.4. Riesgo potencial

El riesgo es la medida de daño probable al cual se somete un sistema; conociendo los niveles de impacto de las amenazas sobre los activos, es posible derivar el riesgo tomando en cuenta la probabilidad de ocurrencia. Para reconocer los riesgos con mayor probabilidad de ocurrencia, y mayor impacto, Magerit define una representación gráfica escalar del riesgo en función del impacto y la probabilidad presentada en la Figura 4.5.

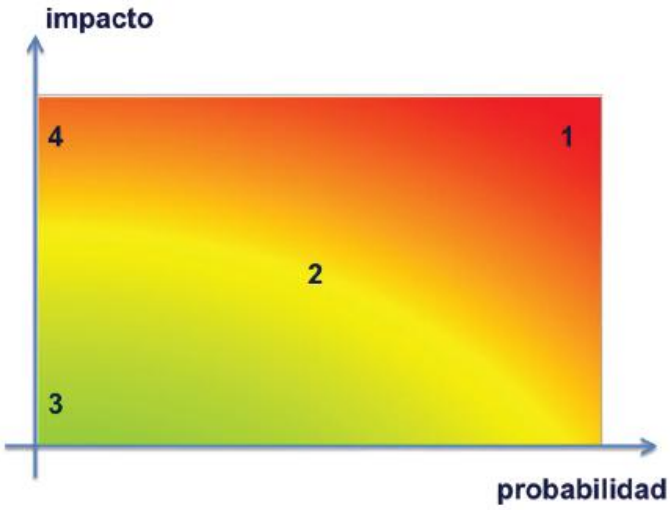

Figura 4.5: El riesgo en función del impacto y la probabilidad
Fuente: Libro I Método, Magerit versión 3

La zona 1, representa a los riesgos muy probables y de muy alto impacto; la zona 2, justamente la franja de color amarilla, indica desde situaciones improbables y de impacto medio, hasta situaciones muy probables pero de bajo o muy bajo impacto; la zona 3, representa los riesgos improbables y de bajo impacto; por último la zona 4, indica riesgos improbables pero de muy alto impacto.

El riesgo acumulado es el resultado de calcular el impacto acumulado sobre un activo debido a una amenaza, y la probabilidad de la amenaza. Esto permite determinar las salvaguardas que se deben establecer en los sistemas de información.

El riesgo repercutido es el resultado de calcular el impacto repercutido sobre un activo debido a una amenaza, y la probabilidad de la amenaza. Al calcularse sobre los activos que tienen valor propio, determina las consecuencias de las incidencias técnicas sobre las operaciones del sistema de información, como también, permite a nivel gerencial, dentro de un análisis de riesgo, tomar la decisión de aceptar un cierto nivel de riesgo sobre el activo.

4.3.1.5. Salvaguardas

“Se definen las salvaguardas o contra medidas como aquellos procedimientos o mecanismos tecnológicos que reducen el riesgo. Hay amenazas que se conjurar simplemente organizándose

adecuadamente, otras requieres elementos técnicos (programas o equipos), otra seguridad física y, por último, está la política de personal.” [10].

Al momento se han tomado en cuenta los impactos y riesgos que estarían expuestos los activos si no se protegieran con las salvaguardas correspondientes. Antes de definir las salvaguardas, es necesario considerar aquellas que son relevantes para los activos que se deben proteger, tomando en cuenta los siguientes aspectos:

a) El tipo de activo que se desea proteger, por su naturaleza difiere la forma de protección.
b) Las dimensiones de seguridad que requiere la protección.
c) Las amenazas que nos afectan y contras las cuales buscamos protección.
d) La existencia de salvaguardas alternativas.
e) Establecer proporcionalidad en la protección, tomando en cuenta:

a. El mayor o menor valor propio o cumulado de un activo, tomando en cuenta lo más valiosos y obviando lo irrelevante.
b. La mayor o menor probabilidad de materialización de una amenaza, tomando como referencia las zonas de riesgos más importantes.
c. Cobertura del riesgo para proporcionar salvaguardas alternativas.

Con la referencia de estos aspectos se determinan dos tipos de declaraciones que permiten excluir a ciertas salvaguardas que son:

- No aplica: cuando la salvaguarda no es adecuada al tipo de activo, o no protege la dimensión requerida por el daño de la materialización de una amenaza.
- No se justifica: cuando la salvaguarda aplica pero no proporciona la cobertura de protección requerida.

Como resultado de este análisis se obtendrá un conjunto de salvaguardas cuyo efecto permitirá reducir de forma preventiva la

probabilidad de la materialización de una amenaza, o a su vez posibilitará limitar el daño y degradación del sistema cuando la amenaza se activa. Magerit presenta diferentes tipos de salvaguardas de acuerdo a la naturaleza de la amenaza, tal como se presentan en la tabla 33:

Tabla 33: Tipos de Salvaguardas

EFECTO	TIPO
Preventivas: reducen la probabilidad	[PR] preventivas
	[DR] disuasorias
	[EL] eliminatorias
Acotan la degradación	[IM] minimizadoras
	[CR] correctivas
	[RC] recuperativas
Consolidan el efecto de las demás	[MN] de monitorización
	[DC] de detección
	[AW] de concienciación
	[AD] administrativas

Fuente: Libro I Método, Magerit versión 3

Así también se deben valorar las salvaguardas para verificar su eficacia frente al riesgo, desde el punto de vista:

- Técnico: se emplea siempre, es perfecta para enfrentarse a un posible riesgo
- Operación: los procedimientos de su activación en caso de incidencias son claros, se encuentra bien configurada, mantenida y desplegada; los usuarios están capacitados y existen controles que advierten fallos

Magerit presenta una escala de madurez para valorar la eficacia de la salvaguarda, desde el 0% para aquellas que fallan en el cumplimiento de protección, hasta el 100% de aquellas que son idóneas; esta escala se puede observar en la tabla 34.

Tabla 34: Eficacia y madurez de las salvaguardas

EFICACIA	NIVEL	MADUREZ
0%	L0	inexistente
10%	L1	inicial / ad hoc
50%	L2	reproducible, pero intuitivo
90%	L3	proceso definido
95%	L4	gestionado y medible
100%	L5	Optimizado

Fuente: Libro I Método, Magerit versión 3

Definidas las salvaguardas, es necesaria una nueva valoración del impacto y riesgo potencial, para determinar las ponderaciones residuales que se mantienen luego de aplicar la protección correspondiente.

4.3.1.6. Impacto Residual

Con la aplicación de las salvaguardas se ha modificado el impacto desde un valor potencial a uno residual; es decir, ha cambiado la magnitud de degradación, tomando en cuenta la eficacia de las salvaguardas (resta entre al eficacia perfecta y la eficacia real). El cálculo del impacto residual es similar al impacto potencial, y puede calcularse acumulado sobre los activo inferiores o repercutido sobre los activos superiores.

4.3.1.7. Riesgo residual

Con el despliegue de las salvaguardas se ha modificado el riesgo desde un valor potencial a uno residual; es decir, ha cambiado la magnitud de degradación y la probabilidad de ocurrencia de las amenazas. Para el cálculo del riesgo residual se usan los valores del impacto residual (magnitud de degradación) y la probabilidad residual de ocurrencia (resta entre al eficacia perfecta y la eficacia real). El cálculo del riesgo residual es similar al impacto potencial, y puede calcularse acumulado sobre los activo inferiores o repercutido sobre los activos superiores.

4.3.2. Formalización de actividades para contingencia

Con la determinación de las salvaguardas, se realizan los procedimientos a seguir para prevenir o sostener los sistemas de información ante la posible materialización de las amenazas. La definición de los procedimientos se concreta con el trabajo colectivo del personal técnico y administrativo de la institución bajo la valoración y análisis constante de los activos y servicios relevantes.

4.3.3. Herramienta PILAR

Es una herramienta desarrollada por el Centro Nacional de Inteligencia del Gobierno de España, como apoyo para el análisis de riesgos de sistemas de información siguiendo la metodología Magerit. PILAR acrónimo de Procedimiento Informático Lógico para el Análisis de Riesgos, soporta las fases de:

- Identificación, clasificación, dependencias y valoración de activos
- Determinación de amenazas
- Estimación de Impactos y riesgos
- Determinación y evaluación de las salvaguardas

La herramienta incorpora un catálogo de elementos que proporcionan una dimensión de valoración en cada una de las fases antes mencionadas, las mismas que se actualizan de acuerdo las necesidades tecnológicas. Proporciona también los modelos cualitativo y cuantitativo para el análisis y valoración de activos, amenazas y salvaguardas. Para el desarrollo del Plan de Contingencia, la herramienta PILAR se

posiciona como un apoyo base para la valoración, análisis y toma de decisiones.

4.4. Identificación de grupos de trabajo y fuentes de información

Al determinar el personal que participará como apoyo en el levantamiento de información, se tomó como referencia a aquellos cuyas actividades de gestión dentro de la Dirección de Tecnologías de la Información, así como en otros departamentos, hacen uso o dan soporte a los sistemas informáticos, servicios e infraestructura tecnológica. Las personas que aportaron con información para el desarrollo del proyecto son:

- Técnico área de Redes, Infraestructura – Dirección de Tecnologías de la Información
- Técnico área de Programación, Desarrollo – Dirección de Tecnologías de la Información
- Directora Financiera – Dirección Financiera
- Contadora – Dirección Financiera
- Directora de Recursos Humanos – Dirección de Recursos Humanos
- Directora Académica- Dirección Académica
- Coordinadora de Secretarias- Dirección Académica

- Coordinadora de Biblioteca- Viceprorrectorado

En los departamentos que no pertenecen al área tecnológica se realizó una entrevista verbal para determinar la importancia por la cual es necesario mantener activos los sistemas informáticos, dejando en última instancia al área tecnológica, que reportó la información solicitada para el presente proyecto. Toda la información recopilada se realiza con la aprobación de Prorrectorado de la PUCESD, bajo los términos legales de la institución (Anexo 2).

CAPÍTULO 5

DESARROLLO DEL PLAN DE CONTINGENCIA INFORMÁTICA

5.1. Identificación y análisis de riesgos críticos

Para el desarrollo del Plan de contingencia informática de la Dirección de Tecnologías de la Información de la PUCE SD, será aplicada la metodología Magerit versión 3, con el soporte de la herramienta PILAR 5.4.4. Mediante el apoyo del personal técnico y administrativo, se identificaron los sistemas de información (activos) relevantes en los procesos de gestión de la universidad (Anexo 2), presentados en las siguientes tablas:

Tabla 35: Servicios Informáticos internos

[IS] SERVICIOS INTERNOS	PROCESO
[INTER_DTI] Internet	Servicios electrónicos utilizados para la comunicación entre el personal administrativo, académico y estudiantil de la universidad.
[WEBS_DTI] Portal Web PUCESD	
[EMAIL_DTI] Servicio Correo Electrónico Gmail	
[FILE_DTI] Almacenamiento de Archivos	

Fuente: Dirección de Tecnologías de la Información – PUCE SD

Tabla 36: Aplicaciones Informáticas Institucionales

[SW] APLICACIONES	PROCESO
[PROD_DTI] Sistemas Informáticos de Producción	Sistemas Informáticos institucionales, y software propietario empleado para el desarrollo de los procesos de gestión de la universidad, como también para asegurar la información y los usuarios.
[PWEB_DTI] Servicios Portal Web	
[BIBL_DTI] Sistema de Biblioteca	
[PROF_DTI] Sistema administrador de personal docente	
[BIOM_DTI] Sistema para control de ingreso de personal	
[FILEBA_DTI] Software para respaldo de archivos	
[OFFI_DTI] Office – Ofimática	
[AV_DTI] Antivirus	
[OS_DTI] Sistema Operativo	

Fuente: Dirección de Tecnologías de la Información – PUCE SD

Tabla 37: Equipos activos, servidores y dispositivos (hardware

[HW] EQUIPOS	PROCESO
[PRODS_DTI] Servidor de Producción	Infraestructura tecnológica (hardware), empleada ya sea para alojar Sistemas informáticos, para seguridad/filtrado de paquetes, y para la conectividad de los medios de comunicación de datos LAN y WLAN
[DSKB_DTI] Disco para respaldos de Sistemas Informáticos de Producción	
[PWEBS_DTI] Servidor Portal Web	
[BIBLS_DTI] Servidor Sistema de Biblioteca	
[PROFS_DTI] Servidor Sistema administrador de personal docente	
[BIOMS_DTI] Servidor Sistema para control de ingreso de personal	
[FILEBAS_DTI] Servidor Respaldo de Archivos	
[PROXS_DTI] Servidor Proxy Firewall	
[DHCPS_DTI] Servidor DHCP	
[SWITCH_DTI] Switch	
[Router] Router	
[WLC_DTI] Controladora de red inalámbrica	
[WAP] Punto de Acceso Inalámbrico	

Fuente: Dirección de Tecnologías de la Información – PUCE SD

Tabla 38: Redes y servicio de comunicación de datos

[COM] COMUNICACIONES	PROCESO
[LAN_DTI] Red LAN	Red de comunicación de Datos LAN y WLAN utilizada en la universidad
[WLAN_DTI] Red LAN Inalámbrica	
[INTERNET_DTI] Servicio de Internet	

Fuente: Dirección de Tecnologías de la Información – PUCE SD

Tabla 39: Equipamiento auxiliar

[AUX] ELEMENTOS AUXILIARES	PROCESO
[SAI_DTI] Sistema de alimentación ininterrumpida	Equipamiento para sostenibilidad y cuidado de los sistemas de información de la universidad
[AC_DTI] Aire Acondicionado	
[CABLE_DTI] Cableado de Datos	

Fuente: Dirección de Tecnologías de la Información – PUCE SD

Tabla 40: Servicios Subcontratados

[SS] SERVICIOS SUBCONTRATADOS	PROCESO
[BIBLIOSUB_DTI] Proveedor Sistema Biblioteca	Servicios informáticos y de comunicación subcontratados
[BIOMSUB_DTI] Proveedor Sistema para control de ingreso de personal	
[INTERSUB_DTI] Servicio de Internet	

Fuente: Dirección de Tecnologías de la Información – PUCE SD

Tabla 41: Instalación física

[L] INSTALACIONES	PROCESO
[CCTRL_DTI] Cuarto de Control	Infraestructura donde se centralizan los sistemas informáticos, dispositivos y medios de comunicación

Fuente: Dirección de Tecnologías de la Información – PUCE SD

Tabla 42: Personal Técnico

[P] PERSONAL	PROCESO
[ADMP_DTI] Administradores de Sistemas Informáticos - Programadores	Personal de la Dirección de Tecnologías de la Información responsable de mantener y dar soporte a los sistemas de información de la universidad
[REDES_DTI] Administradores de infraestructura y telecomunicaciones	
[SOPTE_DTI] Soporte Técnico	

Fuente: Dirección de Tecnologías de la Información – PUCE SD

5.1.1. Dependencias entre Activos

Identificados los activos, se procede con la asignación de dependencias; tal como se indicó anteriormente, las dependencias permiten conocer las necesidades de seguridad en caso de la materialización de una amenaza, debido que su efecto desencadenará en un daño secuencial de acuerdo al trabajo compartido o dependiente entre activos.

En la Figura 5.1, se puede observar la asignación de dependencia realizada para los Sistemas Informáticos de producción de la universidad [PROD_DTI], los cuales dependen directamente de la Red LAN [LAN_DTI] para la disponibilidad del servicio, así como de los Servidores de Producción (hardware) [PRODS_DTI] donde se encuentran alojados.

Además, se determinan dependencias adicionales en niveles inferiores, que son el apoyo para la seguridad de los niveles superiores, como es el caso de la unidad de Redes [REDES_DTI], responsables de mantener estabilizados los medios de comunicación, equipos activos y servidores; o también la unidad de Programación [PROG_DTI], encargados de mantener el correcto funcionamiento de los sistemas y servicios informáticos de la universidad.

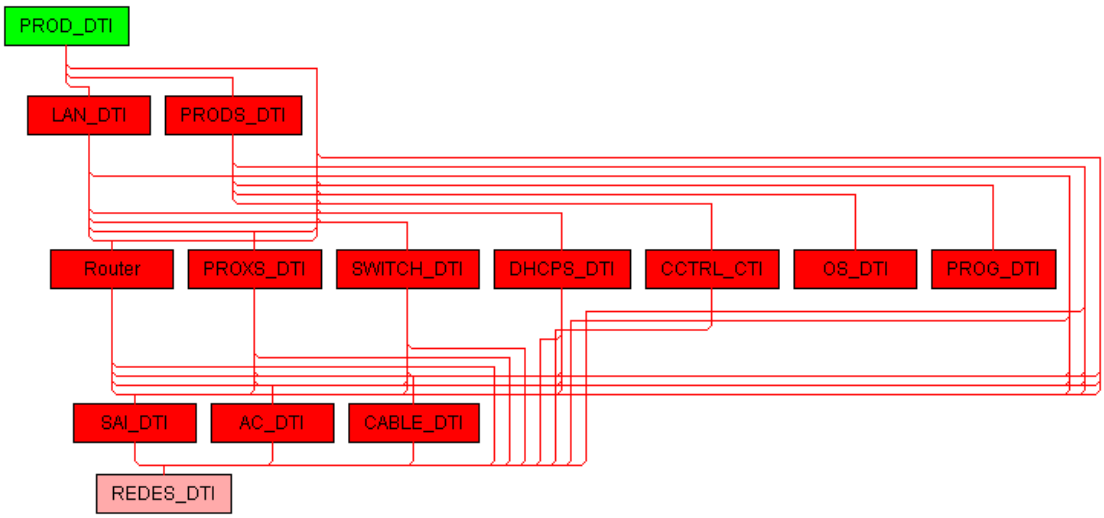

Figura 5.1: Dependencia de activos de los Sistemas Informáticos de Producción
Fuente: Análisis de riesgos Plan de Contingencia Informática PUCESD - PILAR
Elaborado: Ing. Franklin Carrasco

Las dependencias entre activos se las ordena de acuerdo a la posición de operación sobre o bajo un determinado activo, tal como se indica en la Figura 5.2

Figura 5.2: Posición de dependencia de activos - PILAR
Fuente: Análisis de riesgos Plan de Contingencia Informática PUCESD - PILAR

En la Figura 5.3, se observa la dependencia de todos los activos identificados para la contingencia en la Dirección de Tecnologías de la Información.

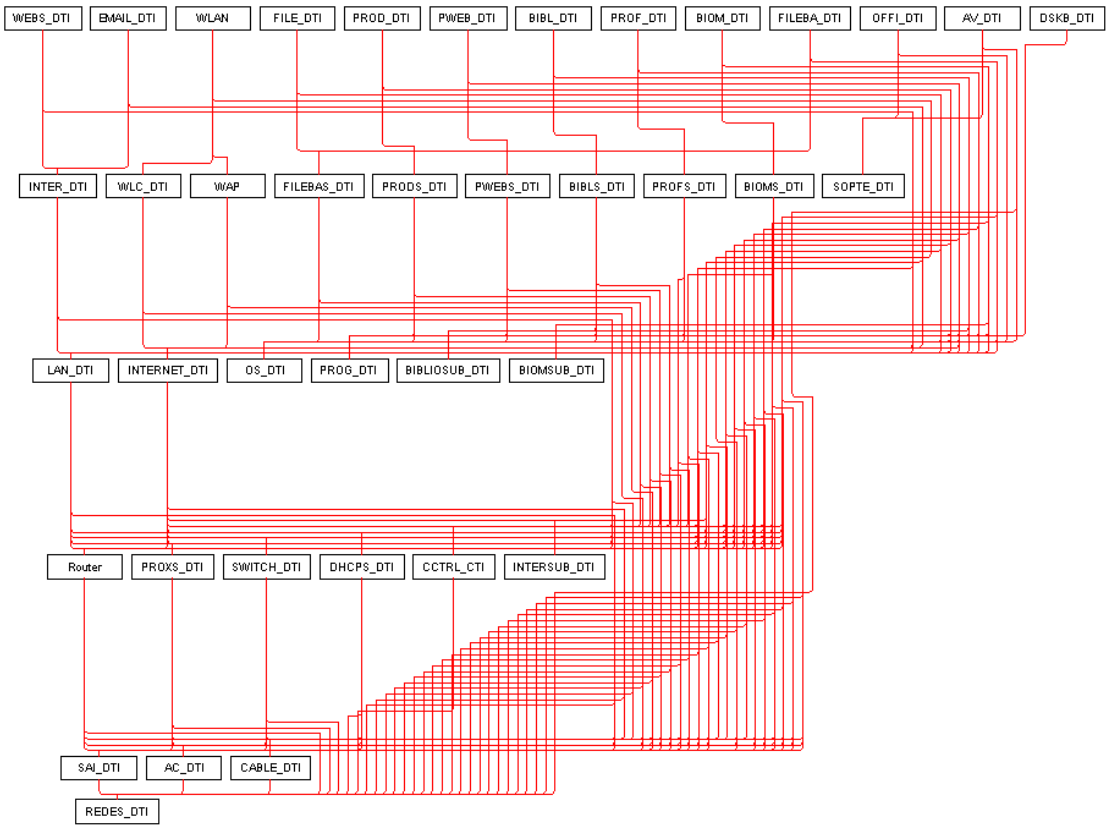

Figura 5.3: Diagrama de dependencia entre activos DTI - PUCESD
Fuente: Análisis de riesgos Plan de Contingencia Informática PUCESD - PILAR
Elaborado: Ing. Franklin Carrasco

5.1.2. Valoración de Activos

La valoración realizada para cada activo se realiza bajo los criterios de Disponibilidad (D), Integridad (I), Confidencialidad (C), Autenticidad (A) y Trazabilidad (T), desde la perspectiva del nivel de importancia que requiere. Se toma como referencia para cada activo la escala de

valoración del tipo cualitativo (rango numérico de 0 a 10), la misma que puede observarse en la anterior tabla 18, y su definición desde la tabla 19 hasta la tabla 30.

Tabla 43: Valoración servicios informáticos internos

[IS] SERVICIOS INTERNOS	**D**	**I**	**C**	**A**	**T**
[INTER_DTI] Internet	9	7	9	4	9
[WEBS_DTI] Portal Web PUCESD	7	7	5		
[EMAIL_DTI] Servicio Correo Electrónico Gmail	9	7	9	7	9
[FILE_DTI] Almacenamiento de Archivos	7	7	9	6	6

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 44: Valoración de aplicaciones informáticas Institucionales

[SW] APLICACIONES	**D**	**I**	**C**	**A**	**T**
[PROD_DTI] Sistemas Informáticos de Producción	9	9	9	9	9
[PWEB_DTI] Servicios Portal Web	7	6	4	3	3
[BIBL_DTI] Sistema de Biblioteca	8	6	0	1	3
[PROF_DTI] Sistema administrador de personal docente	4	6	7	6	7
[BIOM_DTI] Sistema para control de ingreso de personal	7	6	3	5	5
[FILEBA_DTI] Software para respaldo de archivos	4		3	9	7
[OFFI_DTI] Office – Ofimática	1				7
[AV_DTI] Antivirus	3				7
[OS_DTI] Sistema Operativo	3			7	7

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 45: Valoración de equipos activos, servidores y dispositivos (hardware)

[HW] EQUIPOS	D	I	C	A	T
[PRODS_DTI] Servidor de Producción	9	9	9	9	9
[DSKB_DTI] Disco para respaldos de Sistemas Informáticos de Producción	7	7	8	9	9
[PWEBS_DTI] Servidor Portal Web	7	7		5	7
[BIBLS_DTI] Servidor Sistema de Biblioteca	9	7		5	5
[PROFS_DTI] Servidor Sistema administrador de personal docente	4	6	6	4	4
[BIOMS_DTI] Servidor Sistema para control de ingreso de personal	7	6	6	6	7
[FILEBAS_DTI] Servidor Respaldo de Archivos	4	6	6	6	6
[PROXS_DTI] Servidor Proxy Firewall	9	7	7	9	9
[DHCPS_DTI] Servidor DHCP	7	5		7	5
[SWITCH_DTI] Switch	7	7		7	7
[Router] Router	9	9		9	9
[WLC_DTI] Controladora de red inalámbrica	6	3		7	7
[WAP] Punto de Acceso Inalámbrico	6	7		7	7

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 46: Valoración de redes y servicio de comunicación de datos

[COM] COMUNICACIONES	D	I	C	A	T
[LAN_DTI] Red LAN	7	7		7	7
[WLAN_DTI] Red LAN Inalámbrica	6	6		7	7
[INTERNET_DTI] Servicio de Internet	9	9	7	7	7

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 47: Valoración de equipamiento auxiliar

[AUX] ELEMENTOS AUXILIARES	D	I	C	A	T
[SAI_DTI] Sistema de alimentación ininterrumpida	7				7
[AC_DTI] Aire Acondicionado	7				7
[CABLE_DTI] Cableado de Datos	7				7

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 48: Valoración de servicios subcontratados

[SS] Servicios subcontratados	D	I	C	A	T
[BIBLIOSUB_DTI] Proveedor Sistema Biblioteca	3				
[BIOMSUB_DTI] Proveedor Sistema para control de ingreso de personal	3				
[INTERSUB_DTI] Servicio de Internet	9				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 49: Valoración de instalación física

[L] Instalaciones	D	I	C	A	T
[CCTRL_DTI] Cuarto de Control	9	9	8	9	9

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 50: Valoración de personal técnico

[P] Personal	**D**	**I**	**C**	**A**	**T**
[PROG_DTI] Administradores de Sistemas Informáticos - Programadores	7		9		
[REDES_DTI] Administradores de infraestructura y telecomunicaciones	7		9		
[SOPTE_DTI] Soporte Técnico	5				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

5.1.3. Valoración de Amenazas en Activos

Para determinar el riesgo e impacto de los daños ante la materialización de las amenazas, es necesario determinar aquellas que afectan directamente a los activos, valorándolas de acuerdo a la degradación de la Disponibilidad (D), Integridad (I), Confidencialidad (C), Autenticidad (A), Trazabilidad (T), y el nivel de probabilidad de ocurrencia (P). Las escalas de valoración para el Nivel de Probabilidad de Ocurrencia, así como para el Valor de Degradación, son empleadas por Magerit a través de la herramienta PILAR versión 5.4.4, y presentadas en las tablas 51 y 52:

Tabla 51: Nivel de Probabilidad de Ocurrencia

VALOR	DETALLE
MA	Muy alta
CS	Casi seguro
P	Posible
PP	Poco Probable
MR	Muy rara vez

Fuente: Herramienta PILAR versión 5.4.4

Tabla 52: Degradación de Valor

VALOR	DETALLE
MA	Muy Alta
A	Alta
M	Media
B	Baja
MB	Muy Baja

Fuente: Herramienta PILAR versión 5.4.4

La valoración de estas amenazas permitirá también determinar las salvaguardas que se activarán durante la contingencia informática para mantener los procesos del negocio, las mismas que se resaltan en las siguientes tablas:

[IS] SERVICIOS INTERNOS

Tabla 53: Amenazas en servicio interno de Internet

[INTER_DTI] INTERNET	P	D	I	C	A	T
Valoración Total		A	M	A	MA	MA
[I.8] Fallo de servicios de comunicaciones	P	A				
[E.1] Errores de los usuarios	P	M	M	M		
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.9] Errores de [re-]encaminamiento	P			M		
[E.10] Errores de secuencia	P		M			
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	M				
[E.19] Fugas de información	P			M		
[E.24] Caída del sistema por agotamiento de recursos	P	A				
[A.5] Suplantación de la identidad	P		M	A	MA	
[A.6] Abuso de privilegios de acceso	P	B	M	A	MA	
[A.7] Uso no previsto	P	M	M	M		
[A.9] [Re-] encaminamiento de mensajes	P			M		
[A.10] Alteración de secuencia	P		M			
[A.11] Acceso no autorizado	P		M	A	MA	
[A.12] Análisis de tráfico	P			B		
[A.13] Repudio (negación de actuaciones)	MA					MA
[A.14] Interceptación de información (escucha)	P			M		
[A.15] Modificación de la información	P		M			
[A.18] Destrucción de la información	P	A				
[A.19] Revelación de información	P			A		
[A.24] Denegación de servicio	MA	A				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 54: Amenazas en servicio Portal Web Institucional

[WEBS_DTI] PORTAL WEB PUCESD	P	D	I	C	A	T
Valoración Total		MA	MA	MA		
[I.5] Avería de origen físico o lógico	P	A				
[E.1] Errores de los usuarios	P	B	M	M		
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.8] Difusión de software dañino	P	M	M	M		
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	A				
[E.19] Fugas de información	P			M		
[E.20] Vulnerabilidades de los programas (software)	P	B	M	M		
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	B	B			
[A.5] Suplantación de la identidad	P		A	A		
[A.6] Abuso de privilegios de acceso	P	B	M	M		
[A.7] Uso no previsto	P	B	M	M		
[A.8] Difusión software dañino	P	MA	MA	MA		
[A.11] Acceso no autorizado	P		M	A		
[A.15] Modificación de la información	P		A			
[A.18] Destrucción de la información	P	A				
[A.19] Revelación de información	P			A		
[A.22] Manipulación de programas	P	A	MA	MA		

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 55: Amenazas en servicio de correo electrónico institucional Gmail

[EMAIL_DTI] SERVICIO CORREO ELECTRÓNICO GMAIL	P	D	I	C	A	T
Valoración Total		A	A	A	MA	MA
[E.1] Errores de los usuarios	P	M	M	M		
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	M				
[E.19] Fugas de información	P			M		

[E.24] Caída del sistema por agotamiento de recursos	MA	A				
[A.5] Suplantación de la identidad	P		A	A	MA	
[A.6] Abuso de privilegios de acceso	P	B	M	M	MA	
[A.7] Uso no previsto	P	B	M	M		
[A.11] Acceso no autorizado	P		M	A	MA	
[A.13] Repudio (negación de actuaciones)	MA					MA
[A.15] Modificación de la información	MA		A			
[A.18] Destrucción de la información	P	A				
[A.19] Revelación de información	P			A		
[A.24] Denegación de servicio	MA	A				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 56: Amenazas en servicio de almacenamiento de archivos

[FILE_DTI] ALMACENAMIENTO DE ARCHIVOS	**P**	**D**	**I**	**C**	**A**	**T**
Valoración Total		A	A	A	MA	MA
[E.1] Errores de los usuarios	P	M	M	M		
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	M				
[E.19] Fugas de información	P			M		
[E.24] Caída del sistema por agotamiento de recursos	MA	A				
[A.5] Suplantación de la identidad	P		A	A	MA	
[A.6] Abuso de privilegios de acceso	P	B	M	M	MA	
[A.7] Uso no previsto	P	B	M	M		
[A.11] Acceso no autorizado	P		M	A	MA	
[A.13] Repudio (negación de actuaciones)	MA					MA
[A.15] Modificación de la información	MA		A			
[A.18] Destrucción de la información	P	A				
[A.19] Revelación de información	P			A		

[A.24] Denegación de servicio	MA	A				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

[SW] APLICACIONES

Tabla 57: Amenazas en sistemas informáticos de producción

[PROD_DTI] SISTEMAS INFORMÁTICOS DE PRODUCCIÓN	**P**	**D**	**I**	**C**	**A**	**T**
Valoración Total		MA	MA	MA	MA	MA
[I.5] Avería de origen físico o lógico	P	A				
[E.1] Errores de los usuarios	P	B	M	M		
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.3] Errores de monitorización (log)	P		B			
[E.4] Errores de configuración	P		B			
[E.8] Difusión de software dañino	P	M	M	M		
[E.15] Alteración de la información	P		M			
[E.18] Destrucción de la información	P	B				
[E.19] Fugas de información	P			M		
[E.20] Vulnerabilidades de los programas (software)	P	B	M	M		
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	B	B			
[E.24] Caída del sistema por agotamiento de recursos	MA	A				
[E.28] Indisponibilidad del personal	P	M				
[A.3] Manipulación de los registros de actividad (log)	CS		A			
[A.4] Manipulación de los ficheros de configuración	MA	M	M	M		
[A.5] Suplantación de la identidad	P		A	A	MA	
[A.6] Abuso de privilegios de acceso	P	B	M	M	MA	
[A.7] Uso no previsto	P	B	M	M		
[A.8] Difusión software dañino	P	MA	MA	MA		
[A.11] Acceso no autorizado	P		M	A	MA	
[A.13] Repudio (negación de actuaciones)	MA		MA		MA	MA
[A.15] Modificación de la información	P		A			
[A.18] Destrucción de la información	P	M				

[A.19] Revelación de información	MA			A		
[A.22] Manipulación de programas	P	A	MA	MA		
[A.24] Denegación de servicio	MA	A				
[A.28] Indisponibilidad del personal	P	M				
[A.29] Extorsión	P	B	MA	MA		
[A.30] Ingeniería social (picaresca)	P	B	MA	MA		

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 58: Amenazas en servicios del portal web PUCE SD

[PWEB_DTI] SERVICIOS PORTAL WEB	**P**	**D**	**I**	**C**	**A**	**T**
Valoración Total		MA	MA	MA	MA	MA
[I.5] Avería de origen físico o lógico	P	A				
[E.1] Errores de los usuarios	P	B	M	M		
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.3] Errores de monitorización (log)	P		B			
[E.4] Errores de configuración	P		B			
[E.8] Difusión de software dañino	P	M	M	M		
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	A				
[E.19] Fugas de información	P			M		
[E.20] Vulnerabilidades de los programas (software)	P	B	M	M		
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	B	B			
[E.24] Caída del sistema por agotamiento de recursos	MA	A				
[A.3] Manipulación de los registros de actividad (log)	CS		A			
[A.4] Manipulación de los ficheros de configuración	MA	M	M	M		
[A.5] Suplantación de la identidad	P		A	A	MA	
[A.6] Abuso de privilegios de acceso	P	B	M	M	MA	
[A.7] Uso no previsto	P	B	M	M		
[A.8] Difusión software dañino	P	MA	MA	MA		
[A.11] Acceso no autorizado	P		M	A	MA	
[A.13] Repudio (negación de actuaciones)	MA		MA		MA	MA
[A.15] Modificación de la información	P		A			
[A.18] Destrucción de la información	P	A				

[A.19] Revelación de información	P			A		
[A.22] Manipulación de programas	P	A	MA	MA		
[A.24] Denegación de servicio	MA	A				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 59: Amenazas en sistema de biblioteca

[BIBL_DTI] SISTEMA DE BIBLIOTECA	**P**	**D**	**I**	**C**	**A**	**T**
Valoración Total		MA	MA	MA	MA	MA
[I.5] Avería de origen físico o lógico	P	A				
[E.1] Errores de los usuarios	P	B	M	M		
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.8] Difusión de software dañino	P	M	M	M		
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	A				
[E.19] Fugas de información	P			M		
[E.20] Vulnerabilidades de los programas (software)	P	B	M	M		
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	B	B			
[E.24] Caída del sistema por agotamiento de recursos	MA	A				
[A.5] Suplantación de la identidad	P		A	A	MA	
[A.6] Abuso de privilegios de acceso	P	B	M	M	MA	
[A.7] Uso no previsto	P	B	M	M		
[A.8] Difusión software dañino	P	MA	MA	MA		
[A.11] Acceso no autorizado	P		M	A	MA	
[A.13] Repudio (negación de actuaciones)	MA					MA
[A.15] Modificación de la información	P		A			
[A.18] Destrucción de la información	P	A				
[A.19] Revelación de información	P			A		
[A.22] Manipulación de programas	P	A	MA	MA		
[A.24] Denegación de servicio	MA	A				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 60: Amenazas en sistema administrador de personal docente

[PROF_DTI] SISTEMA ADMINISTRADOR DE PERSONAL DOCENTE	P	D	I	C	A	T
Valoración Total		MA	MA	MA	MA	
[I.5] Avería de origen físico o lógico	P	A				
[E.1] Errores de los usuarios	P	B	M	M		
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.8] Difusión de software dañino	P	M	M	M		
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	A				
[E.19] Fugas de información	P			M		
[E.20] Vulnerabilidades de los programas (software)	P	B	M	M		
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	B	B			
[A.5] Suplantación de la identidad	P		A	A	MA	
[A.6] Abuso de privilegios de acceso	P	B	M	M		
[A.7] Uso no previsto	P	B	M	M		
[A.8] Difusión software dañino	P	MA	MA	MA		
[A.11] Acceso no autorizado	P		M	A		
[A.15] Modificación de la información	P		A			
[A.18] Destrucción de la información	P	A				
[A.19] Revelación de información	P			A		
[A.22] Manipulación de programas	P	A	MA	MA		

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 61: Amenazas en sistema para control de ingreso de personal

[BIOM_DTI] SISTEMA PARA CONTROL DE INGRESO DE PERSONAL	P	D	I	C	A	T
Valoración Total		MA	MA	MA	MA	MA
[I.5] Avería de origen físico o lógico	P	A				
[E.1] Errores de los usuarios	P	B	M	M		
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.8] Difusión de software dañino	P	M	M	M		
[E.15] Alteración de la información	P		B			

[E.18] Destrucción de la información	P	A				
[E.19] Fugas de información	P			M		
[E.20] Vulnerabilidades de los programas (software)	P	B	M	M		
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	B	B			
[E.24] Caída del sistema por agotamiento de recursos	MA	A				
[A.5] Suplantación de la identidad	P		A	A	MA	
[A.6] Abuso de privilegios de acceso	P	B	M	M	MA	
[A.7] Uso no previsto	P	B	M	M		
[A.8] Difusión software dañino	P	MA	MA	MA		
[A.11] Acceso no autorizado	P		M	A	MA	
[A.13] Repudio (negación de actuaciones)	MA					MA
[A.15] Modificación de la información	P		A			
[A.18] Destrucción de la información	P	A				
[A.19] Revelación de información	P			A		
[A.22] Manipulación de programas	P	A	MA	MA		
[A.24] Denegación de servicio	MA	A				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 62: Amenazas en software para respaldo de archivos

[FILEBA_DTI] SOFTWARE PARA RESPALDO DE ARCHIVOS	**P**	**D**	**I**	**C**	**A**	**T**
Valoración Total		MA		MA	MA	MA
[I.5] Avería de origen físico o lógico	P	A				
[E.1] Errores de los usuarios	P	B		M		
[E.2] Errores del administrador del sistema / de la seguridad	P	M		M		
[E.8] Difusión de software dañino	P	M		M		
[E.18] Destrucción de la información	P	A				
[E.19] Fugas de información	P			M		
[E.20] Vulnerabilidades de los programas (software)	P	B		M		
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	B				
[E.24] Caída del sistema por agotamiento de recursos	MA	A				

[A.5] Suplantación de la identidad	P			A	MA	
[A.6] Abuso de privilegios de acceso	P	B		M	MA	
[A.7] Uso no previsto	P	B		M		
[A.8] Difusión software dañino	P	MA		MA		
[A.11] Acceso no autorizado	P			A	MA	
[A.13] Repudio (negación de actuaciones)	MA					MA
[A.18] Destrucción de la información	P	A				
[A.19] Revelación de información	P			A		
[A.22] Manipulación de programas	P	A		MA		
[A.24] Denegación de servicio	MA	A				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 63: Amenazas en Ofimática - Ms Office

[OFFI_DTI] OFFICE – OFIMÁTICA	**P**	**D**	**I**	**C**	**A**	**T**
Valoración Total		MA				
[I.5] Avería de origen físico o lógico	P	A				
[E.1] Errores de los usuarios	P	B				
[E.2] Errores del administrador del sistema / de la seguridad	P	M				
[E.8] Difusión de software dañino	P	M				
[E.18] Destrucción de la información	P	A				
[E.20] Vulnerabilidades de los programas (software)	P	B				
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	B				
[A.6] Abuso de privilegios de acceso	P	B				
[A.7] Uso no previsto	P	B				
[A.8] Difusión software dañino	P	MA				
[A.18] Destrucción de la información	P	A				
[A.22] Manipulación de programas	P	A				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 64: Amenazas en antivirus

[AV_DTI] ANTIVIRUS	P	D	I	C	A	T
Valoración Total		MA				
[I.5] Avería de origen físico o lógico	P	A				
[E.1] Errores de los usuarios	P	B				
[E.2] Errores del administrador del sistema / de la seguridad	P	M				
[E.8] Difusión de software dañino	P	M				
[E.18] Destrucción de la información	P	A				
[E.20] Vulnerabilidades de los programas (software)	P	B				
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	B				
[A.6] Abuso de privilegios de acceso	P	B				
[A.7] Uso no previsto	P	B				
[A.8] Difusión software dañino	P	MA				
[A.18] Destrucción de la información	P	A				
[A.22] Manipulación de programas	P	A				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 65: Amenazas en sistema operativo

[OS_DTI] SISTEMA OPERATIVO	P	D	I	C	A	T
Valoración Total		MA	MA	MA	MA	
[I.5] Avería de origen físico o lógico	P	A				
[E.1] Errores de los usuarios	P	B	M	M		
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.8] Difusión de software dañino	P	M	M	M		
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	A				
[E.19] Fugas de información	P			M		
[E.20] Vulnerabilidades de los programas (software)	P	B	M	M		
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	B	B			
[A.5] Suplantación de la identidad	P		A	A	MA	
[A.6] Abuso de privilegios de acceso	P	B	M	M		

[A.7] Uso no previsto	P	B	M	M		
[A.8] Difusión software dañino	P	MA	MA	MA		
[A.11] Acceso no autorizado	P		M	A		
[A.15] Modificación de la información	P		A			
[A.18] Destrucción de la información	P	A				
[A.19] Revelación de información	P			A		
[A.22] Manipulación de programas	P	A	MA	MA		

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

[HW] EQUIPOS

Tabla 66: Amenazas en servidor de producción – hardware

[PRODS_DTI] SERVIDOR DE PRODUCCIÓN	**P**	**D**	**I**	**C**	**A**	**T**
Valoración Total		MA	MA	MA	MA	
[N.1] Fuego	PP	MA				
[N.2] Daños por agua	PP	A				
[N.*] Desastres naturales	PP	MA				
[I.1] Fuego	P	MA				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	MA				
[I.3] Contaminación medioambiental	PP	A				
[I.4] Contaminación electromagnética	P	M				
[I.5] Avería de origen físico o lógico	P	A				
[I.6] Corte de suministro eléctrico	P	MA				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	MA				
[I.11] Emanaciones electromagnéticas	P			B		
[E.1] Errores de los usuarios	MA	M	M	M		
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	B				
[E.19] Fugas de información	P			M		

[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M				
[E.24] Caída del sistema por agotamiento de recursos	MA	A				
[E.25] Pérdida de equipos	P	MA		MA		
[A.5] Suplantación de la identidad	MA		M	A	MA	
[A.6] Abuso de privilegios de acceso	P	M	MA	MA		
[A.7] Uso no previsto	P	M	M	MA		
[A.11] Acceso no autorizado	P	M	MA	MA		
[A.15] Modificación de la información	MA		MA			
[A.18] Destrucción de la información	MA	A				
[A.19] Revelación de información	MA			MA		
[A.23] Manipulación de hardware	P	A		A		
[A.24] Denegación de servicio	P	MA				
[A.25] Robo de equipos	PP	MA		MA		
[A.26] Ataque destructivo	P	MA				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 67: Amenazas en disco externo para respaldo de sistemas informáticos de producción

[DSKB_DTI] DISCO PARA RESPALDOS DE SISTEMAS INFORMÁTICOS DE PRODUCCIÓN	**P**	**D**	**I**	**C**	**A**	**T**
Valoración Total		MA	MA	MA	MA	
[N.1] Fuego	PP	MA				
[N.2] Daños por agua	PP	A				
[N.*] Desastres naturales	PP	MA				
[I.1] Fuego	P	MA				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	MA				
[I.3] Contaminación medioambiental	PP	A				
[I.4] Contaminación electromagnética	P	M				
[I.5] Avería de origen físico o lógico	P	A				
[I.6] Corte de suministro eléctrico	P	MA				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	MA				

[I.11] Emanaciones electromagnéticas	P			B		
[E.1] Errores de los usuarios	MA	M	M	M		
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	B				
[E.19] Fugas de información	P			M		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M				
[E.24] Caída del sistema por agotamiento de recursos	MA	A				
[E.25] Pérdida de equipos	P	MA		A		
[A.5] Suplantación de la identidad	MA		M	A	MA	
[A.6] Abuso de privilegios de acceso	P	M	M	A		
[A.7] Uso no previsto	P	M	B	M		
[A.11] Acceso no autorizado	P	M	M	A		
[A.15] Modificación de la información	MA		MA			
[A.18] Destrucción de la información	MA	A				
[A.19] Revelación de información	MA			MA		
[A.23] Manipulación de hardware	P	A		A		
[A.24] Denegación de servicio	P	MA				
[A.25] Robo de equipos	P	MA		A		
[A.26] Ataque destructivo	P	MA				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

Tabla 68: Amenazas en servidor portal web - hardware

[PWEBS_DTI] SERVIDOR PORTAL WEB	**P**	**D**	**I**	**C**	**A**	**T**
Valoración Total		MA	MA	MA	MA	MA
[N.1] Fuego	PP	MA				
[N.2] Daños por agua	PP	A				
[N.*] Desastres naturales	PP	MA				
[I.1] Fuego	P	MA				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	MA				
[I.3] Contaminación medioambiental	PP	A				
[I.4] Contaminación electromagnética	P	M				

[I.5] Avería de origen físico o lógico	P	A				
[I.6] Corte de suministro eléctrico	P	MA				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	MA				
[I.11] Emanaciones electromagnéticas	P			B		
[E.1] Errores de los usuarios	P	M	M	M		
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	M				
[E.19] Fugas de información	P			M		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M				
[E.24] Caída del sistema por agotamiento de recursos	MA	A				
[E.25] Pérdida de equipos	P	MA		MA		
[A.5] Suplantación de la identidad	P		A	A	MA	
[A.6] Abuso de privilegios de acceso	P	M	MA	MA	MA	
[A.7] Uso no previsto	P	M	M	MA		
[A.11] Acceso no autorizado	P	M	MA	MA	MA	
[A.13] Repudio (negación de actuaciones)	MA					MA
[A.15] Modificación de la información	MA		A			
[A.18] Destrucción de la información	P	A				
[A.19] Revelación de información	P			A		
[A.23] Manipulación de hardware	P	A		A		
[A.24] Denegación de servicio	P	MA				
[A.25] Robo de equipos	PP	MA		MA		
[A.26] Ataque destructivo	P	MA				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 69: Amenazas en servidor sistema de biblioteca – hardware

[BIBLS_DTI] SERVIDOR SISTEMA DE BIBLIOTECA	**P**	**D**	**I**	**C**	**A**	**T**
Valoración Total		MA	MA	MA	MA	MA
[N.1] Fuego	PP	MA				
[N.2] Daños por agua	PP	A				
[N.*] Desastres naturales	PP	MA				

[I.1] Fuego	P	MA				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	MA				
[I.3] Contaminación medioambiental	PP	A				
[I.4] Contaminación electromagnética	P	M				
[I.5] Avería de origen físico o lógico	P	A				
[I.6] Corte de suministro eléctrico	P	MA				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	MA				
[I.11] Emanaciones electromagnéticas	P			B		
[E.1] Errores de los usuarios	P	B	M	M		
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.8] Difusión software dañino	P	M	M	M		
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	A				
[E.19] Fugas de información	P			M		
[E.20] Vulnerabilidades de los programas (software)	P	B	M	M		
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	B	B			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M				
[E.24] Caída del sistema por agotamiento de recursos	MA	A				
[E.25] Pérdida de equipos	PP	MA		MA		
[A.5] Suplantación de la identidad	P		A	A	MA	
[A.6] Abuso de privilegios de acceso	P	M	M	A		
[A.7] Uso no previsto	P	B	B	M		
[A.8] Difusión de software dañino	P	MA	MA	MA		
[A.11] Acceso no autorizado	P	M	M	A		
[A.15] Modificación de la información	P		A			
[A.18] Destrucción de la información	P	A				
[A.19] Revelación de información	P			A		
[A.22] Manipulación de programas	P	A	MA	MA		
[A.23] Manipulación de hardware	P	A		A		
[A.24] Denegación de servicio	P	MA				
[A.25] Robo de equipos	PP	MA		MA		
[A.26] Ataque destructivo	P	MA				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 70: Amenazas en servidor sistema administrador de personal docente - hardware

[PROFS_DTI] SERVIDOR SISTEMA ADMINISTRADOR DE PERSONAL DOCENTE	P	D	I	C	A	T
Valoración Total		MA	MA	MA	MA	MA
[N.1] Fuego	PP	MA				
[N.2] Daños por agua	PP	A				
[N.*] Desastres naturales	PP	MA				
[I.1] Fuego	P	MA				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	PP	MA				
[I.3] Contaminación medioambiental	P	A				
[I.4] Contaminación electromagnética	P	M				
[I.5] Avería de origen físico o lógico	P	A				
[I.6] Corte de suministro eléctrico	P	MA				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	MA				
[I.11] Emanaciones electromagnéticas	P			B		
[E.1] Errores de los usuarios	P	B	M	M		
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.8] Difusión software dañino	P	M	M	M		
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	A				
[E.19] Fugas de información	P			M		
[E.20] Vulnerabilidades de los programas (software)	P	B	M	M		
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	B	B			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M				
[E.24] Caída del sistema por agotamiento de recursos	MA	A				
[E.25] Pérdida de equipos	P	MA		MA		
[A.5] Suplantación de la identidad	P		A	A	MA	
[A.6] Abuso de privilegios de acceso	P	M	MA	MA	MA	
[A.7] Uso no previsto	P	M	M	MA		
[A.8] Difusión de software dañino	P	MA	MA	MA		
[A.11] Acceso no autorizado	P	M	MA	MA	MA	
[A.13] Repudio (negación de actuaciones)	MA					MA
[A.15] Modificación de la información	P		A			
[A.18] Destrucción de la información	P	A				
[A.19] Revelación de información	P			A		
[A.22] Manipulación de programas	P	A	MA	MA		
[A.23] Manipulación de hardware	P	A		A		
[A.24] Denegación de servicio	P	MA				

[A.25] Robo de equipos	PP	MA		MA		
[A.26] Ataque destructivo	P	MA				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 71: Amenazas en servidor sistema para control de ingreso de personal

[BIOMS_DTI] SERVIDOR SISTEMA PARA CONTROL DE INGRESO DE PERSONAL	**P**	**D**	**I**	**C**	**A**	**T**
Valoración Total		MA	MA	MA	MA	MA
[N.1] Fuego	PP	MA				
[N.2] Daños por agua	PP	A				
[N.*] Desastres naturales	PP	MA				
[I.1] Fuego	P	MA				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	MA				
[I.3] Contaminación medioambiental	PP	A				
[I.4] Contaminación electromagnética	P	M				
[I.5] Avería de origen físico o lógico	P	A				
[I.6] Corte de suministro eléctrico	P	MA				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	MA				
[I.11] Emanaciones electromagnéticas	P			B		
[E.1] Errores de los usuarios	P	B	M	M		
[E.2] Errores del administrador del sistema / de la seguridad	PP	M	M	M		
[E.8] Difusión software dañino	P	M	M	M		
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	A				
[E.19] Fugas de información	P			M		
[E.20] Vulnerabilidades de los programas (software)	P	B	M	M		
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	B	B			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M				
[E.24] Caída del sistema por agotamiento de recursos	MA	A				
[E.25] Pérdida de equipos	PP	MA		MA		
[A.5] Suplantación de la identidad	P		A	A	MA	

[A.6] Abuso de privilegios de acceso	P	M	M	A	MA	
[A.7] Uso no previsto	P	B	B	M		
[A.8] Difusión de software dañino	P	MA	MA	MA		
[A.11] Acceso no autorizado	P	M	M	A	MA	
[A.13] Repudio (negación de actuaciones)	MA					MA
[A.15] Modificación de la información	P		A			
[A.18] Destrucción de la información	P	A				
[A.19] Revelación de información	P			A		
[A.22] Manipulación de programas	P	A	MA	MA		
[A.23] Manipulación de hardware	P	A		A		
[A.24] Denegación de servicio	P	MA				
[A.25] Robo de equipos	PP	MA		MA		
[A.26] Ataque destructivo	P	MA				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 72: Amenazas en servidor de respaldo de archivos - hardware

[FILEBAS_DTI] SERVIDOR RESPALDO DE ARCHIVOS	**P**	**D**	**I**	**C**	**A**	**T**
Valoración Total		MA	M	MA		
[N.1] Fuego	PP	MA				
[N.2] Daños por agua	PP	A				
[N.*] Desastres naturales	PP	MA				
[I.1] Fuego	P	MA				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	MA				
[I.3] Contaminación medioambiental	PP	A				
[I.4] Contaminación electromagnética	P	M				
[I.5] Avería de origen físico o lógico	P	A				
[I.6] Corte de suministro eléctrico	P	MA				
[I.7] Condiciones inadecuadas de temperatura o humedad	PP	MA				
[I.11] Emanaciones electromagnéticas	P			B		

[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M				
[E.24] Caída del sistema por agotamiento de recursos	MA	A				
[E.25] Pérdida de equipos	PP	MA		MA		
[A.6] Abuso de privilegios de acceso	P	M	M	A		
[A.7] Uso no previsto	P	B	B	M		
[A.11] Acceso no autorizado	P	M	M	A		
[A.23] Manipulación de hardware	P	A				
[A.24] Denegación de servicio	P	MA				
[A.25] Robo de equipos	PP	MA		MA		
[A.26] Ataque destructivo	P	MA				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 73: Amenazas en servidor proxy/firewall – hardware

[PROXS_DTI] SERVIDOR PROXY FIREWALL	**P**	**D**	**I**	**C**	**A**	**T**
Valoración Total		MA	MA	MA	MA	MA
[N.1] Fuego	PP	MA				
[N.2] Daños por agua	PP	A				
[N.*] Desastres naturales	PP	MA				
[I.1] Fuego	P	MA				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	MA				
[I.3] Contaminación medioambiental	PP	A				
[I.4] Contaminación electromagnética	P	M				
[I.5] Avería de origen físico o lógico	P	A				
[I.6] Corte de suministro eléctrico	P	MA				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	MA				
[I.8] Fallo de servicios de comunicaciones	P	A				
[I.11] Emanaciones electromagnéticas	P			B		
[E.1] Errores de los usuarios	P	B	M	M		

[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.8] Difusión software dañino	P	M	M	M		
[E.9] Errores de [re-]encaminamiento	P			M		
[E.10] Errores de secuencia	P		M			
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	A				
[E.19] Fugas de información	P			M		
[E.20] Vulnerabilidades de los programas (software)	P	B	M	M		
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	B	B			
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M				
[E.24] Caída del sistema por agotamiento de recursos	P	A				
[E.25] Pérdida de equipos	PP	MA		MA		
[A.5] Suplantación de la identidad	P		M	A	MA	
[A.6] Abuso de privilegios de acceso	P	M	M	A	MA	
[A.7] Uso no previsto	P	M	M	M		
[A.8] Difusión de software dañino	P	MA	MA	MA		
[A.9] [Re-]encaminamiento de mensajes	P			M		
[A.10] Alteración de secuencia	P		M			
[A.11] Acceso no autorizado	P	M	M	A	MA	
[A.12] Análisis de tráfico	P			B		
[A.13] Repudio (negación de actuaciones)	MA					MA
[A.14] Interceptación de información (escucha)	P			M		
[A.15] Modificación de la información	P		M			
[A.18] Destrucción de la información	P	A				
[A.19] Revelación de información	P			A		
[A.22] Manipulación de programas	P	A	MA	MA		
[A.23] Manipulación de hardware	P	A		A		
[A.24] Denegación de servicio	MA	A				
[A.25] Robo de equipos	PP	MA		MA		
[A.26] Ataque destructivo	P	MA				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 74: Amenazas en servidor dhcp – hardware

[DHCPS_DTI] SERVIDOR DHCP	P	D	I	C	A	T
Valoración Total		MA	A	MA	MA	MA
[N.1] Fuego	PP	MA				
[N.2] Daños por agua	PP	A				
[N.*] Desastres naturales	PP	MA				
[I.1] Fuego	P	MA				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	MA				
[I.3] Contaminación medioambiental	PP	A				
[I.4] Contaminación electromagnética	P	M				
[I.5] Avería de origen físico o lógico	PP	A				
[I.6] Corte de suministro eléctrico	P	MA				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	MA				
[I.11] Emanaciones electromagnéticas	P			B		
[E.1] Errores de los usuarios	P	M	M	M		
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	M				
[E.19] Fugas de información	P			M		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M				
[E.24] Caída del sistema por agotamiento de recursos	MA	A				
[E.25] Pérdida de equipos	P	M		MA		
[A.5] Suplantación de la identidad	P		A	A	MA	
[A.6] Abuso de privilegios de acceso	P	M	M	A	MA	
[A.7] Uso no previsto	P	M	B	M		
[A.11] Acceso no autorizado	P	M	M	A	MA	
[A.13] Repudio (negación de actuaciones)	MA					MA
[A.15] Modificación de la información	MA		A			
[A.18] Destrucción de la información	P	A				
[A.19] Revelación de información	P			A		
[A.23] Manipulación de hardware	P	MA		A		
[A.24] Denegación de servicio	P	MA				
[A.25] Robo de equipos	PP	M		MA		
[A.26] Ataque destructivo	P	MA				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 75: Amenazas en Switches

[SWITCH_DTI] SWITCH	P	D	I	C	A	T
Valoración Total		MA	M	A	MA	MA
[N.1] Fuego	PP	MA				
[N.2] Daños por agua	PP	A				
[N.*] Desastres naturales	PP	MA				
[I.1] Fuego	P	MA				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	MA				
[I.3] Contaminación medioambiental	PP	A				
[I.4] Contaminación electromagnética	P	M				
[I.5] Avería de origen físico o lógico	P	A				
[I.6] Corte de suministro eléctrico	P	MA				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	MA				
[I.8] Fallo de servicios de comunicaciones	P	A				
[I.11] Emanaciones electromagnéticas	P			B		
[E.1] Errores de los usuarios	P	M	M	M		
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.9] Errores de [re-]encaminamiento	P			M		
[E.10] Errores de secuencia	P		M			
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	M				
[E.19] Fugas de información	P			M		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M				
[E.24] Caída del sistema por agotamiento de recursos	P	A				
[E.25] Pérdida de equipos	P	M		A		
[A.5] Suplantación de la identidad	P		M	A	MA	
[A.6] Abuso de privilegios de acceso	P	M	M	A	MA	
[A.7] Uso no previsto	P	M	M	M		
[A.9] [Re-]encaminamiento de mensajes	P			M		
[A.10] Alteración de secuencia	P		M			
[A.11] Acceso no autorizado	P	M	M	A	MA	
[A.12] Análisis de tráfico	P			B		
[A.13] Repudio (negación de actuaciones)	MA					MA
[A.14] Interceptación de información (escucha)	P			M		
[A.15] Modificación de la información	P		M			

[A.18] Destrucción de la información	P	A				
[A.19] Revelación de información	P			A		
[A.23] Manipulación de hardware	P	MA		A		
[A.24] Denegación de servicio	MA	A				
[A.25] Robo de equipos	P	M		A		
[A.26] Ataque destructivo	P	MA				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 76: Amenazas en Router

[ROUTER] ROUTER	**P**	**D**	**I**	**C**	**A**	**T**
Valoración Total		MA	A	A	MA	MA
[N.1] Fuego	PP	MA				
[N.2] Daños por agua	PP	A				
[N.*] Desastres naturales	PP	MA				
[I.1] Fuego	P	MA				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	MA				
[I.3] Contaminación medioambiental	PP	A				
[I.4] Contaminación electromagnética	P	M				
[I.5] Avería de origen físico o lógico	P	A				
[I.6] Corte de suministro eléctrico	P	MA				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	MA				
[I.11] Emanaciones electromagnéticas	P			B		
[E.1] Errores de los usuarios	P	M	M	M		
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	M				
[E.19] Fugas de información	P			M		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M				
[E.24] Caída del sistema por agotamiento de recursos	MA	A				
[E.25] Pérdida de equipos	P	M		A		

[A.5] Suplantación de la identidad	P		A	A	MA	
[A.6] Abuso de privilegios de acceso	P	M	M	A	MA	
[A.7] Uso no previsto	P	M	B	M		
[A.11] Acceso no autorizado	P	M	M	A	MA	
[A.13] Repudio (negación de actuaciones)	MA					MA
[A.15] Modificación de la información	MA		A			
[A.18] Destrucción de la información	P	A				
[A.19] Revelación de información	P			A		
[A.23] Manipulación de hardware	P	MA		A		
[A.24] Denegación de servicio	P	MA				
[A.25] Robo de equipos	P	M		A		
[A.26] Ataque destructivo	P	MA				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 77: Amenazas en controladora de red inalámbrica

[WLC_DTI] CONTROLADORA DE RED INALÁMBRICA	**P**	**D**	**I**	**C**	**A**	**T**
Valoración Total		MA	A		MA	MA
[N.1] Fuego	PP	MA				
[N.2] Daños por agua	PP	A				
[N.*] Desastres naturales	PP	MA				
[I.1] Fuego	P	MA				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	MA				
[I.3] Contaminación medioambiental	PP	A				
[I.4] Contaminación electromagnética	P	M				
[I.5] Avería de origen físico o lógico	P	A				
[I.6] Corte de suministro eléctrico	P	MA				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	MA				
[E.1] Errores de los usuarios	P	M	M			
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M			
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	M				

[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M				
[E.24] Caída del sistema por agotamiento de recursos	MA	A				
[E.25] Pérdida de equipos	P	M				
[A.5] Suplantación de la identidad	P		A		MA	
[A.6] Abuso de privilegios de acceso	P	M	M		MA	
[A.7] Uso no previsto	P	M	B			
[A.11] Acceso no autorizado	P	M	M		MA	
[A.13] Repudio (negación de actuaciones)	MA					MA
[A.15] Modificación de la información	MA		A			
[A.18] Destrucción de la información	P	A				
[A.23] Manipulación de hardware	P	MA				
[A.24] Denegación de servicio	P	MA				
[A.25] Robo de equipos	P	M				
[A.26] Ataque destructivo	P	MA				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 78: Amenazas en Punto de Acceso Inalámbrico

[WAP] PUNTO DE ACCESO INALÁMBRICO	**P**	**D**	**I**	**C**	**A**	**T**
Valoración Total		MA	A		MA	MA
[N.1] Fuego	PP	MA				
[N.2] Daños por agua	PP	A				
[N.*] Desastres naturales	PP	MA				
[I.1] Fuego	P	MA				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	MA				
[I.3] Contaminación medioambiental	PP	A				
[I.4] Contaminación electromagnética	P	M				
[I.5] Avería de origen físico o lógico	P	A				
[I.6] Corte de suministro eléctrico	P	MA				
[I.7] Condiciones inadecuadas de temperatura o humedad	P	MA				
[E.1] Errores de los usuarios	P	M	M			
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M			
[E.15] Alteración de la información	P		B			

[E.18] Destrucción de la información	P	M				
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M				
[E.24] Caída del sistema por agotamiento de recursos	MA	A				
[E.25] Pérdida de equipos	P	M				
[A.5] Suplantación de la identidad	P		A		MA	
[A.6] Abuso de privilegios de acceso	P	M	M		MA	
[A.7] Uso no previsto	P	M	B			
[A.11] Acceso no autorizado	P	M	M		MA	
[A.13] Repudio (negación de actuaciones)	MA					MA
[A.15] Modificación de la información	MA		A			
[A.18] Destrucción de la información	P	A				
[A.23] Manipulación de hardware	P	MA				
[A.24] Denegación de servicio	P	MA				
[A.25] Robo de equipos	P	M				
[A.26] Ataque destructivo	P	MA				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

[COM] COMUNICACIONES

Tabla 79: Amenazas en medio cableado Red LAN

[LAN_DTI] RED LAN	**P**	**D**	**I**	**C**	**A**	**T**
Valoración Total		A	M	A	MA	MA
[I.8] Fallo de servicios de comunicaciones	P	A				
[E.1] Errores de los usuarios	P	M	M	M		
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.9] Errores de [re-]encaminamiento	P			M		
[E.10] Errores de secuencia	P		M			
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	M				
[E.19] Fugas de información	P			M		
[E.24] Caída del sistema por agotamiento de recursos	P	A				

[A.5] Suplantación de la identidad	P		M	A	MA	
[A.6] Abuso de privilegios de acceso	P	B	M	A	MA	
[A.7] Uso no previsto	P	M	M	M		
[A.9] [Re-]encaminamiento de mensajes	P			M		
[A.10] Alteración de secuencia	P		M			
[A.11] Acceso no autorizado	P		M	A	MA	
[A.12] Análisis de tráfico	P			B		
[A.13] Repudio (negación de actuaciones)	MA					MA
[A.14] Interceptación de información (escucha)	P			M		
[A.15] Modificación de la información	P		M			
[A.18] Destrucción de la información	P	A				
[A.19] Revelación de información	P			A		
[A.24] Denegación de servicio	P	A				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 80: Amenazas en medio inalámbrico Red WLAN

[WLAN_DTI] RED LAN INALÁMBRICA	**P**	**D**	**I**	**C**	**A**	**T**
Valoración Total		A	M		MA	MA
[I.8] Fallo de servicios de comunicaciones	P	A				
[E.1] Errores de los usuarios	P	M	M			
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M			
[E.10] Errores de secuencia	P		M			
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	M				
[E.24] Caída del sistema por agotamiento de recursos	P	A				
[A.5] Suplantación de la identidad	P		M		MA	
[A.6] Abuso de privilegios de acceso	P	B	M		MA	
[A.7] Uso no previsto	P	M	M			
[A.10] Alteración de secuencia	P		M			
[A.11] Acceso no autorizado	P		M		MA	
[A.13] Repudio (negación de actuaciones)	MA					MA

[A.15] Modificación de la información	P		M			
[A.18] Destrucción de la información	P	A				
[A.24] Denegación de servicio	MA	A				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 81: Amenazas en servicio externo de Internet

[INTERNET_DTI] SERVICIO DE INTERNET	**P**	**D**	**I**	**C**	**A**	**T**
Valoración Total		A	M	A	MA	MA
[I.8] Fallo de servicios de comunicaciones	P	A				
[E.1] Errores de los usuarios	P	M	M	M		
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.9] Errores de [re-]encaminamiento	P			M		
[E.10] Errores de secuencia	P		M			
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	M				
[E.19] Fugas de información	P			M		
[E.24] Caída del sistema por agotamiento de recursos	P	A				
[A.5] Suplantación de la identidad	P		M	A	MA	
[A.6] Abuso de privilegios de acceso	P	B	M	A	MA	
[A.7] Uso no previsto	P	M	M	M		
[A.9] [Re-]encaminamiento de mensajes	P			M		
[A.10] Alteración de secuencia	P		M			
[A.11] Acceso no autorizado	P		M	A	MA	
[A.12] Análisis de tráfico	P			B		
[A.13] Repudio (negación de actuaciones)	MA					MA
[A.14] Interceptación de información (escucha)	P			M		
[A.15] Modificación de la información	P		M			
[A.18] Destrucción de la información	P	A				
[A.19] Revelación de información	P			A		
[A.24] Denegación de servicio	MA	A				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

[AUX] ELEMENTOS AUXILIARES

Tabla 82: Amenazas en sistema de alimentación ininterrumpida

[SAI_DTI] SISTEMA DE ALIMENTACIÓN ININTERRUMPIDA	P	D	I	C	A	T
Valoración Total		B	MB	MB		
[N.1] Fuego	PP	B				
[N.2] Daños por agua	PP	B				
[N.*] Desastres naturales	PP	B				
[I.1] Fuego	P	B				
[I.2] Daños por agua	P	B				
[I.*] Desastres industriales	P	B				
[I.3] Contaminación medioambiental	PP	B				
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	B				
[A.7] Uso no previsto	P	B	MB	MB		
[A.23] Manipulación de hardware	P	B		MB		
[A.25] Robo de equipos	P	B				
[A.26] Ataque destructivo	P	B				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 83: Amenazas en funcionamiento de aire acondicionado

[AC_DTI] AIRE ACONDICIONADO	P	D	I	C	A	T
Valoración Total		M	MB	MB		
[N.1] Fuego	PP	M				
[N.2] Daños por agua	PP	M				
[N.*] Desastres naturales	PP	M				
[I.1] Fuego	P	M				
[I.2] Daños por agua	P	M				
[I.*] Desastres industriales	P	M				
[I.3] Contaminación medioambiental	PP	M				
[I.6] Corte de suministro eléctrico	P	M				
[I.9] Interrupción de otros servicios o suministros esenciales	P	M				

[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M				
[A.7] Uso no previsto	P	M	MB	MB		
[A.23] Manipulación de hardware	P	M		MB		
[A.25] Robo de equipos	P	M				
[A.26] Ataque destructivo	P	M				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 84: Amenazas en cableado de datos

[CABLE_DTI] CABLEADO DE DATOS	**P**	**D**	**I**	**C**	**A**	**T**
Valoración Total		MA	A	A	MA	MA
[N.1] Fuego	PP	MA				
[N.2] Daños por agua	PP	A				
[N.*] Desastres naturales	PP	MA				
[I.1] Fuego	P	MA				
[I.2] Daños por agua	P	A				
[I.*] Desastres industriales	P	MA				
[I.3] Contaminación medioambiental	PP	A				
[I.4] Contaminación electromagnética	P	M				
[I.11] Emanaciones electromagnéticas	P			B		
[E.1] Errores de los usuarios	P	M	M	M		
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	M				
[E.19] Fugas de información	P			M		
[E.23] Errores de mantenimiento / actualización de equipos (hardware)	P	M				
[E.24] Caída del sistema por agotamiento de recursos	MA	A				
[A.5] Suplantación de la identidad	P		A	A	MA	
[A.6] Abuso de privilegios de acceso	P	B	M	M	MA	
[A.7] Uso no previsto	P	A	B	B		
[A.11] Acceso no autorizado	P		M	A	MA	
[A.13] Repudio (negación de actuaciones)	MA					MA
[A.15] Modificación de la información	MA		A			
[A.18] Destrucción de la información	P	A				

[A.19] Revelación de información	P			A		
[A.23] Manipulación de hardware	P	A		A		
[A.24] Denegación de servicio	MA	A				
[A.25] Robo de equipos	P	MA		0		
[A.26] Ataque destructivo	P	MA				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

[SS] SERVICIOS SUBCONTRATADOS

Tabla 85: Amenazas proveedor de sistema informático de biblioteca

[BIBLIOSUB_DTI] PROVEEDOR SISTEMA BIBLIOTECA	**P**	**D**	**I**	**C**	**A**	**T**
Valoración Total		MA	MA	MA	MA	
[I.5] Avería de origen físico o lógico	P	A				
[E.1] Errores de los usuarios	P	B	M	M		
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.8] Difusión de software dañino	P	M	M	M		
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	A				
[E.19] Fugas de información	P			M		
[E.20] Vulnerabilidades de los programas (software)	P	B	M	M		
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	B	B			
[A.5] Suplantación de la identidad	P		A	A	MA	
[A.6] Abuso de privilegios de acceso	P	B	M	M		
[A.7] Uso no previsto	P	B	M	M		
[A.8] Difusión de software dañino	P	MA	MA	MA		
[A.11] Acceso no autorizado	P		M	A		
[A.15] Modificación de la información	P		A			
[A.18] Destrucción de la información	P	A				
[A.19] Revelación de información	P			A		
[A.22] Manipulación de programas	P	A	MA	MA		

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 86: Amenazas proveedor de sistema para control de ingreso de personal

[BIOMSUB_DTI] PROVEEDOR SISTEMA PARA CONTROL DE INGRESO DE PERSONAL	P	D	I	C	A	T
Valoración Total		MA	MA	MA	MA	
[I.5] Avería de origen físico o lógico	P	A				
[E.1] Errores de los usuarios	P	B	M	M		
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.8] Difusión de software dañino	P	M	M	M		
[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	A				
[E.19] Fugas de información	P			M		
[E.20] Vulnerabilidades de los programas (software)	P	B	M	M		
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	B	B			
[A.5] Suplantación de la identidad	P		A	A	MA	
[A.6] Abuso de privilegios de acceso	P	B	M	M		
[A.7] Uso no previsto	P	B	M	M		
[A.8] Difusión de software dañino	P	MA	MA	MA		
[A.11] Acceso no autorizado	P		M	A		
[A.15] Modificación de la información	P		A			
[A.18] Destrucción de la información	P	A				
[A.19] Revelación de información	P			A		
[A.22] Manipulación de programas	P	A	MA	MA		

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 87: Amenazas proveedor servicios de Internet

[INTERSUB_DTI] SERVICIO DE INTERNET	P	D	I	C	A	T
Valoración Total		A	MA	A	MA	MA
[I.8] Fallo de servicios de comunicaciones	P	A				
[E.1] Errores de los usuarios	P	M	M	M		
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.9] Errores de [re-]encaminamiento	P			M		
[E.10] Errores de secuencia	P		M			

[E.15] Alteración de la información	P		B			
[E.18] Destrucción de la información	P	M				
[E.19] Fugas de información	P			M		
[E.24] Caída del sistema por agotamiento de recursos	P	A				
[A.5] Suplantación de la identidad	P		M	A	MA	
[A.6] Abuso de privilegios de acceso	P	B	M	A	MA	
[A.7] Uso no previsto	P	M	M	M		
[A.9] [Re-]encaminamiento de mensajes	P			M		
[A.10] Alteración de secuencia	P		M			
[A.11] Acceso no autorizado	P		M	A	T	
[A.12] Análisis de tráfico	P			B		
[A.13] Repudio (negación de actuaciones)	MA					T
[A.14] Interceptación de información (escucha)	P			M		
[A.15] Modificación de la información	P		M			
[A.18] Destrucción de la información	P	A				
[A.19] Revelación de información	P			A		
[A.24] Denegación de servicio	MA	A				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

[L] INSTALACIONES

Tabla 88: Amenazas en cuarto de control

[CCTRL_DTI] CUARTO DE CONTROL	**P**	**D**	**I**	**C**	**A**	**T**
Valoración Total		MA	M	A		
[N.1] Fuego	P	MA				
[N.2] Daños por agua	P	MA				
[N.*] Desastres naturales	P	MA				
[I.1] Fuego	P	MA				
[I.2] Daños por agua	P	MA				
[I.*] Desastres industriales	P	MA				
[I.3] Contaminación medioambiental	P	MA				
[I.4] Contaminación electromagnética	PP	M				
[I.11] Emanaciones electromagnéticas	PP	M		B		

[A.5] Suplantación de la identidad	P		M	A		
[A.6] Abuso de privilegios de acceso	P	M	M	A		
[A.7] Uso no previsto	P	M	M	A		
[A.11] Acceso no autorizado	MA		M	A		
[A.26] Ataque destructivo	PP	MA				
[A.27] Ocupación enemiga	P	MA		A		

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

[P] PERSONAL

Tabla 89: Amenazas personal administrador de sistemas informáticos – programadores

[PROG_DTI] ADMINISTRADORES DE SISTEMAS INFORMÁTICOS - PROGRAMADORES	**P**	**D**	**I**	**C**	**A**	**T**
Valoración Total		MA	MA	MA	MA	MA
[I.5] Avería de origen físico o lógico	P	A				
[E.1] Errores de los usuarios	P	B	M	M		
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.8] Difusión de software dañino	P	M	M	M		
[E.15] Alteración de la información	P		M			
[E.18] Destrucción de la información	P	B				
[E.19] Fugas de información	P			M		
[E.20] Vulnerabilidades de los programas (software)	P	B	M	M		
[E.21] Errores de mantenimiento / actualización de programas (software)	MA	B	B			
[E.24] Caída del sistema por agotamiento de recursos	MA	A				
[E.28] Indisponibilidad del personal	P	M				
[A.5] Suplantación de la identidad	P		A	A	MA	
[A.6] Abuso de privilegios de acceso	P	B	M	M	MA	
[A.7] Uso no previsto	P	B	M	M		
[A.8] Difusión software dañino	P	MA	MA	MA		
[A.11] Acceso no autorizado	P		M	A	MA	
[A.13] Repudio (negación de actuaciones)	MA					MA
[A.15] Modificación de la información	P		A			

[A.18] Destrucción de la información	P	M				
[A.19] Revelación de información	MA			A		
[A.22] Manipulación de programas	P	A	MA	MA		
[A.24] Denegación de servicio	MA	A				
[A.28] Indisponibilidad del personal	P	M				
[A.29] Extorsión	P	B	MA	MA		
[A.30] Ingeniería social (picaresca)	P	B	MA	MA		

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 90: Amenazas personal administrador de infraestructura y telecomunicaciones

[REDES_DTI] ADMINISTRADORES DE INFRAESTRUCTURA Y TELECOMUNICACIONES	**P**	**D**	**I**	**C**	**A**	**T**
Valoración Total		A	A	A	MA	
[I.8] Fallo de servicios de comunicaciones	P	A				
[E.2] Errores del administrador del sistema / de la seguridad	P	M	M	M		
[E.9] Errores de [re-]encaminamiento	P			M		
[E.10] Errores de secuencia	P		M			
[E.15] Alteración de la información	P		M			
[E.18] Destrucción de la información	P	B				
[E.19] Fugas de información	P			M		
[E.24] Caída del sistema por agotamiento de recursos	P	A				
[E.28] Indisponibilidad del personal	P	M				
[A.5] Suplantación de la identidad	P		M	A	MA	
[A.6] Abuso de privilegios de acceso	P		M	A	MA	
[A.7] Uso no previsto	P	M	M	M		
[A.9] [Re-]encaminamiento de mensajes	P			M		
[A.10] Alteración de secuencia	P		M			
[A.11] Acceso no autorizado	P		M	A	MA	
[A.12] Análisis de tráfico	P			B		
[A.14] Interceptación de información (escucha)	P			M		
[A.15] Modificación de la información	P		A			
[A.18] Destrucción de la información	P	M				
[A.19] Revelación de información	P			A		

[A.24] Denegación de servicio	MA	A				
[A.28] Indisponibilidad del personal	P	M				
[A.29] Extorsión	P	A	A	A		
[A.30] Ingeniería social (picaresca)	P	A	A	A		

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Tabla 91:Amenazas personal de soporte técnico

[SOPTE_DTI] SOPORTE TÉCNICO	**P**	**D**	**I**	**C**	**A**	**T**
Valoración Total		A				MA
[E.1] Errores de los usuarios	P	M				
[E.2] Errores del administrador del sistema / de la seguridad	P	M				
[E.18] Destrucción de la información	P	B				
[E.24] Caída del sistema por agotamiento de recursos	MA	A				
[E.28] Indisponibilidad del personal	P	A				
[A.6] Abuso de privilegios de acceso	P	B				
[A.7] Uso no previsto	P	B				
[A.13] Repudio (negación de actuaciones)	MA					MA
[A.18] Destrucción de la información	P	M				
[A.24] Denegación de servicio	MA	A				
[A.28] Indisponibilidad del personal	P	A				
[A.29] Extorsión	P	M				
[A.30] Ingeniería social (picaresca)	P	M				

Fuente: PILAR - Valoración de activos Dirección de Tecnologías de la Información – PUCESD
Elaborado: Ing. Franklin Carrasco

Analizando las valoraciones realizadas en cada activo sobre la probabilidad de ocurrencia y el nivel de degradación por cada amenaza, se determina:

- Los servicios internos pueden verse altamente afectados por el agotamiento de la capacidad de recursos en los equipos que los soportan, como también por errores de configuración, actualización o mantenimiento realizados por el personal técnico; sin dejar atrás las posibles fallas de comunicación que se presenten en la red de datos.

- Las aplicaciones, entre ellos Sistemas y Servicios Informáticos dependen en gran parte de los equipos servidores donde han sido instalados, puesto que una posible avería de origen físico o lógico podría afectar en niveles extremos a la institución; también el acceso no autorizado de los usuarios puede influir en la pérdida o manipulación de la información, sin dejar de mencionar los posibles errores que el personal técnico pueda tener durante el mantenimiento de los sistemas.

- Los equipos como Servidores, Switches, Routers, entre otros, se ven afectados por una amenaza continua como es el corte del suministro eléctrico, cuyo impacto puede desencadenar en averías de tipo físico o lógico, que llevan a la caída de los servicios o sistemas

informáticos; de igual manera se toma como referencia el acceso no autorizado de personas a los cuartos de comunicación, y los errores por mantenimiento, configuración o actualización de estos equipos.

- Los medios físicos e inalámbricos en las redes de comunicación LAN y WLAN están expuestos a daños lógicos como: intercepción de información, re-encaminamiento de datos, y suplantación de identidad; así también se presentan fallas físicas como: destrucción, interferencias electromagnéticas o efectos externos que perjudican al correcto paso de los datos y la disponibilidad de los servicios de la universidad.

- El funcionamiento de los elementos auxiliares, como el aire acondicionado, y el sistema de alimentación ininterrumpida pueden estar altamente afectados por la contaminación medio ambiental y por los errores de mantenimiento o mala manipulación del hardware; estos equipos son complementarios y necesarios para el funcionamiento de servidores, switches, y routers, pues componen un ambiente de resguardo.

- Los servicios subcontratados de la universidad pueden verse afectados por vulnerabilidades en los servicios o productos (software) que se contraten, así también en la continuidad de las empresas proveedoras.

- Los cuartos de control que albergan los equipos informáticos como: servidores, routers, switches, sistemas de alimentación ininterrumpida, sistemas contra incendios, entre otros, pueden afectarse por al acceso no autorizado de personas, quienes de forma maliciosa podrían realizar ataques destructivos o hacer uso de indebida de los servicios de la universidad.

- El personal técnico encargado de la administración de los sistemas de información, se considera como uno de los principales activos que posee la universidad, puesto que con sus actos podrían afectar los sistemas informáticos y servicios de una institución, como es el caso del abuso de privilegios de acceso, modificación o revelación de la información, extorsión, e indisponibilidad del personal. Los daños que llegaran a ocasionar, llevaría a la institución a emprender procedimientos legales contra el personal.

5.2. Evaluación del impacto en la interrupción de la universidad

Con la valoración de las amenazas se determina que la Disponibilidad (D) es el criterio principal para determinar el Impacto de daños, el nivel de Riesgo ante la materialización de una amenaza, y el impacto económico o inversión que la universidad debe realizar por la pérdida de los servicios o activos. Para valorar el Impacto y el Riesgo se definen niveles de criticidad, presentados en las tablas 92 y 93:

Tabla 92: Niveles de Impacto

10	Extremo
9	Muy Alto
8	Alto (+)
7	Alto
6	Alto (-)
5	Medio (+)
4	Medio
3	Medio (-)
2	Bajo(+)
1	Bajo
0	Despreciable

Fuente: PILAR

Tabla 93: Niveles de criticidad

{9}	Catástrofe
{8}	desastre
{7}	extremadamente crítico
{6}	muy crítico
{5}	crítico
{4}	muy alto
{3}	alto
{2}	medio
{1}	bajo
{0}	despreciable

Fuente: PILAR

Considerando la inversión económica que debe realizar la universidad para mantener la disponibilidad de sus activos informáticos, actividades o procesos en caso de la materialización de una amenaza, se ha desarrollado una escala de costos, cuya valoración permitirá tener una visión potencial de la importancia del activo y cuanto se puede afectar económicamente la institución. Esta escala se presenta en la siguiente tabla 94.

Tabla 94: Escala de costos

Muy Alto	Mayor a $50.000
Alto	Entre 20.000 hasta $50.000
Medio	Entre $10.000 hasta $19.999
Bajo	Entre $3.000 hasta $9.999
Despreciable	Entre $0 hasta $2.999

Fuente: Dirección de Tecnologías de la Información – PUCE SD

En las siguientes tablas se presentan los resultados de las valoraciones potenciales de impacto, riesgo y costo:

Tabla 95: Impacto, riesgo y costo potencial en Servicios Internos

[IS] Servicios Internos		**D**	**I**	**C**	**A**	**T**	**Costo**
[INTER_DTI] Internet	Impacto	8	5	8	7	9	Alto
	Riesgo	{6,6}	{3,8}	{5,7}	{5,1}	{6,9}	
[WEBS_DTI] Portal Web PUCESD	Impacto	7	7	5			Medio
	Riesgo	{5,1}	{5,1}	{3,9}			
[EMAIL_DTI] Servicio Correo Electrónico Gmail	Impacto	8	6	8	7	9	Alto
	Riesgo	{6,6}	{5,4}	{5,7}	{5,1}	{6,9}	
[FILE_DTI] Almacenamiento de Archivos	Impacto	6	6	8	6	6	Medio
	Riesgo	{5,4}	{5,4}	{5,7}	{4,5}	{5,1}	

Fuente: PILAR - Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

Tabla 96: Impacto, riesgo y costo potencial en Aplicaciones

[SW] Aplicaciones		D	I	C	A	T	Costo
[PROD_DTI] Sistemas Informáticos de Producción	Impacto	9	9	9	9	9	Muy Alto
	Riesgo	{6,6}	{7,5}	{6,6}	{6,9}	{6,9}	
[PWEB_DTI] Servicios Portal Web	Impacto	7	6	4	3	3	Medio
	Riesgo	{5,4}	{5,7}	{3,3}	{3,3}	{3,3}	
[BIBL_DTI] Sistema de Biblioteca	Impacto	9	6	0	1	3	Medio
	Riesgo	{6,6}	{4,5}	{0,98}	{1,5}	{3,3}	
[PROF_DTI] Sistema administrador de personal docente	Impacto	4	6	7	6		Medio
	Riesgo	{3,3}	{4,5}	{5,1}	{4,5}		
[BIOM_DTI] Sistema para control de ingreso de personal	Impacto	7	6	3	5	5	Medio
	Riesgo	{5,4}	{4,5}	{2,7}	{3,9}	{4,5}	
[FILEBA_DTI] Software para respaldo de archivos	Impacto	4		3	9	7	Despreciable
	Riesgo	{3,7}		{2,7}	{6,2}	{5,7}	
[PFFI_DTI] Office - Ofimática	Impacto	1					Despreciable
	Riesgo	{1,5}					
[AV_DTI] Antivirus	Impacto	3					Despreciable
	Riesgo	{2,7}					
[OS_DTI] Sistema Operativo	Impacto	9	9	9	9		Despreciable
	Riesgo	{6,2}	{6,2}	{6,2}	{6,2}		

Fuente: PILAR - Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

Tabla 97: Impacto, riesgo y costo potencial en Equipos (Hardware)

[HW] Equipos		D	I	C	A	T	Costo
[PRODS_DTI] Servidor de Producción	Impacto	9	9	9	9		Muy Alto
	Riesgo	{6,6}	{7,1}	{7,1}	{7,1}		
[DSKB_DTI] Disco para respaldos de Sistemas Informáticos de Producción	Impacto	7	7	8	9		Alto
	Riesgo	{5,4}	{5,9}	{6,5}	{7,1}		
[PWEBS_DTI] Servidor Portal Web	Impacto	7	7	4	5	7	Medio
	Riesgo	{5,4}	{5,4}	{3,3}	{3,9}	{5,7}	

[BIBLS_DTI] Servidor Sistema de Biblioteca	Impacto	9	7	0	5		Medio
	Riesgo	{6,6}	{5,1}	{0,98}	{3,9}		
[PROFS_DTI] Servidor Sistema administrador de personal docente	Impacto	4	6	7	6	7	Medio
	Riesgo	{3,7}	{4,5}	{5,1}	{4,5}	{5,7}	
[BIOMS_DTI] Servidor Sistema para control de ingreso de personal	Impacto	7	6	6	6	7	Alto
	Riesgo	{5,4}	{4,5}	{4,5}	{4,5}	{5,7}	
[FILEBAS_DTI] Servidor Respaldo de Archivos	Impacto	7	5	9			Alto
	Riesgo	{5,4}	{3,8}	{5,7}			
[PROXS_DTI] Servidor Proxy Firewall	Impacto	9	9	9	9	9	Alto
	Riesgo	{6,6}	{6,2}	{6,2}	{6,2}	{6,9}	
[DHCPS_DTI] Servidor DHCP	Impacto	9	8	9	9	9	Alto
	Riesgo	{6,6}	{6,6}	{6,2}	{6,2}	{6,9}	
[SWITCH_DTI] Switch	Impacto	9	7	8	9	9	Alto
	Riesgo	{6,6}	{5,0}	{5,7}	{6,2}	{6,9}	
[Router] Router	Impacto	9	8	8	9	9	Alto
	Riesgo	{6,6}	{6,6}	{5,7}	{6,2}	{6,9}	
[WLC_DTI] Controladora de red inalámbrica	Impacto	6	5		7	7	Alto
	Riesgo	{4,8}	{4,8}		{5,1}	{5,7}	
[WAP] Punto de Acceso Inalámbrico	Impacto	6	6		7	7	Bajo
	Riesgo	{4,8}	{5,4}		{5,1}	{5,7}	

Fuente: PILAR - Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

Tabla 98: Impacto, riesgo y costo potencial en Comunicaciones

[COM] Comunicaciones		**D**	**I**	**C**	**A**	**T**	**Costo**
[LAN_DTI] Red LAN	Impacto	8	7	8	9	9	Alto
	Riesgo	{6,6}	{5,0}	{5,7}	{6,2}	{6,9}	
[WLAN_DTI] Red LAN Inalámbrica	Impacto	5	4		7	7	Medio
	Riesgo	{4,8}	{3,2}		{5,1}	{5,7}	
[INTERNET_DTI] Servicio de Internet	Impacto	8	7	8	7	9	Alto
	Riesgo	{6,6}	{5,0}	{5,7}	{5,1}	{6,9}	

Fuente: PILAR - Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

Tabla 99: Impacto, riesgo y costo potencial en Elementos Auxiliares

[AUX] Elementos Auxiliares		D	I	C	A	T	Costo
[SAI_DTI] Sistema de alimentación ininterrumpida	Impacto	3					Alto
	Riesgo	{2,7}					
[AC_DTI] Aire Acondicionado	Impacto	6					Medio
	Riesgo	{4,5}					
[CABLE_DTI] Cableado de Datos	Impacto	9	8	8	9	9	Alto
	Riesgo	{6,6}	{6,6}	{5,7}	{6,2}	{6,9}	

Fuente: PILAR - Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

Tabla 100: Impacto, riesgo y costo potencial en Servicios subcontratados

[SS] Servicios subcontratados		D	I	C	A	T	Costo
[BIBLIOSUB_DTI] Proveedor Sistema Biblioteca	Impacto	9	7	0	5		Medio
	Riesgo	{6,2}	{5,1}	{0,98}	{3,9}		
[BIOMSUB_DTI] Proveedor Sistema para control de ingreso de personal	Impacto	7	6	6	6		Medio
	Riesgo	{5,1}	{4,5}	{4,5}	{4,5}		
[INTERSUB_DTI] Servicio de Internet	Impacto	8	7	8	7	9	Alto
	Riesgo	{6,6}	{5,0}	{5,7}	{5,1}	{6,9}	

Fuente: PILAR - Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

Tabla 101: Impacto, riesgo y costo potencial en Instalaciones

[L] Instalaciones		D	I	C	A	T	Costo
[CCTRL_DTI] Cuarto de Control	Impacto	9	6	8			Alto
	Riesgo	{6,2}	{5,1}	{6,3}			

Fuente: PILAR - Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

Tabla 102: Impacto, riesgo y costo potencial en Personal

[P] Personal		D	I	C	A	T	Costo
[ADMP_DTI] Administradores de Sistemas Informáticos - Programadores	Impacto	9	9	9	9	9	Medio
	Riesgo	{6,6}	{6,2}	{6,6}	{6,2}	{6,9}	
[REDES_DTI] Administradores de infraestructura y telecomunicaciones	Impacto	8	8	8	9		Medio
	Riesgo	{6,6}	{5,7}	{5,7}	{6,2}		
[SOPTE_DTI] Soporte Técnico	Impacto	4				7	Medio
	Riesgo	{4,2}				{5,7}	

Fuente: PILAR - Dirección de Tecnologías de la Información – PUCE SD

Elaborado: Ing. Franklin Carrasco

5.2.1. Salvaguardas

Para contrarrestar el riesgo, es decir la probabilidad de la materialización de una amenaza, se deben identificar y valorar las posibles salvaguardas. Las salvaguardas son protecciones para prevenir, corregir, recuperar, disuadir, monitorizar los activos y que se aplican en la gestión del personal, la seguridad física, y actividades técnicas.

Las salvaguardas seleccionadas se presentan agrupadas bajo la clasificación de la metodología Magerit, y las indicaciones expuestas por

el personal técnico y la Dirección de Tecnologías de la Información de la Universidad:

5.2.1.1. Protecciones Generales

Identificación y autenticación

- Disponer de normativa y procedimientos para las tareas de identificación y autenticación.
- Identificación exclusiva de cada usuario.
- Gestión de la identificación y autenticación de usuario, comprobar la identidad de los usuarios y los privilegios requeridos antes de entregar la credencial.

Control de acceso lógico

- Procedimiento de concesión, cancelación, reactivación y suspensión temporal de privilegios.
- Definir y documentar las autorizaciones de acceso.

- Identificar los perfiles de acceso y sus privilegios asociados.
- Mantener un registro de los privilegios de acceso.
- Controlar los privilegios de los usuarios (lectura, escritura, modificación, borrado, ejecución).
- Autorización previa para el acceso a las utilidades del sistema. Los derechos de acceso son aprobados por el propietario del servicio o de la información.
- Se restringe el uso de las aplicaciones a ciertas estaciones.
- Se restringe el acceso a un número limitado de usuarios.
- Concienciación de los usuarios.

Herramientas de seguridad

- Implantación de IDS/IPS: Herramienta de detección / prevención de intrusión.
- Implantación de herramienta de monitorización de tráfico.
- Comprobación de virus desde diferentes puntos de la red.

Gestión de vulnerabilidades

- Analizar el impacto potencial (estimación de riesgos) en daños sobre la misión o negocio del sistema, daños sobre los activos del sistema, y perjuicios a terceros.
- Gestión de las actividades de registro y auditoría, además de disponer de un inventario de las fuentes de información.

5.2.1.2. Protección de la Información

- Disponer de un registro de activos de información tales como bases de datos, copias de seguridad, manuales, libros, software, hardware, contratos, equipo de comunicaciones, servicios informáticos y de comunicaciones, entre otros.
- Realizar copias de seguridad (backups)
- Gestión de las copias de seguridad de los datos (backup)
- Acceder a las copias de seguridad con previa autorización
- Uso de firmas electrónicas

5.2.1.3. Gestión de claves criptográficas

- Generación de claves en aplicación informática

5.2.1.4. Protección de los Servicios

Protección y uso del correo electrónico (e-mail)

- Normativa de uso de correo electrónico.
- Formar a los usuarios en el uso del servicio.
- Disponer de un procedimiento de actuación y medidas disciplinarias en caso de incumplimiento.
- Proteger la información en el cuerpo y adjunta al mensaje.
- Medidas frente a la recepción de spam.
- Medidas frente a código dañino en los clientes de correo, como anti-virus, anti-spyware, o deshabilitar la apertura automática de datos adjuntos.
- Asignar responsable para la administración del software.
- Registrar el uso del servicio.

Navegación web

- Disponer de normativa de uso
- Describir los usos autorizados
- Disponer de normativa sobre el uso de los servicios Internet
- El usuario se compromete por escrito a cumplir la normativa
- Verificar el cumplimiento de la política
- Herramienta de monitorización del tráfico
- Herramienta de control de contenidos con filtros actualizados
- Registrar navegación web
- Controlar la configuración de los navegadores
- Actualización regular de los navegadores

Protección de servicios y aplicaciones web

- Designar responsable del servicio web
- Publicación de datos previa autorización
- Se debe proteger la información sensible durante su recogida y tratamiento
- Protección del servidor de nombres de dominio (DNS)
- Designar responsable(s) para la administración del servicio DNS
- Registran las modificaciones de los datos en el servicio DNS

- Actualización regular del software (DNS)
- Mantener el servidor interno aislado del exterior

Servicios subcontratados

- Disponer de un registro de servicios subcontratados.
- Requerir aprobación previa para el uso de servicios externos.
- Requerir se incluyan los requisitos de seguridad en servicios externos.
- Definir las responsabilidades sobre instalación y mantenimiento de HW y SW.
- Definen las responsabilidades en la supervisión del cumplimiento del contrato.

5.2.1.5. Protección de las Aplicaciones Informáticas (SW)

Inventarios

- Inventario de aplicaciones

- Inventario de software base
- Inventario de sistemas operativos
- Registro de actualización de los inventarios

Copias de seguridad (backup)

- Procedimiento para realizar copias de seguridad
- Realizar copias de las aplicaciones críticas para el negocio
- Verificar que las copias pueden ser restauradas correctamente
- Almacenar las copias de seguridad en lugares alternativos

Puesta en producción

- Normativa de paso a operación / producción
- Procedimientos de paso a operación / producción
- Registro de paso a operación / producción bajo previa autorización

Perfiles de seguridad

- Sólo los administradores autorizados pueden modificar la configuración

Explotación / Producción

- Formación del personal en configuración de aplicaciones

Cambios (actualizaciones y mantenimiento)

- Disponer de políticas para designar responsables para: autorizar cambios, realizar cambios, abortar y, en su caso recuperar, la situación inicial antes de un cambio.
- Disponer de procedimiento formal para: autorización de cambios, comunicación de detalles del cambio a todo el personal afectado.
- Priorizar las actuaciones encaminadas a corregir riesgos elevados.
- Verificar que el cambio no inhabilita los mecanismos de detección, monitorización y registro.

- Retener copias de las versiones anteriores de software como medida de precaución para contingencias.
- Probar previamente en un equipo que no esté en producción.
- Realizar pruebas de regresión.
- Registrar toda actualización de SW.
- Documentar todos los cambios.
- Actualizar todos los procedimientos de recuperación afectados.

5.2.1.6. Protección de los Equipos Informáticos (HW)

Inventarios de equipos

- Registro de equipos propios.
- Registro de equipos ajenos.
- Identificar el propietario (persona responsable).
- Inventario regularmente actualizado.
- Registro de traslados internos.

Puesta en producción

- Registro de puesta en producción con autorización.

Aseguramiento de la disponibilidad

- Mantenimiento realizado por personal debidamente autorizado.
- Realizar copias de seguridad de la configuración.
- Monitoreo de fallos e incidentes.
- Registro de fallos, reales o sospechados y de mantenimiento preventivo y correctivo.

Instalación

- Instalar atendiendo a las especificaciones del fabricante.
- Evitar el acceso visual a pantallas y monitores por personas no autorizadas.

Operación

- Los nuevos medios deben tener la aprobación adecuada, autorizando su propósito y uso.
- Comprobar compatibilidad con los demás dispositivos del sistema.
- Formar al personal en configuración de equipos.
- Protección de los equipos para evitar: accesos innecesarios, accesos no autorizados, y daños.
- Registro de activos fuera de las instalaciones en cada momento (salida, retorno).
- Revisión del activo a su retorno.
- Requerir autorización previa para utilización de dispositivos de red.
- Actualización regular por el fabricante / proveedor de dispositivos de red.
- Identificación y autenticación de los dispositivos de red antes de conectarse al sistema.
- Controlar el acceso a las consolas de administración de los dispositivos de red.
- Prohibir la compartición de cuentas de administración de los dispositivos de red.

Cambios (actualizaciones y mantenimiento)

- Procedimiento formal para autorización y comunicación de cambios.
- Seguimiento permanente de actualizaciones.
- Priorizar las actuaciones encaminadas a corregir riesgos elevados.
- Verificar que el cambio no inhabilita los mecanismos de detección, monitorización y registro.
- Planificar el cambio de forma que minimice la interrupción del servicio.
- Realización de cambios por personal debidamente autorizado.
- Probar previamente en un entorno que no esté en producción.

5.2.1.7. Protección de las Comunicaciones

- Sólo los administradores autorizados pueden modificar la configuración.
- Disponer de conexión redundante (mediante doble tarjeta de red) de los dispositivos críticos.

Control de acceso a la red

- Se requiere autorización para que medios y dispositivos tengan acceso a redes y servicios.
- Control de conexiones remotas a las redes (filtrado de tráfico, origen / destino).
- Autenticación e identificación de nodos de la red (dirección, nombre, etc.)
- Protección frente a análisis del tráfico.
- Formación del personal en configuración de las comunicaciones.

Seguridad Wireless (WiFi)

- Requerir autorización para desplegar puntos de acceso (AP).
- Al instalar un punto de acceso (AP) tener en cuenta el alcance de la señal para evitar una exposición gratuita a ataques.
- Requerir autorización previa para la conexión de clientes.
- Desactivar el modo de conexión ad-hoc en los dispositivos de usuario.

5.2.1.8. Punto de interconexión: conexiones entre zonas de confianza

- Procedimiento formal para autorización y comunicación de cambios.
- Ocultar las direcciones IP internas (servicio NAT o similar).
- Ocultar los puertos internos (servicio PAT o similar).
- Todo el tráfico debe atravesar el cortafuego.
- Todo el tráfico debe atravesar el proxy.
- El servidor de proxy debe tener dos puertos, uno en cada red.

5.2.1.9. Protección de los Soportes de Información

- Disponer de un inventario de los soportes de información.
- Identificar al propietario (persona responsable) de los soportes de información.
- Disponer de armarios de seguridad.
- Tomar medidas contra el deterioro físico del soporte.

5.2.1.10. Elementos Auxiliares

- Disponer de un inventario de equipamiento auxiliar.
- Identifica el propietario (persona responsable).
- Registran las entradas y salidas de equipamiento auxiliar

Suministro eléctrico

- Dimensionar el sistema eléctrico considerando necesidades futuras.
- Proteger las líneas de alimentación del sistema frente a fluctuaciones y sobrecargas.
- Determinar interruptor general de la alimentación del sistema situado en la entrada de cada área.
- Etiquetar y proteger interruptores frente a activaciones accidentales.
- Activación de alimentación de respaldo eléctrico en caso de emergencia.
- Probar regularmente la alimentación de respaldo eléctrico.
- Mantenimiento: el sistema de alimentación de respaldo eléctrico se revisa regularmente.

- Sistema de alimentación ininterrumpida (SAI) que permite el funcionamiento de los equipos críticos, hasta su correcto cierre y apagado.
- Sistema de alimentación redundante que garantiza el funcionamiento de los equipos críticos, y la continuidad de las operaciones.

Climatización

- Controlar temperatura
- Controlar humedad
- Controlar flujo de aire
- Indicación de alarma en tiempo real cuando el sistema se sale de especificaciones
- Mantenimiento regular del sistema de climatización.

Protección del cableado

- Cableado centralizado
- Disponer de planos actualizados del cableado

- Todos los elementos de cableado debe estar etiquetados
- Controlar todos los accesos al cableado.
- Protección cableado contra daños o interceptaciones no autorizadas (conductos blindados, cajas o salas cerradas,...).
- El cableado debe ser tolerante a fallos (redundancia de líneas críticas, etc.).

5.2.1.11. Protección de las Instalaciones

- Disponer de normativa de seguridad.
- Establecer normas de conducta (prohibición de fumar, beber, comer,...).
- Disponer de inventario de instalaciones.
- Actualizar regularmente el inventario de instalaciones.
- Reducir al mínimo necesario el número de entradas.
- Disponer de puertas de acceso acorazadas.
- Disponer de protección en los conductos y aberturas (techo falso, conductos de aire, etc.).
- Separación entre áreas de seguridad y de acceso público.

- Disponer de áreas específicas para equipos informáticos.
- Disponer de áreas con acceso a medios de transmisión.
- Disponer de áreas para elementos auxiliares.
- Separar las áreas dónde se llevan a cabo actividades peligrosas (cuartos de basura, depósitos de combustible, etc.).
- Las instalaciones deben ser discretas minimizando indicaciones sobre su propósito.
- El perímetro exterior previene el acceso no autorizado (defensa en profundidad).

Control de los accesos físicos

- El acceso tiene que ser a través de un área de recepción.
- Acceso previa autorización.
- Mantiene un registro de los accesos.
- Investigar cualquier sospecha o intento de acceso físico no autorizado.
- Disponer de mecanismos de autenticación (huella dactilar, texto manuscrito).

- Dispone de un sistema de cámaras de vigilancia.
- Se requiere autorización previa para el acceso de visitas, personal de mantenimiento, o personal de empresas contratistas.
- Comprobar la identidad de las visitas.
- Mantener un registro de entrada / salida (nombre, empresa, fecha y horas de entrada y salida, objeto del acceso, y persona que recibe).
- Se revisa regularmente el registro de visitas.
- Los accesos permanecen cerrados fuera de las horas de trabajo.
- Evitar el trabajo no supervisado.
- [Prohibir equipos de registro (fotografía, video, audio, telefonía, etc.) salvo autorización especial.
- El perímetro está claramente definido con una valla, muro o similar.
- Protección frente a desastres.
- Protección frente a incendios.
- Protección frente a contaminación medio ambiental (polvo, vibraciones).
- Protección frente a contaminación electromagnética.

5.2.1.12. Gestión del Personal

- Identificar responsables.
- Asignación de tareas.
- Se definen roles con autorización exclusiva para realizar tareas: Usuario del sistema, Administrador del sistema, Administrador de comunicaciones (redes), Administrador de Seguridad, Desarrollo y mantenimiento de sistemas, Administración de cambios, Auditoría de seguridad.
- Proporcionar formación en las funciones de cada rol del sistema.
- Registran todas las operaciones del personal.
- Impedir que alguien pueda autorizarse a sí mismo.
- Los usuarios ni desarrollan ni pueden modificar los desarrollos.
- Los usuarios ni configuran ni pueden modificar la configuración.
- Revisar funciones del personal en periodos de vacaciones.
- Rotar turnos de trabajo.
- Asegurar que en todo momento hay más de un operador.
- Supervisar las operaciones críticas.
- Monitorear continuamente los incidentes de disponibilidad de personal.

- Respaldo de personal con formación de urgencia.

5.2.1.13. Gestión de incidentes

- Ante incidentes, el personal designado debe cubrir las 24h los 7 días de la semana.
- Se debe suspender cautelarmente los trabajos en el sistema afectado.
- Se debe identificar y analizar la causa del incidente.
- Se debe analizar el impacto del incidente, como daños sobre la misión o negocio del sistema, daños sobre los activos del sistema, perjuicios a terceros, y daños colaterales.
- Comunicación con los afectados y los implicados en la recuperación del incidente.
- Se debe informar a las autoridades correspondientes.
- Se deben recoger pistas de auditoría, atendiendo a su validez, calidad y completitud.

- Medios Evidenciar por escrito el incidente (identificar autor del documento, testigos del incidente, medidas para prevenir la alteración del documento).
- Evidenciar en medios electrónicos el incidente (identificar el origen de la evidencia, copias de medios de alta fiabilidad, registro de todas las acciones del proceso de copia, testigos del proceso de copia).
- Ayudar a los usuarios afectados.

Comunicación de los fallos del software

- Establecer canales para la comunicación de los fallos de SW.
- Definir criterios para interpretar síntomas y mensajes que aparecen en pantalla.
- Definir instrucciones de cómo actuar frente a sistemas que fallan, como: ¿A quién se debe informar?, ¿Qué datos se deben registrar?, ¿Qué se debe hacer con el sistema que falla?

Disponer de un registro de incidentes

- Tipo de incidente.
- Momento en que se ha producido.
- Persona que realiza la notificación.
- A quién se le comunica.
- Efectos derivados de la misma.
- Acciones tomadas.

Registro de fallos y medidas correctoras

- Registrar toda comunicación sobre fallos en el sistema.
- Revisar los registros de fallos para asegurar que todos han sido resueltos satisfactoriamente.
- Revisar las medidas correctoras para comprobar que son efectivas.
- Retener los registros de fallos durante el periodo establecido.

Control formal del proceso de recuperación ante el incidente

- Identificar al personal que va a gestionar el incidente.
- Requerir autorización previa del personal que va a gestionar el incidente.
- Realizar un registro de todas las acciones realizadas.
- Cada acción de emergencia debe ser aprobada por la Dirección.
- Comprobar la integridad de los sistemas y de las medidas de control de seguridad.

Formación y concienciación

- Concienciación en la detección y reporte de incidentes.
- Formación del personal en detección y gestión de incidentes.

5.2.1.14. Continuidad del negocio

- Actualización regular del inventario de sistemas de información, cuando entran, se actualizan o se retiran aplicaciones (SW) y equipamiento (HW).

Realizar un análisis de impacto (BIA)

- Identificar y priorizar los procesos críticos
- Identificar los activos involucrados en los procesos críticos
- Establecer objetivos de recuperación para cada proceso crítico (RTO)
- Establecer objetivos de recuperación para cada información crítica (RPO)
- Identificar eventos posibles y su potencialidad de producir una interrupción
- Identificar los impactos en términos de tiempo de interrupción, daños y tiempo de recuperación

Actividades preparatorias

- Adoptar medidas preventivas

- Identificar las necesidades de copias de seguridad (backup) y su almacenamiento.
- Identificar las necesidades de equipamiento alternativo.
- Disponer de seguros contra interrupciones en el negocio.
- Identificar la necesidad de un centro alternativo

5.2.1.15. Organización

- Arquitectura Empresarial
- Comité de seguridad de la información
- Roles identificados (responsables de la información, responsables del sistema).

Documentación técnica (componentes)

- Documentación de las instalaciones (descripción de las áreas, puntos de acceso a las instalaciones).
- Documentación de las comunicaciones (descripción de redes internas, descripción de conexiones a redes externas, descripción de conexiones a Internet).

- Puntos de interconexión (entre zonas de confianza internas, a zonas de confianza externas controladas, conexiones a Internet).
- Empleo de cortafuegos.
- Empleo de productos de diferentes fabricantes.

Criterios de aceptación para versiones o sistemas nuevos

- Revisar la documentación del sistema (nueva o actualizada).
- Revisar procedimientos de operación del sistema.
- Comprobar la facilidad de uso.

Seguridad de la documentación del sistema

- El acceso se limita a quien necesita conocer.
- El propietario del sistema sólo concede acceso a un número restringidos de personas.
- Norma de copias de seguridad (backup).

Documentación organizativa (normas y procedimientos)

- Revisar periódicamente el cumplimiento de las normas por parte del personal.

Gestión de Riesgos

- Disponer de normativa en materia de gestión de riesgos, que indique criterios de valoración de activos, criterios de valoración de amenazas y vulnerabilidades, roles y responsabilidades, criterios de evaluación de riesgos.
- Designación de responsables.
- Disponer de procedimientos para llevar a cabo las tareas de análisis y gestión de riesgos.

Activos

- Identificar y valorar los activos más valiosos.
- Identificar y valorar todos los activos del sistema.

Amenazas

- Identificar y valorar las amenazas más probables.
- Identificar amenazas con un impacto notable.
- Identificar y valorar todas las amenazas posibles.
- Identificar las vulnerabilidades del sistema.

Salvaguardas

- Identificar y valorar las principales salvaguardas.

Evaluación de Riesgos

- Identificar y evaluar los principales riesgos residuales.
- Revisión periódica de activos, de las amenazas, de las vulnerabilidades, de los controles implantados.

Planificación de capacidades

- Disponer una Normativa de Planificación de la seguridad.

- Estimar las necesidades de: procesamiento, software, almacenamiento, transmisión, personal.
- Estudiar la dependencia de otros servicios.

Planificación de actividades de seguridad

- Mantener en todo momento la regla de 'funcionalidad mínima'.
- Mantener en todo momento la regla de 'seguridad por defecto'.
- Buscar la interrupción mínima del servicio.
- Comunicar a todo el personal relacionado.
- Definir responsabilidades y responsables.

5.2.1.16. Adquisición / desarrollo

Servicios: Adquisición o desarrollo

- Establecer previamente los requisitos funcionales.

- Tomar en cuenta los requisitos de: control de acceso, identificación y autenticación, disponibilidad, integridad y confidencialidad.
- Identificar los requisitos técnicos de seguridad en disponibilidad, integridad y confidencialidad.

Aplicaciones: Adquisición o desarrollo

- Establecer metodología de desarrollo.
- Emplear datos de prueba.
- Inspeccionar código fuente.
- Controlar cambio de asignaciones en programadores.
- Controlar el acceso al código fuente.
- Nombrar un responsable del código fuente para cada aplicación
- Requerir autorización previa para la actualización y entrega de código fuente a programadores.
- Controlar la realización de copias de seguridad del código fuente.
- Mantener un archivo de versiones anteriores.

- Evitar acceder al código fuente en los sistemas en producción.
- El entorno de desarrollo debe estar separado del de producción.
- Separación de funciones entre el personal que desarrolla y el personal encargado de producción.
- Las herramientas de desarrollo no deben ser accesibles al personal de producción.
- Controlar el acceso a las herramientas de desarrollo.
- El entorno de pre-producción (pruebas) debe estar separado del de producción.
- El entorno de pruebas debe simular realísticamente el entorno de producción.
- Emplear cuentas de usuario diferentes: pruebas y producción
- Revisar la corrección y completitud de la documentación en pruebas y producción.
- Verificar que el nuevo sistema no afecta negativamente a las otras funciones del sistema en el que va a operar.

Comunicaciones: Adquisición o contratación

- Establecer requisitos funcionales
- Identificar el tipo de conexión a establecer
- Revisar las características de la solución propuesta (sobre red pública o privada, de datos, de voz y datos, etc.)
- Identificar los requisitos de seguridad de acuerdo a los condicionantes del negocio (obligaciones legales, contractuales, estándares aplicables, políticas de la organización, certificaciones y/o acreditaciones).
- Revisar la arquitectura de la red de la organización, tipos de redes existentes (LAN, MAN, WLAN), protocolos empleados y aplicaciones de red.

Soportes de Información: Adquisición

- Disponer de normativa de adquisición.
- Planificar las necesidades e soportes de información.

Con la aplicación de las anteriores salvaguardas, el riesgo e impacto se reducen a un valor residual, el mismo que puede

aceptar la universidad o buscar una salvaguarda adicional con el fin de mitigar toda acción de amenaza. Si las salvaguardas no logran soportar la materialización de una amenaza, se aplicará el Plan de Contingencia Informática en situaciones críticas. En la Figura 5.4, se puede observar una proyección del nivel de protección cubierto con las salvaguardas.

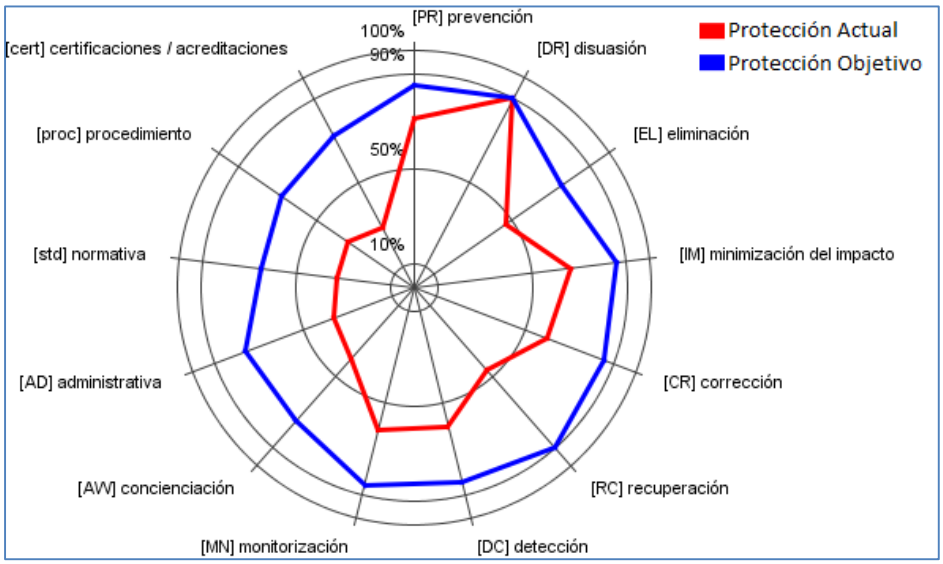

Figura 5.4: Proyección de protección con aplicación de Salvaguardas
Fuente: PILAR - Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

En las siguientes tablas se presenta la valoración de los activos en impacto y riesgo residual, luego de aplicar las salvaguardas:

Tabla 103: Impacto, riesgo y costo residual en Servicios Internos

[IS] Servicios Internos		D	I	C	A	T	Costo
[INTER_DTI] Internet	Impacto	5	2	5	1	5	Medio
	Riesgo	{3,6}	{1,6}	{2,6}	{0,7}	{4,4}	
[WEBS_DTI] Portal Web PUCESD	Impacto	3	2	1			Bajo
	Riesgo	{2,4}	{1,6}	{0,8}			
[EMAIL_DTI] Servicio Correo Electrónico Gmail	Impacto	5	2	5	4	5	Medio
	Riesgo	{3,6}	{1,6}	{2,6}	{1,8}	{4,4}	
[FILE_DTI] Almacenamiento de Archivos	Impacto	3	2	5	3	2	Despreciable
	Riesgo	{2,4}	{1,7}	{2,6}	{1,2}	{2,6}	

Fuente: PILAR - Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

Tabla 104: Impacto, riesgo y costo residual en Aplicaciones

[SW] Aplicaciones		D	I	C	A	T	Costo
[PROD_DTI] Sistemas Informáticos de Producción	Impacto	5	4	5	6	5	Medio
	Riesgo	{3,6}	{3,3}	{3,3}	{4,2}	{4,4}	
[PWEB_DTI] Servicios Portal Web	Impacto	3	1	0	0	0	Bajo
	Riesgo	{2,4}	{1,4}	{0,7}	{0,6}	{0,9}	
[BIBL_DTI] Sistema de Biblioteca	Impacto	5	1	1	0	0	Bajo
	Riesgo	{3,6}	{0,9}	{0,8}	{0,4}	{0,9}	
[PROF_DTI] Sistema administrador de personal docente	Impacto	0	1	3	3	3	Despreciable
	Riesgo	{0,9}	{0,9}	{1,4}	{1,2}	{3,2}	

[BIOM_DTI] Sistema para control de ingreso de personal	Impacto	3	1	0	2	1	Bajo
	Riesgo	{2,4}	{0,9}	{0,6}	{0,9}	{2,0}	
[FILEBA_DTI] Software para respaldo de archivos	Impacto	0		0	6	3	Despreciable
	Riesgo	{0,9}		{0,6}	{2,9}	{3,2}	
[PFFI_DTI] Office - Ofimática	Impacto	0				2	Despreciable
	Riesgo	{0,4}				{1,9}	
[AV_DTI] Antivirus	Impacto	0				2	Despreciable
	Riesgo	{0,6}				{1,9}	
[OS_DTI] Sistema Operativo	Impacto	0			4		Despreciable
	Riesgo	{0,6}			{1,8}		

Fuente: PILAR - Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

Tabla 105: Impacto, riesgo y costo residual en Equipos

[HW] Equipos		**D**	**I**	**C**	**A**	**T**	**Costo**
[PRODS_DTI] Servidor de Producción	Impacto	4	4	5	6	4	Medio
	Riesgo	{3,6}	{3,1}	{3,3}	{4,2}	{4,1}	
[DSKB_DTI] Disco para respaldos de Sistemas Informáticos de Producción	Impacto	2	2	4	6	4	Medio
	Riesgo	{2,3}	{1,7}	{2,7}	{4,2}	{2,6}	
[PWEBS_DTI] Servidor Portal Web	Impacto	2	2		2	2	Bajo
	Riesgo	{2,4}	{1,6}		{0,9}	{2,9}	
[BIBLS_DTI] Servidor Sistema de Biblioteca	Impacto	4	2		2	0	Bajo
	Riesgo	{3,6}	{1,6}		{0,9}	{1,7}	
[PROFS_DTI] Servidor Sistema administrador de personal docente	Impacto	0	1	1	1	0	Despreciable
	Riesgo	{0,9}	{0,9}	{0,9}	{0,7}	{1,1}	
[BIOMS_DTI] Servidor Sistema para control de ingreso de personal	Impacto	2	1	1	3	2	Bajo
	Riesgo	{2,4}	{0,9}	{0,9}	{1,2}	{2,9}	
[FILEBAS_DTI] Servidor Respaldo de Archivos	Impacto	0	1	1	3	1	Bajo
	Riesgo	{0,9}	{0,9}	{0,9}	{1,2}	{2,3}	

[PROXS_DTI] Servidor Proxy Firewall	Impacto	4	2	2	6	4	Bajo
	Riesgo	{3,6}	{1,6}	{1,3}	{2,9}	{4,1}	
[DHCPS_DTI] Servidor DHCP	Impacto	3	0		4	1	Bajo
	Riesgo	{2,4}	{0,8}		{1,8}	{2,0}	
[SWITCH_DTI] Switch	Impacto	2	2		4	2	Bajo
	Riesgo	{2,4}	{1,6}		{1,8}	{2,9}	
[Router] Router	Impacto	5	4		6	4	Medio
	Riesgo	{3,6}	{2,7}		{2,9}	{4,2}	
[WLC_DTI] Controladora de red inalámbrica	Impacto	2	0		4	3	Bajo
	Riesgo	{1,8}	{0,6}		{1,8}	{3,2}	
[WAP] Punto de Acceso Inalámbrico	Impacto	2	2		4	3	Despreciable
	Riesgo	{1,8}	{1,6}		{1,8}	{3,2}	

Fuente: PILAR - Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

Tabla 106: Impacto, riesgo y costo residual en Comunicaciones

[COM] Comunicaciones		**D**	**I**	**C**	**A**	**T**	**Costo**
[LAN_DTI] Red LAN	Impacto	3	2		4	3	Bajo
	Riesgo	{2,4}	{1,6}		{1,8}	{3,2}	
[WLAN_DTI] Red LAN Inalámbrica	Impacto	2	1		4	3	Bajo
	Riesgo	{1,8}	{0,9}		{1,8}	{3,2}	
[INTERNET_DTI] Servicio de Internet	Impacto	5	4	3	4	3	Medio
	Riesgo	{3,6}	{2,7}	{1,4}	{1,8}	{3,2}	

Fuente: PILAR - Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

Tabla 107: Impacto, riesgo y costo residual en Elementos Auxiliares

[AUX] Elementos Auxiliares		D	I	C	A	T	Costo
[SAI_DTI] Sistema de alimentación ininterrumpida	Impacto	1					Bajo
	Riesgo	{2,7}					
[AC_DTI] Aire Acondicionado	Impacto	1					Bajo
	Riesgo	{0,6}					
[CABLE_DTI] Cableado de Datos	Impacto	2				2	Bajo
	Riesgo	{2,4}				{2,9}	

Fuente: PILAR - Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

Tabla 108: Impacto, riesgo y costo residual en Servicios subcontratados

[SS] Servicios subcontratados		D	I	C	A	T	Costo
[BIBLIOSUB_DTI] Proveedor Sistema Biblioteca	Impacto	0					Bajo
	Riesgo	{0,6}					
[BIOMSUB_DTI] Proveedor Sistema para control de ingreso de personal	Impacto	0					Bajo
	Riesgo	{0,6}					
[INTERSUB_DTI] Servicio de Internet	Impacto	3					Medio
	Riesgo	{3,6}					

Fuente: PILAR - Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

Tabla 109: Impacto, riesgo y costo residual en Instalaciones

[L] Instalaciones		D	I	C	A	T	Costo
[CCTRL_DTI] Cuarto de Control	Impacto	4	3	3	4		Medio
	Riesgo	{2,8}	{1,9}	{1,3}	{2,4}		

Fuente: PILAR - Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

Tabla 110: Impacto, riesgo y costo residual en Personal

[P] Personal		D	I	C	A	T	Costo
[ADMP_DTI] Administradores de Sistemas Informáticos - Programadores	Impacto	2		4			Bajo
	Riesgo	{1,6}		{2,4}			
[REDES_DTI] Administradores de infraestructura y telecomunicaciones	Impacto	1		3			Bajo
	Riesgo	{1,6}		{1,9}			
[SOPTE_DTI] Soporte Técnico	Impacto	0					Bajo
	Riesgo	{0,8}					

Fuente: PILAR - Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

En la Figura 5.5 se presenta de forma gráfica el resultado del análisis de riesgos e impacto, permitiendo identificar con mayor facilidad aquellos activos que aún poseen un alto nivel de riesgo, y en los cuales se plantea la contingencia correspondiente.

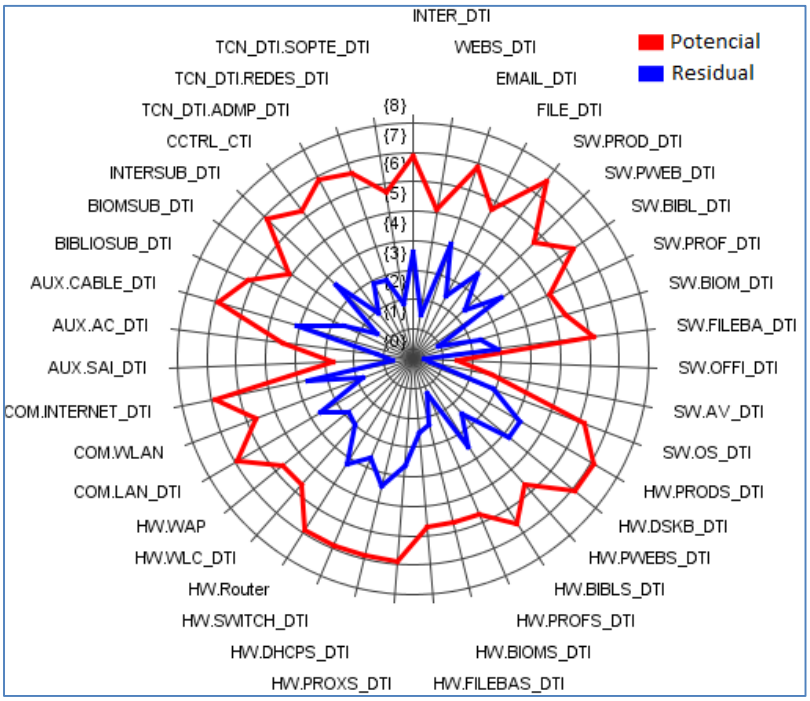

Figura 5.5: Identificación de Riesgo Potencial y Residual en Activos
Fuente: PILAR - Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

5.3. Definición de eventos a ser considerados para contingencia

Partiendo de los resultados arrojados del análisis de riesgos e impacto, se identifican los activos que poseen un alto nivel de riesgo y que comprometen importantes actividades o procesos de gestión en la universidad. Los activos seleccionados son:

Tabla 111: Activos seleccionados para Contingencia

SERVICIOS INTERNOS Y SERVICIOS SUBCONTRATADOS	
1	[INTER_DTI] Internet
2	[EMAIL_DTI] Servicio Correo Electrónico Gmail
3	[INTERNET_DTI] Servicio de Internet
4	[INTERSUB_DTI] Servicio de Internet
APLICACIONES Y EQUIPOS	
5	[PROD_DTI] Sistemas Informáticos de Producción
6	[PRODS_DTI] Servidor de Producción
7	[BIBL_DTI] Sistema de Biblioteca
8	[BIBLS_DTI] Servidor Sistema de Biblioteca
9	[BIOM_DTI] Sistema para control de ingreso de personal
10	[BIOMS_DTI] Servidor Sistema para control de ingreso de personal
11	[DSKB_DTI] Disco para respaldos de Sistemas Informáticos de Producción
12	[PROXS_DTI] Servidor Proxy Firewall
13	[DHCPS_DTI] Servidor DHCP
14	[SWITCH_DTI] Switch
15	[Router] Router
COMUNICACIONES	
16	[LAN_DTI] Red LAN
ELEMENTOS AUXILIARES	
17	[CABLE_DTI] Cableado de Datos
PERSONAL	
18	[ADMP_DTI] Administradores de Sistemas Informáticos - Programadores
19	[REDES_DTI] Administradores de infraestructura y telecomunicaciones

Fuente: Resultados de análisis de riesgos e impacto
Elaborado: Ing. Franklin Carrasco

Para mantener la disponibilidad de los activos mediante el plan de contingencia informática, se solicitó la cooperación de la Dirección de Tecnologías de la Información con el fin de determinar los principales eventos (riesgos) que pueden afectar a las actividades de la universidad.

También se definieron los tiempos requeridos para la recuperación parcial o total de los servicios, y los departamentos afectados. Estos eventos se presentan en las siguientes tablas:

5.3.1. Riesgo: Interrupción Total o Parcial del Servicio de Internet

Tabla 112: Riesgo Interrupción total o parcial del servicio de Internet

<table>
<tr><td colspan="3">RIESGO: INTERRUPCIÓN TOTAL O PARCIAL DEL SERVICIO DE INTERNET</td></tr>
<tr><td colspan="3">SITUACIONES CRÍTICAS:</td></tr>
<tr><td colspan="3">• Periodo de Matrículas
• Periodo normal de clases de grado y posgrado</td></tr>
<tr><td>DEPARTAMENTOS AFECTADOS:</td><td colspan="2">SERVICIOS AFECTADOS:</td></tr>
<tr><td>Todos los departamentos</td><td colspan="2">• Correo electrónico institucional
• Almacenamiento de Archivos
• Mensajería Instantánea (Chat)
• Salas de Cómputo</td></tr>
<tr><td>ACTIVOS EN RIESGO</td><td>PUNTO OBJETIVO DE RECUPERACIÓN (RPO)</td><td>TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)</td></tr>
<tr><td>[INTERSUB_DTI] Proveedor de Servicios de Internet</td><td>1 hora</td><td>1 hora</td></tr>
<tr><td>[DHCPS_DTI] Servidor DHCP</td><td>2 horas</td><td>3 horas</td></tr>
<tr><td>[PROXS_DTI] Servidor Proxy Firewall</td><td>2 horas</td><td>3 horas</td></tr>
<tr><td>[Router] Router</td><td>2 horas</td><td>2 días</td></tr>
<tr><td>[CABLE_DTI] Cableado de Datos - Fibra</td><td>1 hora</td><td>2 días</td></tr>
</table>

Fuente: Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

5.3.2. Riesgo: Daño Físico o Lógico en Servidor de Producción

Tabla 113: Riesgo por daño físico o lógico en servidor de producción

<table>
<tr><td colspan="3">RIESGO: DAÑO FÍSICO O LÓGICO EN SERVIDOR DE PRODUCCIÓN</td></tr>
<tr><td colspan="3">SITUACIONES CRÍTICAS:</td></tr>
<tr><td colspan="3">• Periodo de Matrículas
• Contabilidad/Adquisiciones/Gestión Tributaria/Facturación/Presupuesto
• Generación de roles</td></tr>
<tr><td>DEPARTAMENTOS AFECTADOS:</td><td colspan="2">SERVICIOS AFECTADOS:</td></tr>
<tr><td>• Dirección Académica
• Dirección Financiera
• Dirección Recursos Humanos</td><td colspan="2">• Sistema Académico
• Sistema Financiero
• Sistema Nómina</td></tr>
<tr><td>ACTIVOS EN RIESGO</td><td>PUNTO OBJETIVO DE RECUPERACIÓN (RPO)</td><td>TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)</td></tr>
<tr><td>[PROD_DTI] Sistemas Informáticos de Producción</td><td rowspan="2">3 horas</td><td rowspan="2">8 horas</td></tr>
<tr><td>[PRODS_DTI] Bases de Datos / Servidor de Producción</td></tr>
</table>

Fuente: Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

5.3.3. Riesgo: Daño Lógico en el Motor de la Base de Datos instalada en el Servidor de Producción

Tabla 114: Riesgo por daño lógico en el motor de la base de datos instalada en el servidor de producción

<table>
<tr><td colspan="3">RIESGO: DAÑO LÓGICO EN EL MOTOR DE LA BASE DE DATOS INSTALADA EN EL SERVIDOR DE PRODUCCIÓN</td></tr>
<tr><td colspan="3">SITUACIONES CRÍTICAS:</td></tr>
<tr><td colspan="3">• Periodo de Matrículas
• Contabilidad/Adquisiciones/Gestión Tributaria/Facturación/Presupuesto
• Generación de roles</td></tr>
<tr><td>DEPARTAMENTOS AFECTADOS:</td><td colspan="2">SERVICIOS AFECTADOS:</td></tr>
<tr><td>• Dirección Académica
• Dirección Financiera
• Dirección Recursos Humanos</td><td colspan="2">• Sistema Académico
• Sistema Financiero
• Sistema Nómina</td></tr>
<tr><td>ACTIVOS EN RIESGO</td><td>PUNTO OBJETIVO DE RECUPERACIÓN (RPO)</td><td>TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)</td></tr>
<tr><td>[PRODS_DTI] Bases de Datos / Servidor de Producción</td><td>2 horas</td><td>4 horas</td></tr>
</table>

Fuente: Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

5.3.4. Riesgo: Daño Físico o Lógico en Servidor de Biblioteca

Tabla 115: Riesgo por daño físico o lógico en servidor de biblioteca

<table>
<tr><td colspan="3">RIESGO: DAÑO FÍSICO O LÓGICO EN SERVIDOR DE BIBLIOTECA</td></tr>
<tr><td colspan="3">SITUACIONES CRÍTICAS:</td></tr>
<tr><td colspan="3">• Periodo de evaluación de servicio de biblioteca
• Periodo normal de clases de grado y posgrado
• Periodo de revisión de bibliografía previo al inicio de clases</td></tr>
<tr><td>DEPARTAMENTOS AFECTADOS:</td><td colspan="2">SERVICIOS AFECTADOS:</td></tr>
<tr><td>• Dirección Académica
• Biblioteca</td><td colspan="2">• Sistema Biblioteca
• Servicio de consulta de Libros</td></tr>
<tr><td>ACTIVOS EN RIESGO</td><td>PUNTO OBJETIVO DE RECUPERACIÓN (RPO)</td><td>TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)</td></tr>
<tr><td>[BIBL_DTI] Sistema de Biblioteca</td><td rowspan="2">8 horas</td><td rowspan="2">2 días</td></tr>
<tr><td>[BIBLS_DTI] Bases de Datos / Servidor Sistema de Biblioteca</td></tr>
</table>

Fuente: Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

5.3.5. Riesgo: Daño Lógico en el Motor de la Base de Datos instalada en el Servidor de Biblioteca

Tabla 116: Riesgo por daño lógico en el motor de la base de datos instalada en el servidor de biblioteca

<table>
<tr><td colspan="3">RIESGO: DAÑO LÓGICO EN EL MOTOR DE LA BASE DE DATOS INSTALADA EN EL SERVIDOR DE BIBLIOTECA</td></tr>
<tr><td colspan="3">SITUACIONES CRÍTICAS:</td></tr>
<tr><td colspan="3">• Periodo de evaluación de servicio de biblioteca
• Periodo normal de clases de grado y posgrado
• Periodo de revisión de bibliografía previo al inicio de clases</td></tr>
<tr><td>DEPARTAMENTOS AFECTADOS:</td><td colspan="2">SERVICIOS AFECTADOS:</td></tr>
<tr><td>• Dirección Académica
• Biblioteca</td><td colspan="2">• Sistema Biblioteca</td></tr>
<tr><td>ACTIVOS EN RIESGO</td><td>PUNTO OBJETIVO DE RECUPERACIÓN (RPO)</td><td>TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)</td></tr>
<tr><td>[BIBLS_DTI] Bases de Datos / Servidor Sistema de Biblioteca</td><td>8 horas</td><td>2 días</td></tr>
</table>

Fuente: Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

5.3.6. Riesgo: Daño Físico o Lógico en Servidor del Sistema para Control de Ingreso de Personal

Tabla 117: Riesgo por daño físico o lógico en servidor del sistema para control de ingreso de personal

<table>
<tr><td colspan="3">RIESGO: DAÑO FÍSICO O LÓGICO EN SERVIDOR DEL SISTEMA PARA CONTROL DE INGRESO DE PERSONAL</td></tr>
<tr><td colspan="3">SITUACIONES CRÍTICAS:</td></tr>
<tr><td colspan="3">• Generación de roles
• Pago de sueldos</td></tr>
<tr><td>DEPARTAMENTOS AFECTADOS:</td><td colspan="2">SERVICIOS AFECTADOS:</td></tr>
<tr><td>• Dirección Académica
• Dirección Financiera
• Dirección Recursos Humanos</td><td colspan="2">• Sistema Nómina
• Sistema Financiero</td></tr>
<tr><td>ACTIVOS EN RIESGO</td><td>PUNTO OBJETIVO DE RECUPERACIÓN (RPO)</td><td>TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)</td></tr>
<tr><td>[BIOM_DTI] Sistema para control de ingreso de personal</td><td rowspan="2">8 horas</td><td rowspan="2">2 días</td></tr>
<tr><td>[BIOMS_DTI] Bases de Datos / Servidor Sistema para control de ingreso de personal</td></tr>
</table>

Fuente: Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

5.3.7. Riesgo: Daño Lógico en el Motor de la Base de Datos instalada en el Servidor del Sistema para Control de Ingreso de Personal

Tabla 118: Riesgo por daño lógico en el motor de la base de datos instalada en el servidor del sistema para control de ingreso de personal

<table>
<tr><td colspan="3">RIESGO: DAÑO LÓGICO EN EL MOTOR DE LA BASE DE DATOS INSTALADA EN EL SERVIDOR DEL SISTEMA PARA CONTROL DE INGRESO DE PERSONAL</td></tr>
<tr><td colspan="3">SITUACIONES CRÍTICAS:</td></tr>
<tr><td colspan="3">• Generación de roles
• Pago de sueldos</td></tr>
<tr><td>DEPARTAMENTOS AFECTADOS:</td><td colspan="2">SERVICIOS AFECTADOS:</td></tr>
<tr><td>• Dirección Académica
• Dirección Financiera
• Dirección Recursos Humanos</td><td colspan="2">• Sistema Nómina
• Sistema Financiero
• Sistema para el control de ingreso de personal</td></tr>
<tr><td>ACTIVOS EN RIESGO</td><td>PUNTO OBJETIVO DE RECUPERACIÓN (RPO)</td><td>TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)</td></tr>
<tr><td>[BIOMS_DTI] Bases de Datos / Servidor Sistema para control de ingreso de personal</td><td>8 horas</td><td>2 días</td></tr>
</table>

Fuente: Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

5.3.8. Riesgo: Daños en Equipos Activos y Medios Físicos empleados para la Comunicación de Datos

Tabla 119: Riesgo por daños en equipos activos y medios físicos empleados para la comunicación de datos

RIESGO: DAÑOS EN EQUIPOS ACTIVOS Y MEDIOS FÍSICOS EMPLEADOS PARA LA COMUNICACIÓN DE DATOS		
SITUACIONES CRÍTICAS:		
• En todo momento		
DEPARTAMENTOS AFECTADOS:	**SERVICIOS AFECTADOS:**	
• Todos los departamentos	• Todos los servicios informáticos	
ACTIVOS EN RIESGO	**PUNTO OBJETIVO DE RECUPERACIÓN (RPO)**	**TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)**
[Router] Router	2 horas	2 días
[SWITCH_DTI] Switch	2 horas	1 día
[DHCPS_DTI] Servidor DHCP	2 horas	3 horas
[PROXS_DTI] Servidor Proxy/Firewall	2 horas	3 horas
[CABLE_DTI] Cableado de Datos – Fibra	1 hora	2 días

Fuente: Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

5.3.9. Riesgo: Corte de Energía Eléctrica

Tabla 120: Riesgo por corte de energía eléctrica

<table>
<tr><td colspan="3">RIESGO: CORTE DE ENERGÍA ELÉCTRICA</td></tr>
<tr><td colspan="3">SITUACIONES CRÍTICAS:</td></tr>
<tr><td colspan="3">• Periodo de Matrículas
• Contabilidad/Adquisiciones/Gestión Tributaria/Facturación/Presupuesto
• Generación de roles</td></tr>
<tr><td>DEPARTAMENTOS AFECTADOS:</td><td colspan="2">SERVICIOS AFECTADOS:</td></tr>
<tr><td>• Todos los departamentos</td><td colspan="2">• Todos los servicios informáticos</td></tr>
<tr><td>ACTIVOS EN RIESGO</td><td>PUNTO OBJETIVO DE RECUPERACIÓN (RPO)</td><td>TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)</td></tr>
<tr><td>[PROD_DTI] Sistemas Informáticos de Producción</td><td rowspan="8">1 hora</td><td rowspan="8">3 horas</td></tr>
<tr><td>[PRODS_DTI] Bases de Datos / Servidor de Producción</td></tr>
<tr><td>[BIBL_DTI] Sistema de Biblioteca</td></tr>
<tr><td>[BIBLS_DTI] Bases de Datos / Servidor Sistema de Biblioteca</td></tr>
<tr><td>[BIOM_DTI] Sistema para control de ingreso de personal</td></tr>
<tr><td>[BIOMS_DTI] Bases de Datos / Servidor Sistema para control de ingreso de personal</td></tr>
<tr><td>[SWITCH_DTI] Switch</td></tr>
</table>

Fuente: Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

5.3.10. Riesgo: Ausencia Parcial o Permanente del Personal Técnico

Tabla 121: Riesgo por ausencia parcial o permanente del personal técnico

<table>
<tr><td colspan="3">RIESGO: AUSENCIA PARCIAL O PERMANENTE DEL PERSONAL TÉCNICO</td></tr>
<tr><td colspan="3">SITUACIONES CRÍTICAS:</td></tr>
<tr><td colspan="3">• Periodo de Matrículas
• Contabilidad/Adquisiciones/Gestión Tributaria/Facturación/Presupuesto
• Generación de roles
• Periodo de evaluación institucional</td></tr>
<tr><td colspan="2">DEPARTAMENTOS AFECTADOS:</td><td>SERVICIOS AFECTADOS:</td></tr>
<tr><td colspan="2">• Dirección de Tecnologías de la Información
• Dirección Académica
• Dirección Financiera
• Dirección Recursos Humanos
• Biblioteca</td><td>• Sistema Académico
• Sistema Financiero
• Sistema Nómina
• Sistema de Biblioteca
• Sistema para control de ingreso de personal
• Servicios Web
• Servicio de Internet
• Seguridad de red
• Data Center (Centro de Datos)
• Comunicaciones
• Soporte a usuarios
• Salas de Cómputo</td></tr>
<tr><td>ACTIVOS EN RIESGO</td><td>PUNTO OBJETIVO DE RECUPERACIÓN (RPO)</td><td>TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)</td></tr>
<tr><td>[PROD_DTI] Sistemas Informáticos de Producción</td><td rowspan="8">7 días</td><td rowspan="8">15 días</td></tr>
<tr><td>[PRODS_DTI] Bases de Datos / Servidor de Producción</td></tr>
<tr><td>[BIBL_DTI] Sistema de Biblioteca</td></tr>
<tr><td>[BIBLS_DTI] Bases de Datos / Servidor Sistema de Biblioteca</td></tr>
<tr><td>[BIOM_DTI] Sistema para control de ingreso de personal</td></tr>
<tr><td>[BIOMS_DTI] Bases de Datos / Servidor Sistema para control de ingreso de personal</td></tr>
<tr><td>[Router] Router</td></tr>
</table>

[SWITCH_DTI] Switch		
[PROXS_DTI] Servidor Proxy/Firewall		
[DHCPS_DTI] Servidor DHCP		
[CABLE_DTI] Cableado de Datos - Fibra		

Fuente: Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

5.3.11. Riesgo: Incendio Oficinas DTI o Centro de Datos

Tabla 122: Riesgo por incendio oficinas de DTI o Centro de Datos

RIESGO: INCENDIO OFICINAS DTI O CENTRO DE DATOS		
SITUACIONES CRÍTICAS:		
• Periodo de Matrículas • Generación de roles • Periodo normal de clases de grado y posgrado		
DEPARTAMENTOS AFECTADOS:	**SERVICIOS AFECTADOS:**	
• Dirección de Tecnologías de la Información • Dirección Académica • Dirección Financiera • Dirección Recursos Humanos • Biblioteca	• Todos los servicios informáticos	
ACTIVOS EN RIESGO	**PUNTO OBJETIVO DE RECUPERACIÓN (RPO)**	**TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)**
[PRODS_DTI] Servidor de Producción	2 días	5 días
[BIBLS_DTI] Servidor Sistema de Biblioteca		
[BIOMS_DTI] Servidor Sistema para control de ingreso de personal		
[DSKB_DTI] Disco para respaldos de Sistemas Informáticos de Producción		
[Router] Router		
[SWITCH_DTI] Switch		
[PROXS_DTI] Servidor Proxy/Firewall		

[DHCPS_DTI] Servidor DHCP		
[LAN_DTI] Red LAN		

Fuente: Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

5.3.12. Riesgo: Desastres Naturales – Terremoto

Tabla 123: Riesgo por Desastres Naturales - Terremoto

RIESGO: DESASTRES NATURALES - TERREMOTO		
SITUACIONES CRÍTICAS:		
• En todo momento		
DEPARTAMENTOS AFECTADOS:	**SERVICIOS AFECTADOS:**	
• Todos los departamentos	• Todos los servicios	
ACTIVOS EN RIESGO	**PUNTO OBJETIVO DE RECUPERACIÓN (RPO)**	**TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)**
[PRODS_DTI] Servidor de Producción	2 días	15 días
[BIBLS_DTI] Servidor Sistema de Biblioteca		
[BIOMS_DTI] Servidor Sistema para control de ingreso de personal		
[DSKB_DTI] Disco para respaldos de Sistemas Informáticos de Producción		
[Router] Router		
[SWITCH_DTI] Switch		
[PROXS_DTI] Servidor Proxy/Firewall		
[DHCPS_DTI] Servidor DHCP		
[LAN_DTI] Red LAN		

Fuente: Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

5.4. Procedimientos para activación del plan

Para la activación del plan de contingencia se debe establecer una Normativa Interna que contenga los procedimientos a seguir con el fin de atender en el menor tiempo posible los daños ocurridos; de igual manera es importante determinar a la persona responsable de contactar al personal requerido para la recuperación de las actividades de la universidad. Entre los procedimientos que debe tener la normativa son:

5.4.1. Notificación de incidencias

El personal encargado de monitorear la funcionalidad de los servicios informáticos de la universidad, debe:

1. Contactar de forma inmediata a través de vía telefónica, al director, y personal técnico de Programación, Soporte Técnico, y Redes de la Dirección de Tecnologías de la Información, proporcionando una breve descripción del problema y los daños

causados. Por regla general, el Coordinador del plan de contingencia informática será siempre el Director de la DTI.

2. Realizar un registro manual donde identifique su nombre, una corta descripción de la incidencia, un resumen de los posibles daños, fecha y hora de la notificación, los nombres de las personas que fueron contactados y un breve detalle de las acciones que haya realizado.

5.4.2. Revisión de daños

Una vez que el personal técnico llegue al lugar del problema y según el tipo de incidente deberá:

1. Revisar la seguridad en las instalaciones (edificios), así como la disponibilidad del servicio eléctrico.
2. Revisar y evaluar los activos como servidores, discos de respaldo de datos, routers, switches, cableado de datos, equipos de oficina.

3. Revisar y evaluar el funcionamiento de los sistemas informáticos, el estado de los datos y los respaldos digitales requeridos para su activación.
4. Identificar daños críticos como pérdida de información, o destrucción física de equipos.
5. Determinar tiempos de recuperación para servidores, sistemas informáticos, routers, switches, cableado de datos, equipos de oficina y estructura física.

5.4.3. Notificación de impacto

Con el conocimiento previo de los daños ocurridos, el Coordinador del plan de contingencia informática debe:

1. Contactar a través de vía telefónica a directores, y principales autoridades para informar de manera verbal la gravedad de la situación.
2. Convocar una reunión emergente precedida por el Coordinador del plan de contingencia informática, en la cual deben participar:

personal técnico, directores y autoridades de la universidad, con el fin de informar el estado actual de los activos informáticos (cantidad de daños, tiempo de interrupción), así como los requerimientos tecnológicos necesarios para la recuperación de las actividades de la institución (adquisición de equipos, activación de centro de datos alterno). En cada reunión debe asignarse un secretario que realice el acta correspondiente para llegar a un acuerdo común entre los presentes.

3. Elaborar un listado de prioridades donde se identifiquen los servicios que puedan tener un mayor o menor tiempo de interrupción, bajo los criterios expuestos por las autoridades de la universidad.
4. Determinar la activación del plan de contingencia informática.

5.4.4. Activación parcial de los servicios informáticos

Definida la activación del plan de contingencia informática, el Coordinador debe dirigir y controlar el trabajo realizado por el personal técnico, para esto debe:

1. Determinar y listar a los miembros del equipo técnico que participarán en las actividades de recuperación inicial de: servidores, sistemas informáticos, equipos de comunicación (Switch, Router), red LAN, y servicios (Internet).
2. Asignar actividades de apoyo al personal técnico que no ha sido considerado dentro del plan de contingencia informática.
3. Listar y compartir los contactos del personal técnico para la comunicación a través de teléfonos celulares.
4. Identificar y activar uno de los sitios alternos establecidos en caso de contingencia, el lugar puede ser dentro o fuera del campus universitario.
5. Activar equipos de respaldo (servidores, switches, routers).
6. Respaldar sistemas informáticos y bases de datos, en servidores o equipos de respaldo (en caso de no poseer equipos espejo o infraestructura en la nube).
7. Asignar otras actividades de soporte y recuperación de Tecnología de la Información requeridas.
8. Registrar una bitácora de las actividades realizadas.
9. Contactar a las autoridades en caso de existir complicaciones con la recuperación de los servicios informáticos.
10. Verificar el funcionamiento de los servicios informáticos

5.4.5. Restablecimiento de los servicios informáticos

Una vez activados los servicios por la correcta ejecución del plan de contingencia informática, el Coordinador debe:

1. Brindar seguimiento a los procesos de adquisición, construcción, arreglo y mantenimiento de activos o instalaciones (edificios).
2. Realizar un cronograma de interrupción y activación, para el restablecimiento de los servicios a producción.
3. Inspeccionar a detalle el funcionamiento de todos los servicios y sistemas informáticos
4. Convocar una reunión informativa precedida por el Coordinador del plan de contingencia informática, en la cual deben participar: directores y autoridades de la universidad, con el fin de informar el restablecimiento de los servicios.
5. Presentar informe de actividades realizadas antes, durante y después de aplicar el plan de contingencia informática.

5.5. Funciones y responsabilidades del personal de TI

Para un adecuado desarrollo de las diferentes actividades del plan de contingencia informática es importante establecer equipos de trabajo, los cuales deberán ser dirigidos de forma organizada por el Coordinador del plan.

El Coordinador es el responsable de capacitar, coordinar y supervisar todas las actividades de recuperación, ya sea a través de simulacros que permitan al personal involucrado, tener una experiencia previa de la materialización de una amenaza; estos resultados asegurarán el éxito de los procedimientos establecidos, en caso de obtener fallas, deberá replantear los procesos de contingencia. Cada equipo de trabajo debe estar conformado por un líder, quien comparte la asignación de funciones y responsabilidades de acuerdo al trabajo que desempeñan en las unidades de Programación, Redes y Soporte Técnico. También se propone la participación de otros equipos de trabajo conformados por directores y coordinadores de departamentos tales como: Dirección Financiera, Dirección de Recursos Físicos, Dirección de Recursos Humanos, y Prorrectorado.

Por requerimiento de confidencialidad de la universidad no se detallan los nombres del personal técnico, pero se identifican los activos que les han sido asignados para su correspondiente recuperación.

5.5.1. Equipo de Redes

Se encarga de recuperar el servicio de comunicación de datos en la universidad, se conforma por dos técnicos de la unidad de Redes y un técnico de la unidad de soporte, las actividades a realizar son:

- Evaluar los daños en la red LAN y WLAN de la universidad.
- Reestablecer las configuraciones de los equipos activos de comunicación.
- Reestablecer los equipos servidores a nivel de Sistema Operativo y servicios de comunicación en servidores DHCP y Proxy.
- Redistribuir los equipos activos de comunicación para activar la comunicación en los principales departamentos de la universidad.
- Redistribuir el cableado de la red LAN para activar la comunicación en los principales departamentos de la universidad.

- Restaurar los servicios de comunicaciones en la red LAN y WLAN.
- Contactar a proveedor de servicio de Internet para la restauración del servicio.
- Realizar pruebas e informar los resultados.

Los activos asignados al equipo de redes se presentan en la tabla 124:

Tabla 124: Asignación de activos - Equipo de Redes

EQUIPO DE REDES	ACTIVOS ASIGNADOS
Técnico Redes 1 - Líder	• Switches • Router • Servicio de Internet
Técnico Redes 2	• Servidor Proxy • Servidor DHCP • Servidor Portal Web
Técnico Soporte A	• Cableado de red

Fuente: Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

5.5.2. Equipo de Programación

Posee una mayor carga de responsabilidad pues deben recuperar los sistemas informáticos de la institución, así como las bases de datos, varias de las actividades que deben realizar son:

- Evaluar los daños ocurridos en servidores y la funcionalidad de los sistemas informáticos.
- Asegurar la disponibilidad de los respaldos necesarios para la recuperación de los sistemas informáticos y sus bases de datos.
- Recuperar funcionalidad en servidores alternos de producción, biblioteca, e ingreso de personal.
- Restaurar sistemas informáticos con sus correspondientes bases de datos en servidores alternos.
- Respaldar los sistemas informáticos y las bases de datos en discos externos o sitios remotos.
- Revisar y configurar los sistemas informáticos en las estaciones de trabajo del personal administrativo (actividad compartida con el equipo de soporte técnico)
- Realizar cronogramas para revisión de funcionalidad en sitios alternos definidos para contingencia.

Los activos asignados al equipo de programación se presentan en la siguiente tabla:

Tabla 125: Asignación de activos - Equipo de Programación

EQUIPO DE PROGRAMACIÓN	ACTIVOS ASIGNADOS
Técnico Programación 1 – Líder	• Servidor de Producción • Sistemas Informáticos de Producción • Bases de datos de los sistemas informáticos de producción
Técnico Programación 2	• Servidor Sistema de Biblioteca • Sistema de Biblioteca • Base de datos del sistema de Biblioteca
Técnico Programación 3 - suplente del Líder	• Servidor Sistema de control de ingreso de personal • Sistema de control de ingreso de personal • Base de datos del Sistema de control de ingreso de personal • Configuración de sistemas informáticos en estaciones de trabajo
Técnico Soporte B	• Configuración de sistemas informáticos en estaciones de trabajo

Fuente: Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

5.5.3. Equipo de Soporte

El personal de la unidad de soporte técnico, además de participar como apoyo de los equipos de redes y programación, también tiene asignadas las siguientes responsabilidades:

- Activación de sitios alternos, establecidos como centro de datos provisionales.
- Recuperar estaciones de trabajo del personal administrativo.
- Revisar y configurar los sistemas informáticos en las estaciones de trabajo del personal administrativo (actividad compartida con el equipo de programación).

Tabla 126: Asignación de activos - Equipo de Soporte

EQUIPO DE SOPORTE	ACTIVOS ASIGNADOS
Técnico Soporte 1 - Líder	Activación de sitios alternos para centro de datos Estaciones de trabajo del personal administrativo
Técnico Soporte 2	

Fuente: Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

5.5.4. Equipo de Administrativo-Financiero

Es el equipo conformado por el personal de Dirección Financiera y Recursos Físicos, los cuales se encargarán de:

Tabla 127: Asignación de actividades al equipo Administrativo-Financiero

EQUIPO ADMINISTRATIVO-FINANCIERO	ACTIVIDADES ASIGNADAS
Auxiliar Adquisiciones	• Contactar proveedores • Contactar técnicos externos • Adquisición de equipos informáticos, como servidores, switches, routers
Auxiliar Recursos Físicos	• Adecuaciones Físicas • Movimiento de mobiliario
Auxiliar Recursos Humanos	• Contratar técnicos de TI

Fuente: Dirección de Tecnologías de la Información – PUCE SD
Elaborado: Ing. Franklin Carrasco

Las asignaciones antes mencionadas deberán ser redistribuidas de acuerdo a las capacidades de servicio que la universidad vaya implantando para docentes, estudiantes y personal administrativo.

5.6. Controles preventivos para procesos del negocio

Para minimizar la probabilidad de ocurrencia de una amenaza, es importante establecer procesos técnicos preventivos, que permitan respaldar o actuar de forma inmediata sobre los activos informáticos de la universidad. Partiendo de los riesgos determinados por la Dirección de Tecnologías de la Información y las salvaguardas definidas en el apartado 5.2 “Evaluación del impacto en la interrupción de la universidad“, se presenta a continuación una propuesta de acciones preventivas que permiten mantener la disponibilidad de los servicios y activos más críticos de la universidad.

5.6.1. Protección de los Servicios de Comunicación

Personal responsable: Equipo de Redes.

Riesgo: Interrupción total o parcial del servicio de Internet.

Acciones preventivas:

- Disponer de normativas que controlen el uso de los servicios de Internet, y correo electrónico.

- Identificar a cada técnico con las funciones asignadas para el control, administración y recuperación de los servicios de comunicación.
- Capacitar a los usuarios en el correcto uso del servicio de Internet e informar sobre las amenazas o ataques que pueden exponerse.
- Establecer y documentar los niveles de acceso del servicio de Internet para estudiantes, docentes y personal administrativo.
- Emplear herramientas de monitorización del tráfico en la red.
- Instalar en cada estación de trabajo software anti-virus y anti-spyware.
- Implantar IDS/IPS: Herramienta de detección / prevención de intrusión.
- Controlar la configuración y actualización de los navegadores.
- Disponer de equipos servidores de respaldo para los servicios DHCP, y Proxy Firewall.
- Disponer de respaldos de equipos activos como switches y router.
- Documentar los procesos a seguir para el restablecimiento del servicio de Internet, ya sea dentro o fuera del campus universitario.
- Disponer de un listado de contactos telefónicos del proveedor de servicios de Internet

5.6.2. Protección de la Información y Aplicaciones Informáticas

Personal responsable: Equipo de Programación.

Riesgo: Daño físico o lógico en el servidor de producción, daño lógico en el motor de la base de datos instalada en el servidor de producción, daño físico o lógico en servidor de biblioteca, daño lógico en el motor de la base de datos instalada en el servidor de biblioteca, daño físico o lógico en servidor del sistema para control de ingreso de personal, daño lógico en el motor de la base de datos instalada en el servidor del sistema para control de ingreso de personal.

Acciones preventivas:

- Disponer de normativas que controlen el uso de los sistemas informáticos institucionales, como también de la información administrada.
- Identificar a cada técnico con las funciones asignadas para el control, administración y recuperación de los sistemas informáticos y sus bases de datos.
- Disponer de un inventario de activos de información tales como sistemas informáticos, bases de datos, copias de seguridad, manuales, libros, software, hardware, contratos, y servicios informáticos.
- Documentar y resguardar credenciales de acceso (usuario/contraseña) a sistemas informáticos y bases de datos.

- Realizar copias de seguridad (backups) de los sistemas informáticos (código fuente- ejecutables) y las bases de datos y almacenarlos en sitios remotos (nube, centro de datos alternos, otra sede universitaria).
- Verificar el correcto funcionamiento de las copias de seguridad de los datos (backup) en entornos de prueba.
- Respaldar y verificar el correcto funcionamiento de las copias de seguridad de sistemas informáticos y bases de datos en servidores destinados para respaldo (backup).
- Registrar por escrito (bitácora) los respaldos obtenidos de los sistemas informáticos y bases de datos.
- Documentar y establecer perfiles de acceso en los sistemas informáticos a los usuarios para resguardar la confidencialidad de la información.
- Restringir el uso de ciertas aplicaciones a los usuarios en sus estaciones de trabajo.
- Respaldar y versionar el código fuente de los sistemas informáticos previa realización de cambios.
- Documentar cada cambio realizado en el código fuente o base de datos de los sistemas informáticos.
- Disponer de normativa u procedimientos de paso a operación / producción.

- Documentar registro de paso a operación / producción bajo previa autorización.

5.6.3. Protección de los Equipos Informáticos (HW)

Personal responsable: Equipo de Programación, Equipo de Redes.

Riesgo: Daño físico o lógico en servidor de producción, servidor de biblioteca, servidor del sistema para control de ingreso de personal, equipos activos y medios físicos empleados para la comunicación de datos.

Acciones preventivas:

- Disponer de normativas que controlen el uso y la administración de los servidores, equipos activos de comunicación y dispositivos de almacenamiento de datos.
- Identificar a cada técnico con las funciones asignadas para la administración, mantenimiento y recuperación de servidores, y equipos activos de comunicación.
- Disponer de un inventario de activos de información tales como bases de datos, copias de seguridad, manuales, libros, software, hardware, contratos, servicios informáticos, entre otros.

- Realizar copias de seguridad (backups) de la configuración de todos los equipos activos como switches, router, y servidores.
- Almacenar en sitios remotos (nube, centro de datos alternos, otra sede universitaria) respaldos de configuración de todos los equipos activos como switches, router, y servidores.
- Documentar y resguardar credenciales de acceso (usuario/contraseña) a switches, router, y servidores.
- Verificar el correcto funcionamiento de las copias de seguridad de las configuraciones en entornos de prueba.
- Registrar por escrito (bitácora) los respaldos de las configuraciones obtenidas en los equipos activos y servidores.
- Monitorear las capacidades de rendimiento (Memoria, CPU) de los equipos activos y servidores.
- Documentar y establecer perfiles de acceso en switches, router, y servidores.
- Resguardar y restringir el acceso de usuarios a los equipos activos y servidores.
- Prever el mantenimiento semestral de equipos activos y servidores, realizado por técnicos profesion0ales debidamente autorizados.
- Etiquetar y proteger servidores, equipos activos y conexiones de red (cableado).

5.6.4. Protección contra amenazas externas

Personal responsable: Equipo de Programación, Equipo de Redes, Equipo de Soporte Técnico.

Riesgo: Corte de energía eléctrica, incendio, desastres naturales.

Acciones preventivas:

- Disponer de sistema de alimentación ininterrumpida (SAI) en centro de datos y edificios de la universidad.
- Disponer de generador de energía eléctrica para centro de datos y edificios de la universidad.
- Proteger las líneas de alimentación del sistema frente a fluctuaciones y sobrecargas.
- Determinar interruptor general de la alimentación del sistema situado en la entrada de cada área.
- Etiquetar y proteger interruptores frente a activaciones accidentales.
- Activación de alimentación de respaldo eléctrico en caso de emergencia.
- Probar regularmente la alimentación de respaldo eléctrico.
- Realizar con regularidad el mantenimiento del sistema de alimentación de respaldo eléctrico.

- Disponer de señalética de emergencia para informar cómo proceder en caso de incendio o terremoto.
- Disponer de un sistema contra incendio en el centro de datos principal, con sensores de humo que generen una alarma identificativa del sitio.
- Disponer de extintores en los cuartos de comunicaciones y salas de cómputo los mismos que deben indicar las fechas de última y próxima recarga.
- Realizar revisiones semestrales de cada extintor, los mismos que deberán ser recargados cada doce meses en caso de no ser utilizados y en un plazo de tres días cuando ya han sido utilizados.
- Disponer de un sistema de aire acondicionado en el centro de datos principal para monitorear y controlar los niveles de temperatura y humedad.
- Capacitar y concientizar al personal sobre los sitios disponibles para fumadores, así como los procedimientos a seguir en caso de incendios o terremoto.
- Disponer de sitios alternos para el levantamiento de un centro de datos provisional.
- Disponer de contratos para asegurar los bienes y activos que se hayan siniestrado.

- Identificar a cada técnico con las funciones asignadas para actuar en caso de incendios o desastres naturales como terremotos.
- Disponer de un plan de evacuación de los activos informáticos (servidores, switches, router) más importantes para ser trasladados a centro de datos alternos.
- Identificar de forma visual (sticker de colores) los activos informáticos más críticos en la universidad, para priorizar su evacuación del lugar afectado.

5.6.5. Personal Técnico

Personal responsable: Dirección de tecnologías de la Información.

Riesgo: Ausencia parcial o permanente del personal técnico.

Acciones preventivas:

- Disponer de políticas o normas para el correcto desarrollo de la gestión en las áreas técnicas de la institución.
- Asignar funciones a cada técnico de acuerdo al área que pertenece.
- Asignar funciones de respaldo o actividades compartidas entre el personal técnico, como apoyo en caso de incidentes.

- Proporcionar formación en las funciones de cada rol del sistema.
- Disponer de personal técnico profesional.
- Asegurar que en todo momento exista más de un operador.
- Revisar funciones del personal en periodos de vacaciones.
- Disponer de un listado de contactos externos, como apoyo inmediato en situaciones de emergencia.
- Realizar capacitaciones periódicas entre el personal técnico de la universidad.

5.7. Estrategias de respaldo y recuperación

Al conocer la capacidad tecnológica que posee la universidad, es necesario disponer de los equipos o dispositivos que permitan la ejecución de las salvaguardas o acciones preventivas, manteniendo la disponibilidad de los servicios y sistemas informáticos. Se propone a la Dirección de Tecnologías de la Información ejecutar procesos de respaldo, para servidores, sistemas informáticos, equipos activos de comunicación, centro de datos alterno, estaciones de trabajo y personal técnico.

5.7.1. Servidores

Disponer de servidores de respaldo bajo la siguiente asignación:

Tabla 128: Propuesta de servidores para respaldo

SERVIDORES CRÍTICOS	SERVIDORES DE RESPALDO
Servidor de Producción	1
Servidor Proxy Firewall	1
Servidor DHCP	1
Servidor de Biblioteca Servidor para control de ingreso de personal	1
TOTAL	4

Fuente: Proyecto Plan de contingencia Informática
Elaborado: Ing. Franklin Carrasco

- Los servidores de respaldo deben estar configurados de forma similar que los servidores en producción.
- Los servidores de respaldo se deben proteger en un centro de datos provisional ya sea dentro o fuera del campus universitario (nube).

- Únicamente el personal técnico autorizado puede acceder a estos servidores, ya sea para su actualización, mantenimiento o contingencia.
- Se recomienda realizar la adquisición de una solución de servidores con tecnología blade, para reducir la complejidad en el respaldo de los servicios (virtualización), además de disponer de una solución inmediata en caso de fallas o daños sobre un equipo.

5.7.2. Sistemas Informáticos

- Disponer de un equipo de almacenamiento de datos (SAN) dedicado, para el respaldo de: configuraciones (equipos activos), documentación digital, Sistemas Informáticos y sus respectivas Bases de Datos, tanto en servicios virtualizados (nube), como en dispositivos físicos (hardware).
- En caso de disponer de un equipo de almacenamiento físico, este debe estar protegido en un centro de datos provisional ya sea dentro o fuera del campus universitario.
- Únicamente el personal técnico autorizado puede acceder a este equipo, ya sea para almacenar los nuevos respaldos o recuperarlos en caso de contingencia.
- Los respaldos deben almacenarse de forma diaria, luego de la revisión de funcionamiento en entornos de prueba.

5.7.3. Equipos Activos de comunicación

- La mayor parte de equipos activos que posee la universidad son CISCO, ante esto es recomendable disponer de un contrato de mantenimiento preventivo y correctivo 24/7 con un partner certificado, que permita el reemplazo inmediato del equipo en caso de daños o fallas.
- Se debe respaldar y almacenar la configuración de todos los switches, router y WLC, en el equipo de almacenamiento de datos correspondiente, cada vez que se realice un cambio en la red.
- Los cambios en las configuraciones de los equipos deben realizarse en entornos de prueba.
- Disponer de una propuesta de redistribución de equipos activos y enlaces de comunicación de datos, para mantener la disponibilidad del servicio de comunicación.

5.7.4. Centro de datos alterno

- Para mantener un control centralizado de los servidores y equipos activos, la institución se debe establecer un centro de datos principal y un centro de datos alterno.
- El centro de datos principal, como su alterno, deben tener la capacidad de mantener la disponibilidad de los servicios y sistemas informáticos, con elementos auxiliares como: aire acondicionado (climatización), sistema de alimentación de respaldo eléctrico (UPS), y generador de energía.
- El centro de datos alterno debe permitir la activación de los servicios y sistemas informáticos en capacidades mínimas.
- Una propuesta para el centro de datos alterno y principal es el levantamiento de los servicios a la sube (SaaS, IaaS, PaaS), así la universidad puede reducir costos e invertir en otros ámbitos de desarrollo institucional.
- Únicamente el personal técnico autorizado puede acceder en ambos centros de datos, bajo un restricto registro manual o digital (biométrico).

5.7.5. Estaciones de trabajo

- Para mantener la disponibilidad de los servicios y atención a los clientes se recomienda la implantación de un sistema de alimentación de respaldo eléctrico en los edificios San José y Misereor.
- Para evitar la pérdida de información en las estaciones de trabajo de los usuarios, se recomienda disponer de políticas, además de una solución de almacenamiento de datos (SAN), centralizando el servicio y resguardando los datos.

5.7.6. Personal Técnico

- Compartir actividades entre el personal técnico, como apoyo en caso de incidentes.
- Entrenar al personal técnico para actuar en situaciones emergentes.
- Disponer de documentación detallada sobre los procesos que debe desempeñar un técnico en caso de recuperación de un servidor, Switch, router, servicio o sistema informático.

5.8. Desarrollo del plan de contingencia informática

El Plan de contingencia Informática se desarrolla bajo los riesgos indicados por la Dirección de Tecnologías de la Información en el apartado "5.3 Definición de eventos a ser considerados para contingencia", los cuales están asociados con los activos más críticos que posee la universidad.

5.8.1. Contingencia: Interrupción Total o Parcial del Servicio de Internet, Daños en Equipos Activos y Medios Físicos empleados para la Comunicación de Datos

Tabla 129: Contingencia: Interrupción Total o Parcial del Servicio de Internet, Daños en Equipos Activos y Medios Físicos empleados para la Comunicación de Datos

CONTINGENCIA: INTERRUPCIÓN TOTAL O PARCIAL DEL SERVICIO DE INTERNET, DAÑOS EN EQUIPOS ACTIVOS Y MEDIOS FÍSICOS EMPLEADOS PARA LA COMUNICACIÓN DE DATOS
EQUIPO RESPONSABLE:
• Líder asignado para contingencia en la unidad de redes (guía e informa) • Personal técnico de la unidad de redes • Técnico de la unidad de soporte (logística)
AUTORIZA CONTINGENCIA:
• Coordinador de contingencia, o • Director de Tecnologías de la Información, o • Prorrectorado

<table>
<tr><td colspan="3">SITUACIONES CRÍTICAS:</td></tr>
<tr><td colspan="3">• Periodo de Matrículas
• Periodo normal de clases de grado y posgrado</td></tr>
<tr><td>DEPARTAMENTOS AFECTADOS:</td><td colspan="2">SERVICIOS AFECTADOS:</td></tr>
<tr><td>Todos los departamentos</td><td colspan="2">• Correo Electrónico Institucional
• Almacenamiento De Archivos
• Mensajería Instantánea (Chat)
• Salas De Cómputo</td></tr>
<tr><td>ACTIVOS EN RIESGO</td><td>PUNTO OBJETIVO DE RECUPERACIÓN (RPO)</td><td>TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)</td></tr>
<tr><td>[INTERSUB_DTI] Proveedor de Servicios de Internet</td><td>1 hora</td><td>1 hora</td></tr>
<tr><td>[DHCPS_DTI] Servidor DHCP</td><td>2 horas</td><td>3 horas</td></tr>
<tr><td>[PROXS_DTI] Servidor Proxy Firewall</td><td>2 horas</td><td>3 horas</td></tr>
<tr><td>[Router] Router</td><td>2 horas</td><td>2 días</td></tr>
<tr><td>[SWITCH_DTI] Switch</td><td>2 horas</td><td>1 día</td></tr>
<tr><td>[CABLE_DTI] Cableado de Datos - Fibra</td><td>1 hora</td><td>2 días</td></tr>
<tr><td colspan="3">ACTIVIDADES DE CONTINGENCIA:</td></tr>
</table>

1. Determinar la causa de la interrupción del servicio de Internet: conectividad con el ISP, configuración/funcionamiento de equipos activos, servidores de comunicación, y enlaces de red.

2. Comprobar los enlaces de red con el ISP, en caso de existir la interrupción del servicio, contactar telefónicamente al proveedor, para informar el problema. Si la solución propuesta excede un día de trabajo, se debe recurrir a un proveedor alterno.

3. Revisar la funcionalidad del router que posee la universidad, en caso de presentar fallas de configuración, reiniciar y cargar las configuraciones de respaldo; en caso de daños de hardware, contactar al partner de CISCO para solicitar el cambio inmediato del equipo, una vez recibido el nuevo router, cargar las configuraciones de respaldo.

4. Revisar la funcionalidad del servidor Proxy Firewall, en caso de encontrar problemas de configuración o hardware, activar el servidor Proxy Firewall alterno y restaurar el servicio; por otra parte debe determinar la causa de las fallas en el servidor Proxy Firewall principal, repararlo (formatear en caso de ser necesario), y realizar el cambio de equipo.

5. Revisar la funcionalidad del servidor DHCP, en caso de encontrar problemas de configuración o hardware, activar el servidor DHCP alterno y restaurar el servicio; por otra parte debe determinar la causa de las fallas en el servidor DHCP principal, repararlo (formatear en caso de ser necesario), y realizar el cambio de equipo.

6. En caso de daño en los equipos activos de comunicación, se deben ejecutar los procesos 3, 4 y 6.

7. Si el problema radica sobre un switch, se debe reemplazar el mismo por su alterno, y en caso de no disponer respaldos, retirar un switch de la Sala de Cómputo I, respaldarlo e eliminar la configuración del mismo, reiniciar el equipo y configurarlo con los parámetros correspondientes.

8. Si el fallo radica en el enlace de fibra, se debe realizar una conexión provisional con cable UTP CAT 6A, desde el sitio más cercano que posea actividad en sus servicios de red.

9. Registrar una memoria técnica de los problemas encontrados.

Elaborado: Ing. Franklin Carrasco

5.8.2. Contingencia: Daño Físico o Lógico en Servidor de Producción

Tabla 130: Daño Físico o Lógico en Servidor de Producción

<table>
<tr><td colspan="3">CONTINGENCIA: DAÑO FÍSICO O LÓGICO EN SERVIDOR DE PRODUCCIÓN</td></tr>
<tr><td colspan="3">EQUIPO RESPONSABLE:</td></tr>
<tr><td colspan="3">• Líder asignado para contingencia en la unidad de programación (Técnico Programación 1 - guía e informa)
• Personal técnico de la unidad de programación
• Equipo de soporte técnico (logística)</td></tr>
<tr><td colspan="3">AUTORIZA CONTINGENCIA:</td></tr>
<tr><td colspan="3">• Coordinador de contingencia, o
• Director de Tecnologías de la Información, o
• Prorrectorado</td></tr>
<tr><td colspan="3">SITUACIONES CRÍTICAS:</td></tr>
<tr><td colspan="3">• Periodo de Matrículas
• Contabilidad/Adquisiciones/Gestión Tributaria/Facturación/Presupuesto
• Generación de roles</td></tr>
<tr><td>DEPARTAMENTOS AFECTADOS:</td><td colspan="2">SERVICIOS AFECTADOS:</td></tr>
<tr><td>• Dirección Académica
• Dirección Financiera
• Dirección Recursos Humanos</td><td colspan="2">• Sistema Académico
• Sistema Financiero
• Sistema Nómina</td></tr>
<tr><td>ACTIVOS EN RIESGO</td><td>PUNTO OBJETIVO DE RECUPERACIÓN (RPO)</td><td>TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)</td></tr>
<tr><td>[PROD_DTI] Sistemas Informáticos de Producción</td><td rowspan="2">3 horas</td><td rowspan="2">8 horas</td></tr>
<tr><td>[PRODS_DTI] Bases de Datos / Servidor de Producción</td></tr>
<tr><td colspan="3">ACTIVIDADES DE CONTINGENCIA:</td></tr>
<tr><td colspan="3">1. Si se requiere de un tiempo mayor a 8 horas para solucionar los problemas ocurridos en el servidor de producción, se deberá realizar la activación del servidor alterno.

2. Contactar al personal administrativo que hace uso de los sistemas informáticos de producción para que eviten su utilización y tengan presente la información que han ingresado al sistema en las últimas 12 horas.</td></tr>
</table>

3. Desconectar al servidor de producción de la red de datos.

4. Activar el servidor alterno de producción.

5. Restaurar en el servidor alterno la base de datos de producción con la última actualización respaldada (en caso de no haberse realizado anticipadamente).

6. Restaurar en el servidor alterno los sistemas informáticos con la última versión utilizada en producción (en caso de no haberse realizado anticipadamente).

7. Cambiar la configuración de conexión en las estaciones de trabajo del personal administrativo, para conectar al servidor alterno (equipo de soporte).

8. Revisar la funcionalidad de los sistemas informáticos con los últimos respaldos aplicados.

9. Determinar la causa del daño en el servidor tanto en hardware, como en software (revisar logs).

10. Comprobar el funcionamiento del hardware del equipo, revisar el paso de corriente eléctrica al equipo, verificar problemas de disco duro, revisar funcionalidad de memorias, revisar funcionalidad de ventiladores, verificar funcionamiento de tarjeta de red.

11. En caso de tener un problema de hardware:

    - Contactar a los proveedores que dispongan de las partes o piezas requeridas y realicen el mantenimiento en sitio del equipo.
    - En caso de daño de disco duro y no existir respaldos, se debe intentar recuperar la información de la base de datos y del sistema informático.
    - Definir el alcance o estado de recuperación de la información de la base de datos y los sistemas informáticos.
    - Arreglado el hardware del servidor principal, se deberá restaurar la base de datos y los sistemas informáticos; si el daño del hardware ocurrió en el disco duro, se debe formatear, instalar y configurar el Sistema Operativo, sistema informático y bases de datos en el servidor.

12. En caso de tener un problema de software:

    - Los problemas de software que pueden ocurrir son: fallos del sistema operativo, virus y errores de configuración.
    - Respaldar el sistema informático y la base de datos.
    - Revisar las causas que generaron el problema para determinar la necesidad de formatear el disco duro.
    - Si se presentan fallas de actualización de Sistema Operativo, eliminar las actualizaciones y revisar su correcto funcionamiento.

- Si el problema se genera por causa de virus, se recomienda sacar una imagen del disco duro, formatear, instalar Sistema Operativo, instalar antivirus, configurar seguridades, instalar motor de base de datos, respaldar base de datos y sistemas informáticos. - Si el problema se genera por fallas de configuración, revisar accesos de usuarios, reglas de seguridad (firewall), fallas de memoria; resolver el problema e informar si es necesario formatear el disco duro del servidor. 13. Registrar una memoria técnica de los problemas encontrados. 14. Los procesos específicos para el levantamiento de los servidores se encuentran documentados por el líder de contingencia del equipo de la unidad de programación

Elaborado: Ing. Franklin Carrasco

5.8.3. Contingencia: Daño Lógico en el Motor de la Base de Datos instalada en el Servidor de Producción

Tabla 131: Contingencia: Daño Lógico en el Motor de la Base de Datos instalada en el Servidor de Producción

CONTINGENCIA: DAÑO LÓGICO EN EL MOTOR DE LA BASE DE DATOS INSTALADA EN EL SERVIDOR DE PRODUCCIÓN
EQUIPO RESPONSABLE:
• Líder asignado para contingencia en la unidad de programación (Técnico Programación 1 - guía e informa) • Personal técnico de la unidad de programación • Equipo de soporte técnico (logística)
AUTORIZA CONTINGENCIA:
• Coordinador de contingencia, o • Director de Tecnologías de la Información, o • Prorrectorado
SITUACIONES CRÍTICAS:
• Periodo de Matrículas

<table>
<tr><td colspan="3">• Contabilidad/Adquisiciones/Gestión Tributaria/Facturación/Presupuesto
• Generación de roles</td></tr>
<tr><td>DEPARTAMENTOS AFECTADOS:</td><td colspan="2">SERVICIOS AFECTADOS:</td></tr>
<tr><td>• Dirección Académica
• Dirección Financiera
• Dirección Recursos Humanos</td><td colspan="2">• Sistema Académico
• Sistema Financiero
• Sistema Nómina</td></tr>
<tr><td>ACTIVOS EN RIESGO</td><td>PUNTO OBJETIVO DE RECUPERACIÓN (RPO)</td><td>TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)</td></tr>
<tr><td>[PRODS_DTI] Bases de Datos / Servidor de Producción</td><td>2 horas</td><td>4 horas</td></tr>
<tr><td colspan="3">ACTIVIDADES DE CONTINGENCIA:

1. Si se requiere de un tiempo mayor a 4 horas para solucionar los problemas ocurridos en el servidor de producción, se deberá realizar la activación del servidor alterno.

2. Contactar al personal de la Coordinación de Secretarias, Secretaría General, Formación Continua, Posgrados, Direcciones de Escuela, Dirección Financiera, Dirección de Recursos Humanos, y Dirección de Recursos Físicos para que eviten utilizar los sistemas informáticos de producción y tengan presente la información que han ingresado al sistema en las últimas 12 horas.

3. Desconectar al servidor de producción de la red de datos.

4. Respaldar la base de datos de producción y los sistemas informáticos.

5. Obtener una imagen de disco del servidor de producción, para análisis de daños.

6. Activar el servidor alterno de producción.

7. El servidor alterno debe tener el mismo motor de la base de datos que el servidor principal, pero antes de activar el servicio debe verificar que el motor de la base datos no posea los mismos problemas que presenta el servidor de producción.

8. Restaurar en el servidor alterno la base de datos de producción con la última actualización respaldada (en caso de no haberse realizado anticipadamente).

9. Restaurar en el servidor alterno los sistemas informáticos con la última versión utilizada en producción (en caso de no haberse realizado anticipadamente).

10. Cambiar la configuración de conexión en las estaciones de trabajo del personal administrativo, para conectar al servidor alterno (equipo de soporte).</td></tr>
</table>

11. Revisar la funcionalidad de los servicios y los sistemas informáticos en las estaciones de trabajo del personal administrativo. 12. Revisar los problemas ocurridos con el motor de la base de datos (logs), se recomienda su reinstalación en caso de tener problemas leves, fáciles de reparar; se recomienda el formateo del disco duro si no se logra a través de las pautas o ayudas del fabricante, la reparación de la base de datos. 13. Registrar una memoria técnica de los problemas encontrados. 14. Realizada la reparación del motor de la base de datos en el servidor principal, se debe realizar el respaldo y activación del servicio fuera del horario normal de trabajo del personal administrativo.

Elaborado: Ing. Franklin Carrasco

5.8.4. Contingencia: Daño Físico o Lógico en Servidor de Biblioteca, Daño Físico o Lógico en Servidor del Sistema para Control de Ingreso de Personal

Tabla 132: Contingencia: Daño Físico o Lógico en Servidor de Biblioteca, Daño Físico o Lógico en Servidor del Sistema para Control de Ingreso de Personal

CONTINGENCIA: DAÑO FÍSICO O LÓGICO EN SERVIDOR DE BIBLIOTECA, DAÑO FÍSICO O LÓGICO EN SERVIDOR DEL SISTEMA PARA CONTROL DE INGRESO DE PERSONAL
EQUIPO RESPONSABLE:
• Líder asignado para contingencia en la unidad de programación (Técnico Programación 1 - guía e informa) • Técnico Programación 2 – Sistema de Biblioteca • Técnico Programación 3 – Sistema para control de ingreso de personal • Equipo de soporte técnico (logística)
AUTORIZA CONTINGENCIA:
• Coordinador de contingencia, o • Director de Tecnologías de la Información, o • Prorrectorado

<table>
<tr><td colspan="3">SITUACIONES CRÍTICAS:</td></tr>
<tr><td colspan="3">• Periodo de evaluación de servicio de biblioteca
• Periodo normal de clases de grado y posgrado
• Periodo de revisión de bibliografía previo al inicio de clases
• Generación de roles
• Pago de sueldos</td></tr>
<tr><td colspan="2">DEPARTAMENTOS AFECTADOS:</td><td>SERVICIOS AFECTADOS:</td></tr>
<tr><td colspan="2">• Dirección Académica
• Biblioteca
• Dirección Financiera
• Dirección Recursos Humanos</td><td>• Sistema Biblioteca
• Servicio de consulta de Libros
• Sistema Nómina
• Sistema Financiero</td></tr>
<tr><td>ACTIVOS EN RIESGO</td><td>PUNTO OBJETIVO DE RECUPERACIÓN (RPO)</td><td>TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)</td></tr>
<tr><td>[BIBL_DTI] Sistema de Biblioteca</td><td rowspan="4">8 horas</td><td rowspan="4">2 días</td></tr>
<tr><td>[BIBLS_DTI] Bases de Datos / Servidor Sistema de Biblioteca</td></tr>
<tr><td>[BIOM_DTI] Sistema para control de ingreso de personal</td></tr>
<tr><td>[BIOMS_DTI] Bases de Datos / Servidor Sistema para control de ingreso de personal</td></tr>
<tr><td colspan="3">ACTIVIDADES DE CONTINGENCIA:</td></tr>
<tr><td colspan="3">1. Para solucionar los problemas ocurridos en los servidores que sostienen al Sistema de Biblioteca, y al Sistema para Control de Personal, debe realizar la activación del servidor alterno que les corresponde.

2. Contactar al personal de biblioteca para que eviten utilizar el Sistema de Biblioteca, o contactar al personal de Recursos Humanos para que eviten utilizar el Sistema para Control de Personal, e indicar que tengan presente la información que han ingresado al sistema en las últimas 12 horas.

3. Desconectar al servidor de la red de datos.

4. Activar el servidor alterno de producción.

5. Restaurar en el servidor alterno la base de datos del Sistema de Biblioteca o la base de datos del Sistema para Control de Personal con la última actualización respaldada (en caso de no haberse realizado anticipadamente).

6. Restaurar o Instalar en el servidor alterno, el Sistema de Biblioteca, o el Sistema para Control de Personal con la última versión utilizada en producción (en caso de no haberse realizado anticipadamente).</td></tr>
</table>

7. Contactar al proveedor de cada Sistema Informático para que realice su activación en el servidor correspondiente.

8. Cambiar la configuración de conexión en las estaciones de trabajo del personal administrativo, para realizar la conexión al servidor alterno (equipo de soporte).

9. Revisar la funcionalidad del sistema informático con los últimos respaldos aplicados.

10. Determinar la causa del daño en el servidor tanto en hardware, como en software (revisar logs).

11. Comprobar el funcionamiento del hardware del servidor, revisar el paso de corriente eléctrica al equipo, verificar problemas de disco duro, revisar funcionalidad de memorias, revisar funcionalidad de ventiladores, verificar funcionamiento de tarjeta de red.

12. En caso de tener un problema de hardware:
    - Contactar a los proveedores que dispongan de las partes o piezas requeridas y realicen el mantenimiento en sitio del equipo.
    - En caso de daño de disco duro y no existir respaldos, se debe intentar recuperar la información de la base de datos.
    - Definir el alcance o estado de recuperación de la información de la base de datos.
    - Arreglado el hardware del servidor principal, se deberá restaurar la base de datos y el sistema informático; si el daño del hardware ocurrió en el disco duro, se debe formatear, instalar y configurar el Sistema Operativo, instalar el sistema informático y su base de datos.

13. En caso de tener un problema de software:
    - Los problemas de software que pueden ocurrir son: fallos del sistema operativo, virus y errores de configuración.
    - Respaldar la base de datos.
    - Revisar las causas que generaron el problema para determinar la necesidad de formatear el disco duro.
    - Si se presentan fallas de actualización de Sistema Operativo, eliminar las actualizaciones y revisar su correcto funcionamiento.
    - Si el problema se genera por causa de virus, se recomienda sacar una imagen del disco duro, formatear, instalar Sistema Operativo, instalar antivirus, configurar seguridades, instalar y subir motor de base de datos, e instalar el respectivo sistema informático.
    - Si el problema se genera por fallas de configuración, revisar accesos de usuarios, reglas de seguridad (firewall), fallas de memoria; resolver el problema e informar si es necesario formatear el disco duro del servidor.

14. Registrar una memoria técnica de los problemas encontrados.

15. Los procesos específicos para el levantamiento de cada servidor se encuentran documentados por el líder de contingencia del equipo de la unidad de programación.

Elaborado: Ing. Franklin Carrasco

5.8.5. Contingencia: Daño Lógico en el Motor de la Base de Datos instalada en el Servidor de Biblioteca, Daño Lógico en el Motor de la Base de Datos instalada en el Servidor del Sistema para Control de Ingreso de Personal

Tabla 133: Contingencia: Daño Lógico en el Motor de la Base de Datos instalada en el Servidor de Biblioteca, Daño Lógico en el Motor de la Base de Datos instalada en el Servidor del Sistema para Control de Ingreso de Personal

CONTINGENCIA: DAÑO LÓGICO EN EL MOTOR DE LA BASE DE DATOS INSTALADA EN EL SERVIDOR DE BIBLIOTECA, DAÑO LÓGICO EN EL MOTOR DE LA BASE DE DATOS INSTALADA EN EL SERVIDOR DEL SISTEMA PARA CONTROL DE INGRESO DE PERSONAL
EQUIPO RESPONSABLE:
• Líder asignado para contingencia en la unidad de programación (Técnico Programación 1 - guía e informa) • Técnico Programación 2 – Sistema de Biblioteca • Técnico Programación 3 – Sistema para control de ingreso de personal • Equipo de soporte técnico (logística)
AUTORIZA CONTINGENCIA:
• Coordinador de contingencia, o • Director de Tecnologías de la Información, o • Prorrectorado
SITUACIONES CRÍTICAS:
• Periodo de evaluación de servicio de biblioteca • Periodo normal de clases de grado y posgrado

<table>
<tr><td colspan="3">• Periodo de revisión de bibliografía previo al inicio de clases
• Generación de roles
• Pago de sueldos</td></tr>
<tr><td colspan="2">DEPARTAMENTOS AFECTADOS:</td><td>SERVICIOS AFECTADOS:</td></tr>
<tr><td colspan="2">• Dirección Académica
• Biblioteca
• Dirección Financiera
• Dirección Recursos Humanos</td><td>• Sistema Biblioteca
• Sistema Nómina
• Sistema Financiero
• Sistema para el control de ingreso de personal</td></tr>
<tr><td>ACTIVOS EN RIESGO</td><td>PUNTO OBJETIVO DE RECUPERACIÓN (RPO)</td><td>TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)</td></tr>
<tr><td>[BIBLS_DTI] Bases de Datos / Servidor Sistema de Biblioteca</td><td rowspan="2">8 horas</td><td rowspan="2">2 días</td></tr>
<tr><td>[BIOMS_DTI] Bases de Datos / Servidor Sistema para control de ingreso de personal</td></tr>
<tr><td colspan="3">ACTIVIDADES DE CONTINGENCIA:</td></tr>
<tr><td colspan="3">1. Para solucionar los problemas ocurridos en los servidores que sostienen al Sistema de Biblioteca, y al Sistema para Control de Personal, debe realizar la activación del servidor alterno que les corresponde.

2. Contactar al personal de biblioteca para que eviten utilizar el Sistema de Biblioteca, o contactar al personal de Recursos Humanos para que eviten utilizar el Sistema para Control de Personal, e indicar que tengan presente la información que han ingresado al sistema en las últimas 12 horas.

3. Desconectar al servidor correspondiente de la red de datos.

4. Respaldar la base de datos.

5. Obtener una imagen de disco del servidor, para análisis de daños.

6. Activar el servidor alterno de producción.

7. Restaurar en el servidor alterno la base de datos del Sistema de Biblioteca o la base de datos del Sistema para Control de Personal con la última actualización respaldada (en caso de no haberse realizado anticipadamente).

8. El servidor alterno debe tener el mismo motor de la base de datos que el servidor principal, pero antes de activar el servicio debe verificar que el motor de la base datos no presente los mismos problemas.

9. Restaurar en el servidor alterno correspondiente, la base de datos del Sistema de Biblioteca o la base de datos del Sistema para Control de Personal, con la</td></tr>
</table>

última actualización respaldada (en caso de no haberse realizado anticipadamente). 10. Restaurar en el servidor alterno, el Sistema de Biblioteca, o el Sistema para Control de Personal con la última versión utilizada en producción (en caso de no haberse realizado anticipadamente). 11. Contactar al proveedor de cada Sistema Informático para que realice su activación en el servidor correspondiente. 12. Cambiar la configuración de conexión en las estaciones de trabajo del personal de Biblioteca o Recursos Humanos, para conectar al servidor alterno (equipo de soporte). 13. Revisar la funcionalidad del sistema informático con los últimos respaldos aplicados en las estaciones de trabajo del personal de Biblioteca o de Recursos Humanos. 14. Revisar los problemas ocurridos con el motor de la base de datos (logs), se recomienda su reinstalación en caso de tener problemas leves, fáciles de reparar. Se recomienda el formateo del disco duro si no se logra a través de las pautas o ayudas del fabricante, la reparación de la base de datos. 15. Registrar una memoria técnica de los problemas encontrados. 16. Realizada la reparación del motor de la base de datos en el servidor principal, se debe realizar el respaldo y activación del servicio fuera del horario normal de trabajo del personal de Biblioteca o de Recursos Humanos.

Elaborado: Ing. Franklin Carrasco

5.8.6. Contingencia: Corte de Energía Eléctrica

Tabla 134: Contingencia: Corte de Energía Eléctrica

CONTINGENCIA: CORTE DE ENERGÍA ELÉCTRICA
EQUIPO RESPONSABLE:
• Dirección de Recursos Físicos • Coordinador de contingencia

<table>
<tr><td colspan="3">• Equipo de Redes
• Equipo de Programación
• Equipo de soporte técnico (logística)</td></tr>
<tr><td colspan="3">AUTORIZA CONTINGENCIA:</td></tr>
<tr><td colspan="3">• Coordinador de contingencia, o
• Director de Tecnologías de la Información, o
• Prorrectorado</td></tr>
<tr><td colspan="3">SITUACIONES CRÍTICAS:</td></tr>
<tr><td colspan="3">• Periodo de Matrículas
• Contabilidad/Adquisiciones/Gestión Tributaria/Facturación/Presupuesto
• Generación de roles</td></tr>
<tr><td colspan="2">DEPARTAMENTOS AFECTADOS:</td><td>SERVICIOS AFECTADOS:</td></tr>
<tr><td colspan="2">• Todos los departamentos</td><td>• Todos los servicios informáticos</td></tr>
<tr><td>ACTIVOS EN RIESGO</td><td>PUNTO OBJETIVO DE RECUPERACIÓN (RPO)</td><td>TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)</td></tr>
<tr><td>[PROD_DTI] Sistemas Informáticos de Producción</td><td rowspan="8">1 hora</td><td rowspan="8">3 horas</td></tr>
<tr><td>[PRODS_DTI] Bases de Datos / Servidor de Producción</td></tr>
<tr><td>[BIBL_DTI] Sistema de Biblioteca</td></tr>
<tr><td>[BIBLS_DTI] Bases de Datos / Servidor Sistema de Biblioteca</td></tr>
<tr><td>[BIOM_DTI] Sistema para control de ingreso de personal</td></tr>
<tr><td>[BIOMS_DTI] Bases de Datos / Servidor Sistema para control de ingreso de personal</td></tr>
<tr><td>[SWITCH_DTI] Switch</td></tr>
<tr><td colspan="3">ACTIVIDADES DE CONTINGENCIA:</td></tr>
<tr><td colspan="3">1. Verificar que el Sistema de Alimentación ininterrumpida (SAI o UPS) esté operando.

2. Verificar que el Generador de Energía se active 30 segundos después de la activación del UPS.

3. En caso de no activarse el generador de energía, proceder con la activación manual del paso de corriente de baterías (UPS) al generador.</td></tr>
</table>

Elaborado: Ing. Franklin Carrasco

4. Revisar los servidores, sistemas informáticos, bases de datos, y sacar respaldos (backups). 5. Energizar los principales sitios de trabajo en los Edificios: - Clara de Asís: unidades de programación y redes - San José: coordinación de secretarias, secretaría general, secretaria de la dirección de formación continua, secretaria de la dirección de posgrados, y direcciones de escuela. - Misereor: dirección de recursos humanos, dirección financiera. 6. Si el corte de energía es mayor a 30 minutos, apagar servidores, y equipos activos tanto en el centro de datos como en los cuartos de control. 7. Contactar al personal administrativo para que eviten utilizar los sistemas informáticos institucionales, e indicar que tengan presente la información que han ingresado al sistema en las últimas 4 horas. 8. Restaurada la energía en el campus universitario, se debe revisar la funcionalidad del sistema y la integridad de la base de datos.

5.8.7. Contingencia: Ausencia Parcial o Permanente del Personal Técnico

Tabla 135: Contingencia: Ausencia Parcial o Permanente del Personal Técnico

CONTINGENCIA: AUSENCIA PARCIAL O PERMANENTE DEL PERSONAL TÉCNICO
EQUIPO RESPONSABLE:
• Dirección de Recursos Humanos • Dirección de Tecnologías de la Información • Prorrectorado • Coordinador de contingencia • Líder equipo de programación
AUTORIZA CONTINGENCIA:
• Coordinador de contingencia, o • Director de Tecnologías de la Información, o • Prorrectorado

<table>
<tr><td colspan="3">SITUACIONES CRÍTICAS:</td></tr>
<tr><td colspan="3">• Periodo de Matrículas
• Contabilidad/Adquisiciones/Gestión Tributaria/Facturación/Presupuesto
• Generación de roles
• Periodo de evaluación institucional</td></tr>
<tr><td colspan="2">DEPARTAMENTOS AFECTADOS:</td><td>SERVICIOS AFECTADOS:</td></tr>
<tr><td colspan="2">• Dirección de Tecnologías de la Información
• Dirección Académica
• Dirección Financiera
• Dirección Recursos Humanos
• Biblioteca</td><td>• Sistema Académico
• Sistema Financiero
• Sistema Nómina
• Sistema de Biblioteca
• Sistema para control de ingreso de personal
• Servicios Web
• Servicio de Internet
• Seguridad de red
• Data Center (Centro de Datos)
• Comunicaciones
• Soporte a usuarios
• Salas de Cómputo</td></tr>
<tr><td>ACTIVOS EN RIESGO</td><td>PUNTO OBJETIVO DE RECUPERACIÓN (RPO)</td><td>TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)</td></tr>
<tr><td>[PROD_DTI] Sistemas Informáticos de Producción</td><td rowspan="12">7 días</td><td rowspan="12">15 días</td></tr>
<tr><td>[PRODS_DTI] Bases de Datos / Servidor de Producción</td></tr>
<tr><td>[BIBL_DTI] Sistema de Biblioteca</td></tr>
<tr><td>[BIBLS_DTI] Bases de Datos / Servidor Sistema de Biblioteca</td></tr>
<tr><td>[BIOM_DTI] Sistema para control de ingreso de personal</td></tr>
<tr><td>[BIOMS_DTI] Bases de Datos / Servidor Sistema para control de ingreso de personal</td></tr>
<tr><td>[Router] Router</td></tr>
<tr><td>[SWITCH_DTI] Switch</td></tr>
<tr><td>[PROXS_DTI] Servidor Proxy/Firewall</td></tr>
<tr><td>[DHCPS_DTI] Servidor DHCP</td></tr>
<tr><td>[CABLE_DTI] Cableado de Datos – Fibra</td></tr>
<tr><td colspan="3">ACTIVIDADES DE CONTINGENCIA:</td></tr>
<tr><td colspan="3"></td></tr>
</table>

Elaborado: Ing. Franklin Carrasco

1. Solicitar a la Dirección de Recursos Humanos y Prorrectorado, en un tiempo máximo de 3 días, la contratación del técnico que reemplazará en funciones al técnico saliente. 2. El técnico saliente debe presentar por escrito las funciones que desempeñó y el trabajo registrado en las unidades de programación o redes en los últimos 12 meses. 3. Incorporado el nuevo trabajador, el técnico saliente debe realizar una capacitación detallada de sus funciones en compañía del técnico o técnicos que se asignaron como respaldo de funciones. 4. El coordinador de contingencia mediante un documento escrito debe solicitar a los técnicos correspondientes, la suspensión de todos los accesos que han sido asignados al técnico saliente, ya sea para sistemas informáticos o servicios de red. 5. El coordinador de contingencia mediante un documento escrito, debe indicar la asignación de las credenciales de acceso para el nuevo técnico, ya sea para sistemas informáticos o servicios de red. 6. Entrenar en entornos de prueba nuevo técnico. 7. Por un tiempo de 15 días se debe asignar a un técnico que acompañe y apoye en las funciones al nuevo técnico.

5.8.8. Contingencia: Incendio Oficinas DTI o Centro de Datos

Tabla 136: Contingencia: Incendio Oficinas DTI o Centro de Datos

CONTINGENCIA: INCENDIO OFICINAS DTI O CENTRO DE DATOS
EQUIPO RESPONSABLE:
• Dirección de Recursos Humanos • Dirección de Tecnologías de la Información • Dirección Financiera • Prorrectorado

<table>
<tr><td colspan="3">• Coordinador de contingencia</td></tr>
<tr><td colspan="3">AUTORIZA CONTINGENCIA:</td></tr>
<tr><td colspan="3">• Coordinador de contingencia, o
• Director de Tecnologías de la Información, o
• Prorrectorado</td></tr>
<tr><td colspan="3">SITUACIONES CRÍTICAS:</td></tr>
<tr><td colspan="3">• Periodo de Matrículas
• Generación de roles
• Periodo normal de clases de grado y posgrado</td></tr>
<tr><td colspan="2">DEPARTAMENTOS AFECTADOS:</td><td>SERVICIOS AFECTADOS:</td></tr>
<tr><td colspan="2">• Dirección de Tecnologías de la Información
• Dirección Académica
• Dirección Financiera
• Dirección Recursos Humanos
• Biblioteca</td><td>• Todos los servicios informáticos</td></tr>
<tr><td>ACTIVOS EN RIESGO</td><td>PUNTO OBJETIVO DE RECUPERACIÓN (RPO)</td><td>TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)</td></tr>
<tr><td>[PRODS_DTI] Servidor de Producción</td><td rowspan="10">2 días</td><td rowspan="10">5 días</td></tr>
<tr><td>[BIBLS_DTI] Servidor Sistema de Biblioteca</td></tr>
<tr><td>[BIOMS_DTI] Servidor Sistema para control de ingreso de personal</td></tr>
<tr><td>[DSKB_DTI] Disco para respaldos de Sistemas Informáticos de Producción</td></tr>
<tr><td>[Router] Router</td></tr>
<tr><td>[SWITCH_DTI] Switch</td></tr>
<tr><td>[PROXS_DTI] Servidor Proxy/Firewall</td></tr>
<tr><td>[DHCPS_DTI] Servidor DHCP</td></tr>
<tr><td>[LAN_DTI] Red LAN</td></tr>
<tr><td colspan="3">ACTIVIDADES DE CONTINGENCIA:</td></tr>
<tr><td colspan="3">1. Verificar que el sistema contra incendios se haya activado en el Centro de Datos.

2. En caso de existir personal técnico dentro del Centro de Datos, solicitar la salida inmediata para evitar daños de salud y esperar hasta que se haya evacuado el gas.</td></tr>
</table>

Elaborado: Ing. Franklin Carrasco

3. Terminada la evacuación del gas, controlado el incendio en el Centro de datos, y si el tiempo lo permite, apagar y retirar los equipos servidores y de comunicación, identificados como críticos. 4. Activar centro de datos alterno y revisar los respaldos externos. 5. Continuar el procedimiento de recuperación de servidores, sistemas informáticos y base de datos indicados en las actividades de contingencia correspondientes. 6. En caso de incendio en las oficinas de DTI, proceder con el manejo de extintores e intentar sofocar el fuego. 7. Si el incendio es considerable no tratar de extinguirlo y llamar a los números de emergencia. 8. Activar el sistema de alarma del edificio. 9. Seguir y respetar la señalética de incendios y rutas de evacuación.

5.8.9. Contingencia: Desastres Naturales – Terremoto

Tabla 137: Contingencia: Desastres Naturales – Terremoto

CONTINGENCIA: DESASTRES NATURALES - TERREMOTO
EQUIPO RESPONSABLE:
• Dirección de Recursos Humanos • Dirección de Tecnologías de la Información • Dirección Financiera • Prorrectorado • Coordinador de contingencia
AUTORIZA CONTINGENCIA:
• Coordinador de contingencia, o • Director de Tecnologías de la Información, o • Prorrectorado
SITUACIONES CRÍTICAS:
• En todo momento

<table>
<tr><td>DEPARTAMENTOS AFECTADOS:</td><td colspan="2">SERVICIOS AFECTADOS:</td></tr>
<tr><td>• Todos los departamentos</td><td colspan="2">• Todos los servicios</td></tr>
<tr><td>ACTIVOS EN RIESGO</td><td>PUNTO OBJETIVO DE RECUPERACIÓN (RPO)</td><td>TIEMPO OBJETIVO DE RECUPERACIÓN (RTO)</td></tr>
<tr><td>[PRODS_DTI] Servidor de Producción</td><td rowspan="10">2 días</td><td rowspan="10">15 días</td></tr>
<tr><td>[BIBLS_DTI] Servidor Sistema de Biblioteca</td></tr>
<tr><td>[BIOMS_DTI] Servidor Sistema para control de ingreso de personal</td></tr>
<tr><td>[DSKB_DTI] Disco para respaldos de Sistemas Informáticos de Producción</td></tr>
<tr><td>[Router] Router</td></tr>
<tr><td>[SWITCH_DTI] Switch</td></tr>
<tr><td>[PROXS_DTI] Servidor Proxy/Firewall</td></tr>
<tr><td>[DHCPS_DTI] Servidor DHCP</td></tr>
<tr><td>[LAN_DTI] Red LAN</td></tr>
<tr><td colspan="3">ACTIVIDADES DE CONTINGENCIA:</td></tr>
<tr><td colspan="3">1. Evacuar los sitios de trabajo y acudir a zonas seguras.

2. Terminado el movimiento sísmico, desactivar toda conexión eléctrica en los edificios y revisar la posibilidad de ingresar al centro de datos principal.

3. En caso de tener un alto nivel de destrucción en la universidad, donde impliquen pérdidas humanas, la primera actividad a realizar es la colaboración por el salvamiento de los compañeros de trabajo.

4. Evaluar daños en los cuartos de comunicación, centro de datos principal y alterno.

5. Si existen daños de infraestructura (edificio) en el centro de datos principal, retirar los servidores y equipos activos.

6. Si existen daños de infraestructura (edificio) en el centro de datos alterno, retirar los servidores y equipos activos de respaldo para ubicarlos en uno de los cuartos de comunicación de los edificios Misereor o San José.

7. En caso de poder habilitar el cuarto de datos alterno, mover los servidores y equipos activos principales a este sitio.

8. Contactar al proveedor de servicios de Internet para la activación del servicio.

9. Activar en mínimos la red LAN de la universidad en sitios como:</td></tr>
</table>

a. Clara de Asís: unidades de programación y redes
b. San José: coordinación de secretarias, secretaría general, secretaria de la dirección de formación continua, secretaria de la dirección de posgrados, y direcciones de escuela.
c. Misereor: dirección de recursos humanos, dirección financiera.

10. Para activar la red LAN se deben revisar los enlaces de fibra redundantes entre edificios, en caso de daños, se realizará una nueva conexión con cable UTP CAT 6A.

11. Los switches de las Salas de Cómputo serán redistribuidos para la activación del servicio en los edificios antes mencionados.

12. Las configuraciones de los equipos activos siniestrados serán obtenidos del disco de almacenamiento de datos local, o a su vez, del servicio de almacenamiento de datos en Internet.

13. Activar servidores y sistemas informáticos en el centro de datos alterno.

14. Revisar el funcionamiento del servidor de producción principal, y extraer un respaldo del sistema informático y su base de datos.

15. Revisar el funcionamiento de los servidores de los sistemas de biblioteca y para el control del personal, y extraer un respaldo de las bases de datos.

16. En caso de presentar daños de hardware en los servidores de los sistemas informáticos y los servidores de los servicios de comunicación, seguir los procedimientos de contingencia indicados para: “Daño físico o lógico en servidor de producción”, y “Daños en equipos activos y medios físicos empleados para la comunicación de datos”.

Elaborado: Ing. Franklin Carrasco

CAPÍTULO 6

CAPACITACIÓN, PRUEBAS Y PLAN DE MANTENIMIENTO

6.1. Capacitación del Plan de Contingencia Informática

El Coordinador del plan de contingencia informática tiene asignada la labor de revisar, evaluar y definir las actividades emergentes en el plan, mediante entrenamiento y simulacro en situaciones críticas, que permitan generar un conocimiento previo (experiencia) entre el personal técnico de la universidad.

La capacitación debe realizarse: cada cuatro meses, cuando se realiza un cambio en la infraestructura tecnológica, o cuando un nuevo técnico se integra a las funciones de la Dirección de Tecnologías de la Información (DTI).

Al ser el plan ejecutado en una institución de educación superior, se han identificado los meses de marzo, julio, y noviembre, como los meses donde se recepta una baja solicitud de trabajo en la DTI, por lo tanto se consideran importantes para realizar la capacitación y el simulacro correspondiente. En cada capacitación se debe realizar una reunión inicial y una reunión de cierre, donde se explique el alcance del plan, la identificación de problemas y las soluciones propuestas. La capacitación no debe durar más de una semana (5 días) y debe organizarse por unidad técnica:

- Programación- 2 días
- Redes – 2 días
- Soporte Técnico – 2 días

En la unidad de Programación se debe dar énfasis al respaldo, recuperación y activación de los servidores, sistemas informáticos y bases de datos de producción, biblioteca y control de ingreso de personal; también se deben evaluar las salvaguardas, además de los controles diarios que aseguren la integridad de los datos, y la disponibilidad del servicio.

En la unidad de Redes, el equipo técnico debe estar preparado para poder establecer una solución inmediata ante fallas en el servicio de comunicación, tomando como criterio principal, la disponibilidad de los equipos activos y servidores para comunicación de datos. El equipo de soporte técnico debe conocer las actividades a realizar como apoyo de los equipos de programación y redes; así también debe revisar las actividades propias de su unidad, como es el servicio de mantenimiento de equipos, y soporte a usuarios.

El coordinador del Plan debe proponer una capacitación dirigida en especial al personal administrativo, para informar cómo proceder ante alguna emergencia; es recomendable emplear el servicio de envío de comunicados que posee la universidad, para mantener informada a la Comunidad Universitaria sobre las amenazas o vulnerabilidades que se exponen los usuarios, y las buenas prácticas con el uso de la tecnología.

En cada capacitación, se debe levantar el acta y registro respectivo del personal técnico o administrativo que ha sido capacitado, evidenciando así la formación y experiencia antes situaciones de riesgo. El formato del Acta de Capacitación se lo presenta en la siguiente tabla:

Tabla 138: Acta de capacitación

PLAN DE CONTINGENCIA INFORMÁTICA
ACTA DE CAPACITACIÓN

Fecha:	**Lugar:**
Duración:	
Capacitación dirigida por:	

Situaciones de riesgo y actividades de Contingencia tratados:

Actividades preventivas / correctivas tratadas:

Conclusiones y Observaciones:

Firma Coordinador de Plan de Contingencia Informática

Fuente: Proyecto Plan de contingencia Informática
Elaborado: Ing. Franklin Carrasco

Tabla 139: Registro de participantes

PLAN DE CONTINGENCIA INFORMÁTICA
REGISTRO DE PARTICIPANTES

Departamento /Unidad	Nombre	Cargo	Correo Electrónico	Firma

Fuente: Proyecto Plan de contingencia Informática
Elaborado: Ing. Franklin Carrasco

6.2. Pruebas del Plan de Contingencia Informática y Análisis de resultados

Durante la aplicación de la propuesta del Plan de contingencia informática en la Dirección de Tecnologías de la Información, se realizaron varias actividades como:

a) La implantación de un servidor de respaldo como contingente para el servidor de producción y sus sistemas informáticos; logrando la

estabilidad de los sistemas informáticos Académico, Financiero y Nómina en un ambiente actualizado.

Durante la etapa de pruebas se corrigieron errores generados en el código fuente del sistema informático, y se normó la creación-suspensión de usuarios.

b) Capacitación de funciones compartidas entre técnicos de la unidad de programación; este contingente ha presentado un resultado positivo, debido a la constante salida e ingreso de técnicos en esta unidad.
c) Construcción, instalación y activación de Centro de Datos principal y Centro de Datos alterno, dejando a este último pendiente de adecuar por las obras civiles que se realizan en el sitio.
d) Contratación de seguro para la reposición y monitoreo de switches y routers CISCO, manteniendo la disponibilidad del servicio ante el reemplazo del equipo cuando se presenten problemas de puertos o su capacidad de trabajo supera el sesenta por ciento de actividad.

Se considera realizar las pruebas del plan de contingencia informática durante los meses de marzo, julio y noviembre al igual que la capacitación del personal técnico de la DTI. Las pruebas también están sujetas a cambios de acuerdo a las soluciones tecnológicas aplicadas, y

las actualizaciones realizadas en el plan de contingencia informática. A continuación se presenta el Cronograma de Pruebas del Pan de Contingencia Informática, al cual se debe sujetar el Coordinador del Plan.

Tabla 140: Cronograma de Pruebas

PLAN DE CONTINGENCIA INFORMÁTICA
CRONOGRAMA DE PRUEBAS

Id	Tarea	Duración
1	Preparación de ambientes de prueba	2 días
2	Capacitación-Entrenamiento del Personal Técnico y administrativo	5 días
3	Preparación de equipos de contingencia	1 día
4	Ejecución de actividades de contingencia en ambientes de prueba	1 día
5	Seguimiento de actividades de contingencia	1 día
6	Análisis de Resultados	1 día
7	Presentación de cambios sobre actividades de contingencia	1 día
8	Verificación funcional de cambios en ambientes de prueba	1 día
9	Actualización de Plan de Contingencia Informática	1 día
10	Realización de Actas	1 día

Fuente: Proyecto Plan de contingencia Informática
Elaborado: Ing. Franklin Carrasco

6.3. Personal responsable de mantenimiento del Plan de Contingencia Informática

Para mantener un control periódico al cumplimiento de las actividades de contingencia, se propone la conformación de la Comisión de Contingencia, cuyos integrantes evaluarán las necesidades y soluciones requeridas para conservar la disponibilidad de los servicios de la universidad en situaciones de emergencia.

La comisión debe estar integrada por el Coordinador del plan, las principales autoridades, directores de los departamentos más críticos de la universidad, y el personal técnico de la Dirección de Tecnologías de la Información. Las actividades asignadas para cada integrante de la comisión responden a la necesidad que tenga la universidad en momentos críticos, como se indica en la tabla 132.

Tabla 141: Comisión para el mantenimiento del Plan de Contingencia Informática

COMISIÓN DE CONTINGENCIA	ACTIVIDAD
Coordinador de Plan de Contingencia - Director(a) de Tecnologías de la Información	Capacitación, supervisión, evaluación, ejecución, y control de las actividades de contingencia, ya sea mediante simulacros o situaciones emergentes.
Prorrectorado Director(a) Financiera Coordinador(a) de Contabilidad/Presupuesto Coordinador(a) de Adquisiciones	Autorizar compras. Contactar a proveedores externos, para la contratación de servicios, o compra de equipos como servidores, switches, y routers.
Director(a) Recursos Humanos	Contratación emergente de personal técnico o administrativo.
Director(a) Recursos Físicos	Recuperación del servicio eléctrico. Reparación de infraestructura (edificios). Identificación de sitios seguros
Técnico Programación 1 - Líder - Equipo de Programación	Recuperar la funcionalidad en los sistemas informáticos, servicios web, y bases de datos que emplea la universidad.
Técnico Redes 1 - Líder - Equipo de Redes	Recuperar el servicio de comunicación de datos en la red LAN y WLAN de la universidad.
Técnico Soporte 1 - Líder - Equipo de Soporte	Activación de sitios alternos para centro de datos, arreglo de computadores asignados al personal administrativo. Apoyo técnico a los equipos de programación y redes.

Fuente: Proyecto Plan de contingencia Informática
Elaborado: Ing. Franklin Carrasco

6.4. Mantenimiento y actualización del Plan de Contingencia Informática

El mantenimiento del plan se realiza mediante la creación de dos grupos de trabajo, que conforman la parte técnica (capacitación-entrenamiento), y la parte administrativa de la universidad (formalidad de procesos).

6.4.1. Reuniones técnicas de capacitación – entrenamiento

Es un conjunto de reuniones conformadas por el personal técnico de la DTI, con la ayuda del coordinador del plan de contingencia informática. Durante el desarrollo de estas reuniones, se realizan simulacros recreando situaciones emergentes, en los cuales se aplican las actividades de contingencia, terminado este entrenamiento, se evalúan los resultados, y se presentan propuestas para mejorar la disponibilidad, además de reducir el tiempo de recuperación de los servicios y sistemas de la universidad.

Las reuniones se realizarán tres veces al año, considerando marzo, julio, y noviembre como los meses preferidos para desarrollar el mantenimiento del plan.

6.4.2. Reuniones formales de mantenimiento y actualización del plan

Tienen la característica de realizarse con los departamentos que conforman la Comisión para el mantenimiento del Plan de Contingencia Informática; su meta es la de revisar y prever de soluciones informáticas, como también de aprobar los cambios propuestos sobre el plan. Se propone realizar esta reunión en los meses de enero, y julio; el Coordinador del plan pondrá a consideración de las autoridades las nuevas soluciones técnicas recogidas de las Reuniones de capacitación-entrenamiento para mejorar la disponibilidad de los servicios y sistemas de la universidad.

6.5. Difusión del Plan de Contingencia Informática

Mediante el uso de los medios de comunicación que posee la universidad, se dará a conocer el Plan de Contingencia Informático. Los medios de difusión a emplear son:

6.5.1. Comunicados Digitales

Mensajes de correo electrónico enviados a la comunidad universitaria, a través de los cuales se informará acerca de las vulnerabilidades o amenazas informáticas que podrían exponerse los docentes y personal administrativo. También se indicará como proceder en caso de ocurrir una emergencia en la universidad, resguardando el bienestar del trabajador y la seguridad de la información.

6.5.2. Campañas de difusión

Mediante la realización de afiches, medios audiovisuales y su respectiva publicación en las redes sociales o carteleras de la universidad, permitirá informar a los estudiantes sobre las medidas preventivas consideradas para evitar la materialización de las amenazas.

6.5.3. Capacitaciones

Dirigidas al personal administrativo que emplea los servicios y sistemas informáticos de la universidad, dando a conocer los procesos o actividades que deben seguir en cada actividad de contingencia. Es importante la realización de esta capacitación, pues concientiza a los usuarios sobre el uso de las tecnologías y fortalece la ejecución del Plan de Contingencia informática.

CONCLUSIONES Y RECOMENDACIONES

CONCLUSIONES

1. Con el Plan de Contingencia Informática se establecieron normas de seguridad y procesos de control que permiten al personal técnico del departamento de tecnología, mantener la disponibilidad de los sistemas y servicios informáticos, además de conocer las amenazas que pueden afectar a los procesos de gestión de la institución.

2. Se identificaron y asignaron actividades de gestión entre el personal técnico de la Dirección de Tecnologías de la Información, y el personal

administrativo con el fin de asegurar la integridad de la información, y evitar situaciones de riesgo en la institución.

3. Al aplicar la metodología Magerit se logró la identificación y clasificación de los principales activos de información de la Sede universitaria, así como las posibles amenazas que serán controladas mediante medidas preventivas, correctivas y de contingencia.

4. En el desarrollo del Plan de Contingencia informático se identificaron las vulnerabilidades que están expuestos los sistemas de información de la Institución, cuyo impacto de daños es contrarrestado mediante la implantación de acciones preventivas, y correctivas ejecutadas por el personal técnico de TI.

5. Con la implantación del Plan de Contingencia Informática se estableció un equipo interdisciplinario comprometido con asegurar la continuidad de las actividades de gestión, y la disponibilidad de los sistemas y servicios informáticos, además de fomentar el cumplimiento de las acciones preventivas, correctivas y actividades de contingencia entre el personal técnico, administrativo y de servicios.

RECOMENDACIONES

1. Capacitar al personal técnico del departamento de TI en temas relacionados a seguridad informática, además de implantar y hacer cumplir las actividades preventivas, correctivas y de contingencia presentadas en el Plan.

2. La institución debe crear el manual de funciones del personal administrativo y de servicios, en apoyo de los jefes departamentales, y ser socializado entre los trabajadores para asegurar la asignación de actividades y responsabilidades.

3. Institucionalizar la metodología Magerit para mantener un análisis de riesgos que permita la identificación de los principales activos de información, fortaleciendo la disponibilidad de servidores y equipos activos de comunicación.

4. Actualizar la infraestructura tecnológica en entornos de producción y contingencia, para fortalecer la disponibilidad de los servicios y sistemas informáticos, así como la información que sostienen, permitiendo la ejecución de las prácticas de seguridad presentadas en el Plan de Contingencia.

5. Actualizar periódicamente el Plan de Contingencia Informático, para identificar riesgos o necesidades técnicas que puedan afectar a los principales procesos de gestión, dentro de un marco de trabajo interdisciplinario establecido por una comisión o un departamento de seguridad de la información.

GLOSARIO

Ataque informático: intento deliberante e intencionado realizado por una o varias personas para causar daños o problemas a un sistema informático o de red.

Autenticidad: reconocimiento autorizado de un usuario al acceder a un sistema informático.

Catálogo: Lista ordenada y clasificada de personas u objetos.

Cliente (informática): computador o aplicación que consume recursos de un servicio remoto denominado servidor.

Confidencialidad: propiedad de la información, por la que se garantiza que está accesible únicamente al personal autorizado.

Continuidad: cualidad de no ser interrumpido, en la informática la idea de continuidad se asocia al funcionamiento del software y hardware informático que soportan las empresas.

Degradación: en el lenguaje informático se conoce como la pérdida de señal o de capacidades de procesamiento de información.

Dirección IP: es una etiqueta numérica que identifica de manera lógica y jerárquica a la interfaz de red de un computador en una red de datos; las siglas IP es un acrónimo para Internet Protocol.

Equipo activos de acceso: equipos de red, empleado para la conexión de los usuarios a la red de datos o Internet.

Equipo activos de distribución: equipos activos de red, empleados para interconectar múltiples sitios en una organización; conectan a los equipos de núcleo con los equipos de acceso.

Equipo activos de núcleo: equipos de red, empleados para interconectar a las empresas con la red de Internet; es la “columna vertebral” de la red de datos de una institución.

Gestionar: acción de dirigir y administrar un negocio o empresa.

Gobierno de TI: es el alineamiento de las Tecnologías de la Información con la estrategia del negocio, movilizando los recursos tecnológicos de forma eficiente en respuesta a requisitos operativos del negocio.

IDS: del inglés Intrusion Detection System (Sistema de Detección de Intrusos), es un software que inspecciona las actividades de acceso no autorizado a una red o a un computador.

IPS: del inglés Intrusion Prevention System (Sistema de Prevención de Intrusos), es un software que controla el acceso no autorizado a una red o a un computador.

Integridad: en lenguaje informático se define en mantener la estructura original de la información tal como se envió desde su origen hasta su destino.

Interrupción: sus pensión temporal de la ejecución de un proceso.

Magerit: metodología de análisis y gestión de riesgos elaborada por el Consejo Superior de Administración Electrónica de España, ofrece un método sistemático para analizar los riesgos derivados del uso de tecnologías de la

información y comunicaciones para de esta forma implementar las medidas de control más adecuadas que permitan tener los riesgos mitigados.

Recursos Informáticos: componentes de hardware y software empleados para la optimización de las actividades del negocio.

Riesgo: es la probabilidad de que una amenaza se materialice, utilizando las vulnerabilidades existentes de un activo o grupos de activos, generándoles pérdidas o daños.

Salvaguardas: actividades que reducen el impacto o degradación que puedan causar los riesgos ante la materialización de una amenaza.

Sistemas de Información: son aquellos elementos empleados para el tratamiento y administración de datos e información, se clasifican en personas, datos, actividades o técnicas de trabajo y recursos materiales (informáticos y de comunicación).

Trazabilidad: reconocimiento de las actividades que realiza un usuario en un sistema informático u ordenador.

ANEXOS

ANEXO 1. Carta de Aprobación para desarrollo de Plan de Contingencia Informática en la Pontificia Universidad Católica del Ecuador Sede Santo Domingo

Pontificia Universidad Católica del Ecuador Sede Santo Domingo

Santo Domingo, 10 de diciembre del 2013
PR-382-2013

Ingeniero
Franklin Carrasco Ramírez
Ciudad

De mi consideración:

Enterada de su carta del 29 de noviembre de este año, en la que manifiesta que ha egresado en la Maestría "Seguridad Informática Aplicada" cursada en la Escuela Politécnica del Litoral; y con el fin de obtener su título de cuarto nivel, desarrollará el Proyecto de Tesis denominada: "Desarrollar e implantar actividades de corto plazo del Plan de Contingencia Informática para la Dirección de Tecnologías de la Información de la Pontificia Universidad Católica del Ecuador Sede Santo Domingo", para lo que requiere la debida autorización.

Le doy a conocer que esta Sede no dispone del trabajo a desarrollarse, y al ser un proyecto que permitirá la solución preventiva y correctiva ante riesgos informáticos que pueden incidir en los procesos de gestión de la Universidad, se autoriza que se proporcione la información necesaria para el desarrollo de la tesis en mención.

Sin otro particular, me suscribo.

Atentamente,

Margalida Font Roig, Ph.D.
Prorrectora

PRORRECTORADO

MFR/Mllc
Cc: Director de Tecnologías de la Información

ANEXO 2. Acuerdo de Confidencialidad

ACUERDO DE CONFIDENCIALIDAD

Entre la Pontificia Universidad Católica del Ecuador Sede Santo Domingo, representada en este acto por Dra. Margalida Font Roig, en calidad de Prorrectora, en adelante PUCESD, por una parte y por la otra parte, el señor Franklin Andrés Carrasco Ramírez a quien también se lo podrá denominar como TESISTA DE POS GRADO, en lo sucesivo se denominarán en forma conjunta e indistinta LAS PARTES, quienes declaran:

a) Que mediante solicitud dirigida a la Dra. Margalida Font Roig, Prorrectora de la PUCESD, con fecha 31 de octubre de 2014, el señor Franklin Andrés Carrasco Ramírez solicitó se le permita realizar en la PUCESD el proyecto de tesis de posgrado denominada "Desarrollar e Implantar actividades de Corto Plazo del Plan de Contingencia Informática para a Dirección de Tecnologías de la Información de la Pontificia Universidad Católica del Ecuador Sede Santo Domingo", para lo cual necesita acceder a la siguiente información:

   - Diagrama de red de la Topología Física de la red LAN.
   - Esquema de la Topología Lógica en la red LAN.
   - Inventario de equipos activos para comunicación de red, agrupados por edificios.
   - Inventario de servidores físicos.
   - Inventario de Access Points.

b) Que con fecha 31 de octubre de 2014, la Dra. Margalida Font Roig aprobó la solicitud presentada por el señor Franklin Andrés Carrasco Ramírez autorizándole para que acceda a la información solicitada en el literal anterior, con la única y exclusiva finalidad de elaborar su tesis de posgrado denominada "Desarrollar e Implantar actividades de Corto Plazo del Plan de Contingencia Informática para a Dirección de Tecnologías de la Información de la Pontificia Universidad Católica del Ecuador Sede Santo Domingo", por un plazo improrrogable de SEIS MESES, contados a partir de la suscripción del presente documento.

En atención a las declaraciones expuestas, LAS PARTES acuerdan:

Primero. Obligaciones:

- Que el TESISTA DE POSGRADO, utilizará la información que le ha sido proporcionada ÚNICA y EXCLUSIVAMENTE para la realización de su tesis denominada "Desarrollar e Implantar actividades de Corto Plazo del Plan de Contingencia Informática para a Dirección de Tecnologías de la Información de la Pontificia Universidad Católica del Ecuador Sede Santo Domingo".

- EL TESISTA DE POSGRADO se obliga en forma irrevocable ante LA PUCESD a no revelar, divulgar o facilitar -bajo cualquier forma- a ninguna persona física o jurídica, sea esta pública o privada, o para beneficio de cualquier otra persona física o jurídica, pública o privada, la información recibida así como así también las políticas y/o cualquier otra información de LA PUCESD.

- EL TESISTA DE POSGRADO se compromete a no hacer constar en su tesis direcciones IP reales, claves de acceso reales, configuraciones reales de equipos activos; para suplir esta información, en el texto de su tesis deberá hacer constar datos simulados o semejantes, los cuales no permitan un fácil reconocimiento de los reales.

- El TESISTA DE POSGRADO se obliga a entregar a Prorrectorado, previo a la disertación un ejemplar de su tesis de grado debidamente aprobada por la Institución de Educación Superior en la cual cursó sus estudios.

- EL TESISTA DE POSGRADO asume la obligación de confidencialidad acordada por todo el plazo de acceso a la información y por un plazo adicional de 5 años contados a partir de la terminación de su tesis de grado.

Segundo. Causales de terminación de autorización.

La autorización para el acceso a la información solicitada por el TESISTA DE POSGRADO, terminará:

- Cuando el TESISTA POSTULANTE incumpla una de las obligaciones consignadas en el numeral primero del presente documento.

- La violación o el incumplimiento de la obligación de confidencialidad a cargo del TESISTA DE POSGRADO, dará derecho a la PUCESD a iniciar las acciones civiles y penales que correspondan, para lo cual las partes renuncian a domicilio y expresamente se someten a los señores Jueces de la ciudad de Santo Domingo, provincia de Santo Domingo de los Tsáchilas y al trámite elegido por el demandante.

Para constancia de lo acordado, firman los intervinientes el presente documento en unidad de acto y en tres ejemplares de igual valor y tenor en Santo Domingo, 4 de noviembre de 2014.

Margalida Font Roig, PhD.
PRORRECTORA PUCESD

Ing. Franklin Carrasco
TESISTA DE POSGRADO

PRORRECTORADO

ANEXO 3. Levantamiento de Información

a) [IS] Servicios Internos

[S] Servicios	
código: INTER_DTI	nombre: Internet
descripción:	Servicio de Internet
Responsable del llenado:	Franklin Carrasco
Fecha de llenado:	6 de octubre 2014
responsable:	Técnico Redes 1 - Líder
Tipo	
( )	[anon] anónimos (sin requerir identificación del usuario)
( )	[pub] al público en general (sin relación contractual)
( )	[ext] a usuarios externos (bajo una relación contractual)
( )	[int] interno (usuarios y medios de la propia organización)
( )	[cont] contrato a terceros (se presta con medios ajenos)
(X)	[www] world wide web
( )	[telnet] acceso remoto a cuenta local
( )	[email] correo electrónico
( )	[ftp] transferencia de ficheros
( )	[edi] intercambio electrónico de datos
( )	[dir] servicio de directorio
( )	[idm] gestión de identidades
( )	[ipm] gestión de privilegios
( )	[pki] PKI - infraestructura de clave pública

[S] Servicios	
código: WEBS_DTI	nombre: Portal Web PUCESD
descripción:	Engloba un conjunto de servicios como: informativo, revisión de calificaciones, evaluación a profesores
Responsable del llenado:	Franklin Carrasco

Fecha de llenado:	6 de octubre 2014
responsable:	Técnico Redes 1 - Líder
tipo	
( )	[anon] anónimos (sin requerir identificación del usuario)
( )	[pub] al público en general (sin relación contractual)
( )	[ext] a usuarios externos (bajo una relación contractual)
(X)	[int] interno (usuarios y medios de la propia organización)
( )	[cont] contrato a terceros (se presta con medios ajenos)
(X)	[www] world wide web
( )	[telnet] acceso remoto a cuenta local
( )	[email] correo electrónico
( )	[ftp] transferencia de ficheros
( )	[edi] intercambio electrónico de datos
( )	[dir] servicio de directorio
( )	[idm] gestión de identidades
( )	[ipm] gestión de privilegios
( )	[pki] PKI - infraestructura de clave pública

[S] Servicios	
código: EMAIL_DTI	nombre: Servicio Correo Electrónico Gmail
descripción:	Servicio de comunicación interna y escrita de la Sede
Responsable del llenado:	Franklin Carrasco
Fecha de llenado:	6 de octubre 2014
responsable:	Técnico Redes 1 - Líder
tipo	
( )	[anon] anónimos (sin requerir identificación del usuario)
( )	[pub] al público en general (sin relación contractual)
( )	[ext] a usuarios externos (bajo una relación contractual)
(X)	[int] interno (usuarios y medios de la propia organización)
( )	[cont] contrato a terceros (se presta con medios ajenos)
(X)	[www] world wide web

( )	[telnet] acceso remoto a cuenta local
( )	[email] correo electrónico
( )	[ftp] transferencia de ficheros
( )	[edi] intercambio electrónico de datos
( )	[dir] servicio de directorio
( )	[idm] gestión de identidades
( )	[ipm] gestión de privilegios
( )	[pki] PKI - infraestructura de clave pública

[S] Servicios	
código: FILE_DTI	nombre: Almacenamiento de Archivos
descripción :	Almacenamiento en archivos digitales en la nube a través del servicio Drive y Servidor de archivos
Responsable del llenado:	Franklin Carrasco
Fecha de llenado:	6 de octubre 2014
responsable:	Técnico Redes 1 - Líder

tipo	
( )	[anon] anónimos (sin requerir identificación del usuario)
( )	[pub] al público en general (sin relación contractual)
( )	[ext] a usuarios externos (bajo una relación contractual)
(X)	[int] interno (usuarios y medios de la propia organización)
( )	[cont] contrato a terceros (se presta con medios ajenos)
(X)	[www] world wide web
( )	[telnet] acceso remoto a cuenta local
( )	[email] correo electrónico
( )	[ftp] transferencia de ficheros
( )	[edi] intercambio electrónico de datos
( )	[dir] servicio de directorio
( )	[idm] gestión de identidades
( )	[ipm] gestión de privilegios
( )	[pki] PKI - infraestructura de clave pública

b) [E] Equipamiento - [D]Datos

[D] Datos / Información		
código: BDD_PROD_DTI		nombre: Bases de datos de Producción
descripción:	Es la Base de Datos de los sistemas informático de producción: Académico, HIPERK, y Nómina	
Responsable del llenado:	Franklin Carrasco	
Fecha de llenado:	6 de octubre 2014	
propietario:	PUCESD	
responsable:	Técnico Programación 1 - Líder	
tipo		
(X)	[vr] datos vitales (registros de la organización)	
(X)	[com] datos de interés comercial	
(X)	[adm] datos de interés para la administración pública	
(X)	[int] datos de gestión interna	
( )	[source] código fuente	
( )	[exe] código ejecutable	
( )	[conf] datos de configuración	
( )	[log] registro de actividad (log)	
( )	[test] datos de prueba	
(X)	[per] datos de carácter personal	
	(X)	[A] de nivel alto
	( )	[M] de nivel medio
	( )	[B] de nivel bajo
(X)	[label] datos clasificados	
	(X)	[S] secreto
	(X)	[R] reservado
	(X)	[C] confidencial
	(X)	[DL] difusión limitada
	( )	[SC] sin clasificar
Valoración		
dimensión	valor	justificación
[I]	9	La mala manipulación de los datos puede afectar en los procesos de la Sede

[C]	9	Soporta toda la información de la Sede
[A_D]	9	Es necesario definir niveles de acceso de acuerdo al rol del trabajador
[T_D]	9	Es necesario saber que realiza el usuario con la información

Dependencias de activos inferiores (hijos)	
activo: [PRODS_DTI] Servidor de Producción	grado:
¿Por qué?	
Se aloja la Base de datos en el servidor	
activo: [ADMP_DTI] Administradores de Sistemas informáticos - Programadores	grado:
¿Por qué?	
Los técnicos administran la base de datos	
activo: Directores , técnicas y secretarias	grado:
¿Por qué?	
Administran los datos de los sistemas financiero y académico	

[D] Datos / Información		
código: BDD_PWEB_DTI	nombre:	Bases de Datos de los servicios del Portal Web
descripción:	Es la Base de Datos del Portal Web PUCESD y servicios web para revisión de notas y heteroevaluación docente	
Responsable del llenado:	Franklin Carrasco	
Fecha de llenado:	6 de octubre 2014	
propietario:	Comunicación Virtual	
responsable:	Técnico Programación 1 - Líder	
tipo		
( )	[vr] datos vitales (registros de la organización)	
( )	[com] datos de interés comercial	
(X)	[adm] datos de interés para la administración pública	
(X)	[int] datos de gestión interna	
( )	[source] código fuente	
( )	[exe] código ejecutable	

( )	[conf] datos de configuración	
( )	[log] registro de actividad (log)	
( )	[test] datos de prueba	
(X)	[per] datos de carácter personal	
	( )	[A] de nivel alto
	(X)	[M] de nivel medio
	( )	[B] de nivel bajo
(X)	[label] datos clasificados	
	(X)	[S] secreto
	(X)	[R] reservado
	( )	[C] confidencial
	( )	[DL] difusión limitada
	( )	[SC] sin clasificar

Valoración		
dimensión	valor	justificación
[I]	6	Información empleada para servicios
[C]	4	mayor parte de información es presentada en el portal y servicios web
[A_D]	3	el acceso a los datos se realiza a través del portal web
[T_D]	3	el acceso a los datos se realiza a través del portal web

Dependencias de activos inferiores (hijos)	
activo: [PWEBS_DTI] Servidor Portal Web	grado:
¿Por qué?	
Se aloja la Base de datos en el servidor	
activo: [ADMP_DTI] Administradores de Sistemas informáticos - Programadores	grado:
¿Por qué?	
Los técnicos administran la base de datos	

[D] Datos / Información		
código: BDD_BIBL_DTI		nombre: Bases de Datos del Sistema de Biblioteca
descripción:	Es la Base de Datos del sistema de biblioteca	
Responsable del llenado:	Franklin Carrasco	
Fecha de llenado:	6 de octubre 2014	
propietario:	Biblioteca	
responsable:	Técnico Programación 2	
tipo		
( )	[vr] datos vitales (registros de la organización)	
( )	[com] datos de interés comercial	
(X)	[adm] datos de interés para la administración pública	
(X)	[int] datos de gestión interna	
( )	[source] código fuente	
( )	[exe] código ejecutable	
( )	[conf] datos de configuración	
( )	[log] registro de actividad (log)	
( )	[test] datos de prueba	
( )	[per] datos de carácter personal	
	( )	[A] de nivel alto
	( )	[M] de nivel medio
	( )	[B] de nivel bajo
( )	[label] datos clasificados	
	( )	[S] secreto
	( )	[R] reservado
	( )	[C] confidencial
	( )	[DL] difusión limitada
	( )	[SC] sin clasificar

Valoración		
dimensión	valor	justificación
[I]	6	La información es requerida para informes y búsqueda de material bibliográfico
[C]	0	La información es de uso público
[A_D]	1	Los usuarios acceden a los datos desde estaciones de búsqueda de libros
[T_D]	3	Sólo las bibliotecarias pueden manipular la información

Dependencias de activos inferiores (hijos)	
activo: [BIBLS_DTI] Servidor Sistema de Biblioteca	grado:
¿Por qué?	
Se aloja la Base de datos en el servidor	
activo: [ADMP_DTI] Administradores de Sistemas informáticos - Programadores	grado:
¿Por qué?	
Los técnicos administran la base de datos	
activo: Bibliotecarios	grado:
¿Por qué?	
Manejan los datos para la administración del material bibliográfico	

[D] Datos / Información		
código: BDD_PROF_DTI	nombre:	Base de datos de sistema administrador de personal docente
descripción:	Es la Base de Datos del sistema para registro de profesores	
Responsable del llenado:	Franklin Carrasco	
Fecha de llenado:	6 de octubre 2014	
propietario:	Recursos Humanos	
responsable:	Técnico Programación 2	
tipo		
( )	[vr] datos vitales (registros de la organización)	
( )	[com] datos de interés comercial	
(X)	[adm] datos de interés para la administración pública	
(X)	[int] datos de gestión interna	
( )	[source] código fuente	
( )	[exe] código ejecutable	
( )	[conf] datos de configuración	
( )	[log] registro de actividad (log)	
( )	[test] datos de prueba	
(X)	[per] datos de carácter personal	
	( ) [A] de nivel alto	
	(X) [M] de nivel medio	
	( ) [B] de nivel bajo	
(X)	[label] datos clasificados	

	( )	[S] secreto
	(X)	[R] reservado
	(X)	[C] confidencial
	( )	[DL] difusión limitada
	( )	[SC] sin clasificar
Valoración		
dimensión	valor	justificación
[I]	6	Los datos no deben presentar errores
[C]	7	La información es sólo para uso del departamento
[A_D]	6	Sólo las técnico de recursos humanos deben ingresar a los datos
[T_D]	7	Se debe saber que acciones realizan las técnico de recursos humanos
Dependencias de activos inferiores (hijos)		
activo: [PROFS_DTI] Servidor Sistema administrador de personal docente		grado:
¿Por qué?		
Posee la Base de datos de sistema		
activo: [ADMP_DTI] Administradores de Sistemas informáticos - Programadores		grado:
¿Por qué?		
Los técnicos administran la base de datos		
activo: Dirección de Recursos Humanos		grado:
¿Por qué?		
Manejan los datos para la administración del personal docente		

[D] Datos / Información		
código: BDD_BIOM_DTI	nombre:	Base de datos del sistema para control de ingreso de personal
descripción:	Base de Datos del sistemas para control de asistencia del personal administrativo y docente de la Sede	
Responsable del llenado:	Franklin Carrasco	
Fecha de llenado:	6 de octubre 2014	
propietario:	Recursos Humanos	
responsable:	Técnico Programación 3	

tipo

( ) [vr] datos vitales (registros de la organización)

( ) [com] datos de interés comercial

(X) [adm] datos de interés para la administración pública

(X) [int] datos de gestión interna

( ) [source] código fuente

( ) [exe] código ejecutable

( ) [conf] datos de configuración

( ) [log] registro de actividad (log)

( ) [test] datos de prueba

(X) [per] datos de carácter personal

- ( ) [A] de nivel alto
- (X) [M] de nivel medio
- ( ) [B] de nivel bajo

(X) [label] datos clasificados

- ( ) [S] secreto
- (X) [R] reservado
- ( ) [C] confidencial
- ( ) [DL] difusión limitada
- ( ) [SC] sin clasificar

Valoración		
dimensión	valor	justificación
[I]	6	Los datos no deben ser manipulados por los técnicos de la Sede
[C]	3	La información es sólo para uso del departamento
[A_D]	5	Sólo las técnico de recursos humanos deben ingresar a los datos

[T_D]	5	Se debe saber que acciones realizan las técnico de recursos humanos
Dependencias de activos inferiores (hijos)		
activo: [BIOMS_DTI] Servidor Sistema para control de ingreso de personal		grado:
¿Por qué?		
Posee la Base de datos de sistema		
activo: [ADMP_DTI] Administradores de Sistemas informáticos - Programadores		grado:
¿Por qué?		
Los técnicos administran la base de datos		
activo: Dirección de Recursos Humanos		grado:
¿Por qué?		
Manejan los datos para la administración del personal administrativo y docente		

c) [E] Equipamiento - [SW]Servicios Internos

[SW] Aplicaciones (software)		
código: PROD_DTI	nombre:	Sistemas Informáticos de Producción
descripción:	El sistema Informático de Producción se compone de los sistemas Informáticos Académico, HIPERK, y Nómina	
Responsable del llenado:	Franklin Carrasco	
Fecha de llenado:	6 de octubre 2014	
responsable:	Técnico Programación 1 - Líder	
Tipo		
(X)	[prp] desarrollo propio (in house)	
( )	[sub] desarrollo a medida (subcontratado)	
( )	[std] standard (off the shelf)	
	( )	[browser] navegador web
	( )	[www] servidor de presentación
	( )	[email_client] cliente de correo electrónico
	( )	[app] servidor de aplicaciones

	( )	[file] servidor de ficheros
	( )	[dbms] sistema de gestión de base de datos
	( )	[tm] monitor transaccional
	( )	[office] ofimática
	( )	[av] anti virus
	( )	[backup] sistema de backup
	( )	[os] sistema operativo
Valoración		
dimensión	valor	justificación
[I]	9	Un cambio mal aplicado en el software puede afectar en los procesos de la Sede
[C]	9	Los códigos fuentes y variables de los sistemas deben estar ocultos a los usuarios
[A_D]	9	Es necesario definir los técnicos y usuarios que acceden al sistema para evidenciar sus acciones
[T_D]	9	Es necesario definir los técnicos y usuarios que acceden al sistema para evidenciar sus acciones
Dependencias de activos inferiores (hijos)		
activo: [PRODS_DTI] Servidor de Producción		grado:
¿Por qué?		
Los sistemas informáticos están instalados en el servidor		
activo: [ADMP_DTI] Administradores de Sistemas informáticos - Programadores		grado:
¿Por qué?		
Los técnicos administran y mantienen en funcionamiento a los sistemas de producción		
activo: Directores , técnicas y secretarias		grado:
¿Por qué?		
Emplean los sistemas para los procesos financiero y académico de la Sede		

[SW] Aplicaciones (software)		
código: PWEB_DTI	**nombre:** Servicios Portal Web	
descripción :	Servicios basados en la Web, como portales Web, y servicios para revisión de notas y heteroevaluación docente	
Responsable del llenado:	Franklin Carrasco	
Fecha de llenado:	6 de octubre 2014	
responsable:	Técnico Programación 3	
Tipo		
(X)	[prp] desarrollo propio (in house)	
( )	[sub] desarrollo a medida (subcontratado)	
( )	[std] standard (off the shelf)	
( )	[browser] navegador web	
( )	[www] servidor de presentación	
( )	[email_client] cliente de correo electrónico	
( )	[app] servidor de aplicaciones	
( )	[file] servidor de ficheros	
( )	[dbms] sistema de gestión de base de datos	
( )	[tm] monitor transaccional	
( )	[office] ofimática	
( )	[av] anti virus	
( )	[backup] sistema de backup	
( )	[os] sistema operativo	

Valoración		
dimensión	valor	justificación
[I]	6	servicio utilizado por la comunidad universitaria
[C]	4	el servicio es de acceso para estudiantes
[A_D]	3	el servicio debe estar siempre disponible para todos los usuarios
[T_D]	3	el servicio debe estar siempre disponible para todos los usuarios

Dependencias de activos inferiores (hijos)	
activo: [PWEBS_DTI] Servidor Portal Web	grado:
¿Por qué?	
Aloja el portal y los servicios web	
activo: [INTERNET_DTI] Servicio de Internet	grado:
¿Por qué?	

Permite el acceso de los usuarios a los servicios web	
activo: [ADMP_DTI] Administradores de Sistemas informáticos - Programadores	grado:
¿Por qué?	
Realizan las modificaciones sobre el código del servicio web	
activo: Usuarios de servicios web	grado:
¿Por qué?	
Emplean el servicio para la revisión de notas, evaluar docente y recibir información de la Sede	

[SW] Aplicaciones (software)		
código: BIBL_DTI	nombre:	Sistema de Biblioteca
descripción:	Sistema de biblioteca de la PUCESD	
Responsable del llenado:	Franklin Carrasco	
Fecha de llenado:	6 de octubre 2014	
responsable:	Técnico Programación 2	
tipo		
( )	[prp] desarrollo propio (in house)	
(X)	[sub] desarrollo a medida (subcontratado)	
( )	[std] standard (off the shelf)	
	( )	[browser] navegador web
	( )	[www] servidor de presentación
	( )	[email_client] cliente de correo electrónico
	( )	[app] servidor de aplicaciones
	( )	[file] servidor de ficheros
	( )	[dbms] sistema de gestión de base de datos
	( )	[tm] monitor transaccional
	( )	[office] ofimática
	( )	[av] anti virus
	( )	[backup] sistema de backup
	( )	[os] sistema operativo

Valoración		
dimensión	valor	justificación
[I]	6	No se poseen códigos fuente del programa
[C]	0	El programa es utilizado por los usuarios de la biblioteca y bibliotecarios
[A_D]	1	El software es administrado sólo por los bibliotecarios
[T_D]	3	El software es administrado sólo por los bibliotecarios
Dependencias de activos inferiores (hijos)		
activo: [BIBLS_DTI] Servidor Sistema de Biblioteca		grado:
¿Por qué?		
Ejecuta y aloja el sistema de biblioteca		
activo: [ADMP_DTI] Administradores de Sistemas informáticos - Programadores		grado:
¿Por qué?		
Los técnicos de TI administran el software		
activo: Bibliotecarios		grado:
¿Por qué?		
Emplean el software para la administración del material bibliográfico		

[SW] Aplicaciones (software)		
código: PROF_DTI	nombre:	Sistema administrador de personal docente
descripción:	Sistema Informático empleado por la Dirección de Recursos Humanos para el registro y seguimiento de los profesores de la Sede	
Responsable del llenado:	Franklin Carrasco	
Fecha de llenado:	6 de octubre 2014	
responsable:	Técnico Programación 2	
tipo (X) [prp] desarrollo propio (in house) ( ) [sub] desarrollo a medida (subcontratado) ( ) [std] standard (off the shelf) ( ) [browser] navegador web		

	( )	[www] servidor de presentación
	( )	[email_client] cliente de correo electrónico
	( )	[app] servidor de aplicaciones
	( )	[file] servidor de ficheros
	( )	[dbms] sistema de gestión de base de datos
	( )	[tm] monitor transaccional
	( )	[office] ofimática
	( )	[av] anti virus
	( )	[backup] sistema de backup
	( )	[os] sistema operativo
Valoración		
dimensión	valor	justificación
[I]	6	El software no debe presentar errores en sus procesos
[C]	7	El software sólo debe ser usado por la técnica asignada
[A_D]	6	Se debe reconocer al usuario que ingresa al sistema para evidenciar sus acciones
[T_D]	7	Se debe reconocer al usuario que ingresa al sistema para evidenciar sus acciones
Dependencias de activos inferiores (hijos)		
activo: [PROFS_DTI] Servidor Sistema administrador de personal docente		grado:
¿Por qué?		
Posee instalado el sistema informático		
activo: [ADMP_DTI] Administradores de Sistemas informáticos - Programadores		grado:
¿Por qué?		
Los técnicos de TI administran el software y el código fuente		
activo: Dirección de Recursos Humanos		grado:
¿Por qué?		
Emplean el software para la administración del personal docente		

[SW] Aplicaciones (software)		
código: BIOM_DTI	nombre:	Sistema para control de ingreso de personal
descripción:	Sistema Informático adquirido por la Sede para para registrar y controlar el ingreso/salida y permisos del personal administrativo, y docente de planta	
Responsable del llenado:	Franklin Carrasco	
Fecha de llenado:	6 de octubre 2014	
responsable:	Técnico Programación 3	
tipo		
( )	[prp] desarrollo propio (in house)	
(X)	[sub] desarrollo a medida (subcontratado)	
( )	[std] standard (off the shelf)	
	( )	[browser] navegador web
	( )	[www] servidor de presentación
	( )	[email_client] cliente de correo electrónico
	( )	[app] servidor de aplicaciones
	( )	[file] servidor de ficheros
	( )	[dbms] sistema de gestión de base de datos
	( )	[tm] monitor transaccional
	( )	[office] ofimática
	( )	[av] anti virus
	( )	[backup] sistema de backup
	( )	[os] sistema operativo

Valoración		
dimensión	valor	justificación
[I]	6	El software no debe presentar errores en sus procesos
[C]	3	El equipo debe ser de conocimiento únicamente del personal técnico de TI
[A_D]	5	Se debe reconocer al usuario que ingresa al sistema para evidenciar sus acciones
[T_D]	5	Se debe reconocer al usuario que ingresa al sistema para evidenciar sus acciones

Dependencias de activos inferiores (hijos)	
activo: [BIOMS_DTI] Servidor Sistema para control de ingreso de personal	grado:
¿Por qué?	

El programa se ejecuta y aloja en el servidor	
activo: [ADMP_DTI] Administradores de Sistemas informáticos - Programadores	grado:
¿Por qué?	
Los técnicos de TI administran el software	
activo: Dirección de Recursos Humanos	grado:
¿Por qué?	
Emplean el software para la administración del personal administrativo y docente	

[SW] Aplicaciones (software)		
código: FILEBA_DTI	**nombre:** Software para respaldo de archivos	
descripción:	Software utilizado para la creación de espacios de almacenamiento para los usuarios con el convenio de portátiles	
Responsable del llenado:	Franklin Carrasco	
Fecha de llenado:	6 de octubre 2014	
responsable:	Técnico Redes 1 - Líder	
tipo		
( )	[prp] desarrollo propio (in house)	
( )	[sub] desarrollo a medida (subcontratado)	
(X)	[std] standard (off the shelf)	
	( )	[browser] navegador web
	( )	[www] servidor de presentación
	( )	[email_client] cliente de correo electrónico
	( )	[app] servidor de aplicaciones
	( )	[file] servidor de ficheros
	( )	[dbms] sistema de gestión de base de datos
	( )	[tm] monitor transaccional
	( )	[office] ofimática
	( )	[av] anti virus
	(X)	[backup] sistema de backup
	( )	[os] sistema operativo

Valoración		
dimensión	valor	justificación
[I]		La información debe ser custodiada por el usuario propietario
[C]	3	El acceso a los archivos es único para cada usuario
[A_D]	9	Se debe identificar al usuario que ingresa al sistema de archivos
[T_D]	7	Se debe conocer las actividades que ha realizado el usuario

Dependencias de activos inferiores (hijos)	
activo: [REDES_DTI] Administradores de infraestructura y telecomunicaciones	grado:
¿Por qué?	
Los técnicos que monitorean el funcionamiento de los servidores	
activo: Usuarios	grado:
¿Por qué?	
Utilizan el software como interfaz para almacenar los archivos	

[SW] Aplicaciones (software)	
código: OFFI_DTI	**nombre:** Office - Ofimática
descripción:	Licencias Microsoft Office 2010 empleadas para la gestión administrativa y académica
Responsable del llenado:	Franklin Carrasco
Fecha de llenado:	6 de octubre 2014
responsable:	Técnico Redes 2
tipo ( ) [prp] desarrollo propio (in house) ( ) [sub] desarrollo a medida (subcontratado) (X) [std] standard (off the shelf) ( ) [browser] navegador web ( ) [www] servidor de presentación ( ) [email_client] cliente de correo electrónico ( ) [app] servidor de aplicaciones	

	( )	[file] servidor de ficheros
	( )	[dbms] sistema de gestión de base de datos
	( )	[tm] monitor transaccional
	(X)	[office] ofimática
	( )	[av] anti virus
	( )	[backup] sistema de backup
	( )	[os] sistema operativo

Valoración		
dimensión	valor	justificación
[I]		
[C]		
[A_D]		
[T_D]	7	Evitar la mal distribución de las licencias institucionales

Dependencias de activos inferiores (hijos)	
activo: [DTI.SOPTE_DTI] Soporte Técnico	grado:
¿Por qué?	
Se encargan de la instalación y funcionamiento del software	
activo: Usuarios	grado:
¿Por qué?	
Hacen uso del software para la gestión en la Sede	

[SW] Aplicaciones (software)	
código: AV_DTI	nombre: Antivirus
descripción:	Software Antivirus empleado para prevenir ataques e infecciones informáticas
Responsable del llenado:	Franklin Carrasco
Fecha de llenado:	6 de octubre 2014
responsable:	Técnico Redes 1 - Líder
tipo	
( )	[prp] desarrollo propio (in house)
( )	[sub] desarrollo a medida (subcontratado)
(X)	[std] standard (off the shelf)
	( ) [browser] navegador web

	( )	[www] servidor de presentación
	( )	[email_client] cliente de correo electrónico
	( )	[app] servidor de aplicaciones
	( )	[file] servidor de ficheros
	( )	[dbms] sistema de gestión de base de datos
	( )	[tm] monitor transaccional
	( )	[office] ofimática
	(X)	[av] anti virus
	( )	[backup] sistema de backup
	( )	[os] sistema operativo
Valoración		
dimensión	valor	justificación
[I]		
[C]		
[A_D]		
[T_D]	7	Evitar la mal distribución de las licencias institucionales
Dependencias de activos inferiores (hijos)		
activo: [DTI.SOPTE_DTI] Soporte Técnico		grado:
¿Por qué?		
Se encargan de la instalación y funcionamiento del software		
activo: Usuarios		grado:
¿Por qué?		
Protección de sus computadores		
activo: [REDES_DTI] Administradores de infraestructura y telecomunicaciones		grado:
¿Por qué?		
Los técnicos monitorean y controlan los ataques ocurridos en la red		

[SW] Aplicaciones (software)		
código: PROD_DTI	**nombre:** Sistema Informático de Producción	
descripción:	El sistema Informático de Producción se compone de los sistemas Informáticos Académico, HIPERK, y Nómina	
Responsable del llenado:	Franklin Carrasco	
Fecha de llenado:	6 de octubre 2014	
responsable:	Edwin Camino - Técnico Programación 1 - Líder	
tipo:		
(X)	[prp] desarrollo propio (in house)	
( )	[sub] desarrollo a medida (subcontratado)	
( )	[std] standard (off the shelf)	
	( ) [browser] navegador web	
	( ) [www] servidor de presentación	
	( ) [email_client] cliente de correo electrónico	
	( ) [app] servidor de aplicaciones	
	( ) [file] servidor de ficheros	
	( ) [dbms] sistema de gestión de base de datos	
	( ) [tm] monitor transaccional	
	( ) [office] ofimática	
	( ) [av] anti virus	
	( ) [backup] sistema de backup	
	( ) [os] sistema operativo	
Valoración		
dimensión	valor	justificación
[I]		
[C]		
[A_D]	7	Evitar la mal distribución de las licencias institucionales
[T_D]	7	Evitar la mal distribución de las licencias institucionales
Dependencias de activos inferiores (hijos)		
activo: Usuarios		grado:
¿Por qué?		
Para la realización de las actividades de gestión		
activo: [DTI.SOPTE_DTI] Soporte Técnico		grado:
¿Por qué?		
Se encargan de la instalación y funcionamiento del software		

d) [E] Equipamiento - [HW]Equipos

[HW] Equipamiento Informático (hardware)		
código: PRODS_DTI	**nombre:** Servidor de Producción	
descripción:	Servidor de Producción donde se alojan los sistemas Informáticos Académico, HIPERK, y Nómina	
Responsable del llenado:	Franklin Carrasco	
Fecha de llenado:	6 de octubre 2014	
responsable: Técnico Programación 1 - Líder		
ubicación: Data center		
número: 1		
tipo (X) [host] grandes equipos ( ) [mi] equipos medios ( ) [pc] informática personal ( ) [Mobile] informática móvil ( ) [PDA] agendas personales ( ) [es] fácilmente reemplazable (X) [data] que almacena datos ( ) [puerperal] periféricos ( ) [pronto] medios de impresión ( ) [san] escáneres ( ) [cripta] dispositivos criptográficos ( ) [Newark] soporte de la red ( ) [modem] módems ( ) [hubo] concentradores ( ) [switch] conmutadores ( ) [router] encaminadores ( ) [bridge] pasarelas ( ) [firewall] cortafuegos ( ) [pava] centralita telefónica		
Valoración		
dimensión	valor	justificación
[I]	9	Ocultar el equipo para evitar acciones contraproducentes
[C]	9	Ocultar el equipo para evitar acciones contraproducentes
[A_D]	9	Asegurar la manipulación del equipo por parte de técnicos especializados

[T_D]	9	Conocer que acciones realiza el técnico en el equipo
Dependencias de activos inferiores (hijos)		
activo: [REDES_DTI] Administradores de infraestructura y telecomunicaciones		grado:
¿Por qué?		
Los técnicos que monitorean el funcionamiento de los servidores		
activo: [CCTRL_CTI] Cuarto de Control		grado:
¿Por qué?		
Posee los elementos que le permiten mantener el funcionamiento continuo al equipo		

[HW] Equipamiento Informático (hardware)	
código: DSKB_DTI	**nombre:** Disco para respaldos de Sistemas Informáticos de Producción
descripción:	Disco externo empleado para respaldar la información los sistemas informáticos de Producción. Código fuente, ejecutables y bases de datos
Responsable del llenado:	Franklin Carrasco
Fecha de llenado:	6 de octubre 2014
responsable: Técnico Programación 1 - Líder	
ubicación: Data center	
número: 2	
tipo	
( )	[host] grandes equipos
( )	[mi] equipos medios
( )	[pc] informática personal
( )	[Mobile] informática móvil
( )	[PDA] agendas personales
( )	[es] fácilmente reemplazable
(X)	[data] que almacena datos
( )	[puerperal] periféricos
( )	[pronto] medios de impresión
( )	[san] escáneres

	( )	[cripta] dispositivos criptográficos
( )	[Newark] soporte de la red	
	( )	[modem] módems
	( )	[hubo] concentradores
	( )	[switch] conmutadores
	( )	[router] encaminadores
	( )	[bridge] pasarelas
	( )	[firewall] cortafuegos
( )	[pava] centralita telefónica	

Valoración		
dimensión	valor	justificación
[I]	7	Información histórica incorruptible
[C]	8	Información histórica segura
[A_D]	9	Acceso permitido al técnico responsable
[T_D]	9	Información histórica no debe ser manipulable por cualquier técnico

Dependencias de activos inferiores (hijos)	
activo: [ADMP_DTI] Administradores de Sistemas informáticos - Programadores	grado:
¿Por qué?	
Custodian los respaldos de los Sistemas Informáticos	

[HW] Equipamiento Informático (hardware)	
código: PWEBS_DTI	**nombre:** Servidor Portal Web
descripción:	Servidor del portal Web PUCESD y servicios para revisión de notas y heteroevaluación docente
Responsable del llenado:	Franklin Carrasco
Fecha de llenado:	6 de octubre 2014
responsable: Técnico Redes 1 - Líder	
ubicación: Data center	
número: 3	
tipo	
(X)	[host] grandes equipos

( )	[mi] equipos medios	
( )	[pc] informática personal	
( )	[Mobile] informática móvil	
( )	[PDA] agendas personales	
( )	[es] fácilmente reemplazable	
(X)	[data] que almacena datos	
( )	[puerperal] periféricos	
	( ) [pronto] medios de impresión	
	( ) [san] escáneres	
	( ) [cripta] dispositivos criptográficos	
( )	[Newark] soporte de la red	
	( ) [modem] módems	
	( ) [hubo] concentradores	
	( ) [switch] conmutadores	
	( ) [router] encaminadores	
	( ) [bridge] pasarelas	
	( ) [firewall] cortafuegos	
( )	[pava] centralita telefónica	

Valoración		
dimensión	valor	justificación
[I]	7	Al equipo sólo debe acercarse el técnico responsable
[C]		El equipo permanece en el Data center
[A_D]	5	El técnico responsable debe controlar el acceso al equipo por externos
[T_D]	5	El técnico responsable debe controlar el acceso al equipo por externos

Dependencias de activos inferiores (hijos)	
activo: [REDES_DTI] Administradores de infraestructura y telecomunicaciones	grado:
¿Por qué?	
Los técnicos que monitorean el funcionamiento de los servidores	
activo: [CCTRL_CTI] Cuarto de Control	grado:
¿Por qué?	
Posee los elementos que le permiten mantener el funcionamiento continuo al equipo	

[HW] Equipamiento Informático (hardware)		
código: BIBLS_DTI	**nombre:** Servidor Sistema de Biblioteca	
descripción:	Servidor del sistema de biblioteca	
Responsable del llenado:	Franklin Carrasco	
Fecha de llenado:	6 de octubre 2014	
responsable: Técnico Redes 1 - Líder		
ubicación: Data center		
número: 4		
tipo (X) [host] grandes equipos ( ) [mi] equipos medios ( ) [pc] informática personal ( ) [Mobile] informática móvil ( ) [PDA] agendas personales ( ) [es] fácilmente reemplazable (X) [data] que almacena datos ( ) [puerperal] periféricos ( ) [pronto] medios de impresión ( ) [san] escáneres ( ) [cripta] dispositivos criptográficos ( ) [Newark] soporte de la red ( ) [modem] módems ( ) [hubo] concentradores ( ) [switch] conmutadores ( ) [router] encaminadores ( ) [bridge] pasarelas ( ) [firewall] cortafuegos ( ) [pava] centralita telefónica		
Valoración		
dimensión	valor	justificación
[I]	7	Al equipo sólo debe acercarse el técnico responsable
[C]		El equipo permanece en el Data center
[A_D]	5	El técnico responsable debe controlar el acceso al equipo por externos
[T_D]	5	El técnico responsable debe controlar el acceso al equipo por externos
Dependencias de activos inferiores (hijos)		

activo: [REDES_DTI] Administradores de infraestructura y telecomunicaciones	grado:
¿Por qué?	
Los técnicos que monitorean el funcionamiento de los servidores	
activo: [CCTRL_CTI] Cuarto de Control	grado:
¿Por qué?	
Posee los elementos que le permiten mantener el funcionamiento continuo al equipo	

[HW] Equipamiento Informático (hardware)	
código: PROFS_DTI	**nombre:** Servidor Sistema administrador de personal docente
descripción:	Servidor del sistema informático empleado para el registro y seguimiento de los profesores de la Sede
Responsable del llenado: Franklin Carrasco	
Fecha de llenado: 6 de octubre 2014	
responsable: Técnico Redes 1 - Líder	
ubicación: Data center	
número: 5	
Tipo	
(X)	[host] grandes equipos
( )	[mi] equipos medios
( )	[pc] informática personal
( )	[Mobile] informática móvil
( )	[PDA] agendas personales
( )	[es] fácilmente reemplazable
(X)	[data] que almacena datos
( )	[puerperal] periféricos
	( ) [pronto] medios de impresión
	( ) [san] escáneres
	( ) [cripta] dispositivos criptográficos
( )	[Newark] soporte de la red
	( ) [modem] módems
	( ) [hubo] concentradores
	( ) [switch] conmutadores

	( )	[router] encaminadores
	( )	[bridge] pasarelas
	( )	[firewall] cortafuegos
( )	[pava] centralita telefónica	
Valoración		
dimensión	Valor	justificación
[I]	6	Al equipo sólo debe acercarse el técnico responsable
[C]	6	El equipo debe ser de conocimiento únicamente del personal técnico de TI
[A_D]	4	El técnico de TI debe evitar el acceso al equipo por otros técnicos
[T_D]	4	El técnico de TI debe evitar el acceso al equipo por otros técnicos
Dependencias de activos inferiores (hijos)		
activo: [REDES_DTI] Administradores de infraestructura y telecomunicaciones		grado:
¿Por qué?		
Los técnicos que monitorean el funcionamiento de los servidores		
activo: [CCTRL_CTI] Cuarto de Control		grado:
¿Por qué?		
Posee los elementos que le permiten mantener el funcionamiento continuo al equipo		

[HW] Equipamiento Informático (hardware)	
código: BIOMS_DTI	**nombre:** Servidor Sistema para control de ingreso de personal
descripción:	Servidor del sistema informático empleado para registrar y controlar el ingreso/salida y permisos del personal administrativo, y docente de planta
Responsable del llenado: Franklin Carrasco	
Fecha de llenado: 6 de octubre 2014	
responsable: Técnico Redes 1 - Líder	
ubicación: Data center	

número: 6		
Tipo		
(X)	[host] grandes equipos	
( )	[mid] equipos medios	
( )	[pc] informática personal	
( )	[mobile] informática móvil	
( )	[pda] agendas personales	
( )	[easy] fácilmente reemplazable	
(X)	[data] que almacena datos	
( )	[peripheral] periféricos	
	( )	[print] medios de impresión
	( )	[scan] escáneres
	( )	[crypto] dispositivos criptográficos
( )	[network] soporte de la red	
	( )	[modem] módems
	( )	[hub] concentradores
	( )	[switch] conmutadores
	( )	[router] encaminadores
	( )	[bridge] pasarelas
	( )	[firewall] cortafuegos
( )	[pabx] centralita telefónica	
Valoración		
dimensión	valor	justificación
[I]	6	Al equipo sólo debe acercarse el técnico responsable
[C]	6	El equipo debe ser de conocimiento únicamente del personal técnico de TI
[A_D]	6	El técnico de TI debe evitar el acceso al equipo por otros técnicos
[T_D]	7	Se debe evidenciar las actividades realizadas en el servidor
Dependencias de activos inferiores (hijos)		
activo: [REDES_DTI] Administradores de infraestructura y telecomunicaciones		grado:
¿Por qué?		
Los técnicos que monitorean el funcionamiento de los servidores		
activo: [CCTRL_CTI] Cuarto de Control		grado:
¿Por qué?		
Posee los elementos que le permiten mantener el funcionamiento continuo al equipo		

[HW] Equipamiento Informático (hardware)		
código: FILEBAS_DTI		**nombre:** Servidor Respaldo de Archivos
descripción:	Servidor de archivos donde se almacenan los archivos digitales de los usuarios que ingresaron al convenio de portátiles	
Responsable del llenado:	Franklin Carrasco	
Fecha de llenado:	6 de octubre 2014	
responsable: Técnico Redes 1 - Líder		
ubicación: Data center		
número: 7		
tipo		
(X)	[host] grandes equipos	
( )	[mid] equipos medios	
( )	[pc] informática personal	
( )	[mobile] informática móvil	
( )	[pda] agendas personales	
( )	[easy] fácilmente reemplazable	
(X)	[data] que almacena datos	
( )	[peripheral] periféricos	
	( )	[print] medios de impresión
	( )	[scan] escáneres
	( )	[crypto] dispositivos criptográficos
( )	[network] soporte de la red	
	( )	[modem] módems
	( )	[hub] concentradores
	( )	[switch] conmutadores
	( )	[router] encaminadores
	( )	[bridge] pasarelas
	( )	[firewall] cortafuegos
( )	[pabx] centralita telefónica	

Valoración		
dimensión	valor	justificación
[I]	6	Al equipo sólo debe acercarse el técnico responsable
[C]	6	El equipo debe ser de conocimiento únicamente del personal técnico de TI
[A_D]	6	El técnico de TI debe evitar el acceso al equipo por otros técnicos

[T_D]	6	Se debe evidenciar las actividades realizadas en el servidor
Dependencias de activos inferiores (hijos)		
activo: [REDES_DTI] Administradores de infraestructura y telecomunicaciones		grado:
¿Por qué?		
Los técnicos monitorean el funcionamiento de los servidores		
activo: [CCTRL_CTI] Cuarto de Control		grado:
¿Por qué?		
Posee los elementos que le permiten mantener el funcionamiento continuo al equipo		

[HW] Equipamiento Informático (hardware)		
código: PROXS_DTI	**nombre:** Servidor Proxy Firewall	
descripción:	Servidor de borde que controla y direcciona el tráfico en la red de datos de la Sede	
Responsable del llenado:	Franklin Carrasco	
Fecha de llenado:	6 de octubre 2014	
responsable: Técnico Redes 1 - Líder		
ubicación: Data center		
número: 8		
tipo (X) [host] grandes equipos ( ) [mid] equipos medios ( ) [pc] informática personal ( ) [mobile] informática móvil ( ) [pda] agendas personales ( ) [easy] fácilmente reemplazable ( ) [data] que almacena datos ( ) [peripheral] periféricos ( ) [print] medios de impresión ( ) [scan] escáneres ( ) [crypto] dispositivos criptográficos (X) [network] soporte de la red ( ) [modem] módems ( ) [hub] concentradores ( ) [switch] conmutadores ( ) [router] encaminadores ( ) [bridge] pasarelas (X) [firewall] cortafuegos ( ) [pabx] centralita telefónica		
Valoración		
dimensión	valor	justificación
[I]	7	El equipo sólo debe ser manipulado por el técnico responsable
[C]	7	El equipo debe ser de conocimiento únicamente del personal técnico de TI
[A_D]	9	Se debe saber que usuario de TI ingresa al equipo
[T_D]	9	Se debe evidenciar las actividades realizadas en el servidor por los técnicos de TI
Dependencias de activos inferiores (hijos)		

activo: [REDES_DTI] Administradores de infraestructura y telecomunicaciones	grado:
¿Por qué?	
Los técnicos monitorean el filtrado y correcto direccionamiento de los datos	
activo: [CCTRL_CTI] Cuarto de Control	grado:
¿Por qué?	
Posee los elementos que le permiten mantener el funcionamiento continuo al equipo	
activo: Usuarios	grado:
¿Por qué?	
Para la comunicación de datos y acceso a Internet	

[HW] Equipamiento Informático (hardware)		
código: DHCPS_DTI	**nombre:** Servidor DHCP	
descripción:	Servidor DHCP (asignación de direcciones IP dinámicas) de la Sede	
Responsable del llenado:	Franklin Carrasco	
Fecha de llenado:	6 de octubre 2014	
responsable: Técnico Redes 1 - Líder		
ubicación: Data center		
número: 9		
tipo		
(X)	[host] grandes equipos	
( )	[mid] equipos medios	
( )	[pc] informática personal	
( )	[mobile] informática móvil	
( )	[pda] agendas personales	
( )	[easy] fácilmente reemplazable	
( )	[data] que almacena datos	
( )	[peripheral] periféricos	
	( )	[print] medios de impresión
	( )	[scan] escáneres
	( )	[crypto] dispositivos criptográficos
(X)	[network] soporte de la red	
	( )	[modem] módems

	( )	[hub] concentradores
	( )	[switch] conmutadores
	( )	[router] encaminadores
	( )	[bridge] pasarelas
	( )	[firewall] cortafuegos
( )	[pabx] centralita telefónica	
Valoración		
dimensión	valor	justificación
[I]	5	El equipo sólo debe ser manipulado por el técnico responsable
[C]		
[A_D]	7	Se debe saber que usuario de TI ingresa al equipo
[T_D]	5	Se debe evidenciar las actividades realizadas en el servidor por los técnicos de TI
Dependencias de activos inferiores (hijos)		
activo: [REDES_DTI] Administradores de infraestructura y telecomunicaciones		grado:
¿Por qué?		
Los técnicos monitorean que se asignen correctamente las direcciones IP		
activo: [CCTRL_CTI] Cuarto de Control		grado:
¿Por qué?		
Posee los elementos que le permiten mantener el funcionamiento continuo al equipo		
activo: Usuarios		grado:
¿Por qué?		
Para la comunicación de datos y acceso a Internet		

[HW] Equipamiento Informático (hardware)	
código: SWITCH_DTI	nombre: Switch
descripción:	Conjunto de switches empleados para la transmisión segura de la información por la red de la Sede
Responsable del llenado:	Franklin Carrasco
Fecha de llenado:	6 de octubre 2014
responsable: Técnico Redes 1 - Líder	

ubicación: Data center

número: 10

tipo

( ) [host] grandes equipos
( ) [mid] equipos medios
( ) [pc] informática personal
( ) [mobile] informática móvil
( ) [pda] agendas personales
( ) [easy] fácilmente reemplazable
( ) [data] que almacena datos
( ) [peripheral] periféricos
    ( ) [print] medios de impresión
    ( ) [scan] escáneres
    ( ) [crypto] dispositivos criptográficos
(X) [network] soporte de la red
    ( ) [modem] módems
    ( ) [hub] concentradores
    (X) [switch] conmutadores
    ( ) [router] encaminadores
    ( ) [bridge] pasarelas
    ( ) [firewall] cortafuegos
( ) [pabx] centralita telefónica

Valoración

dimensión	valor	justificación
[I]	7	Paso de datos sin interrupciones o intercepciones
[C]		
[A_D]	7	Es necesario identificar al usuario de TI que accede al equipo
[T_D]	7	Es necesario saber las actividades que realiza el usuario de TI en el equipo

Dependencias de activos inferiores (hijos)

activo: [REDES_DTI] Administradores de infraestructura y telecomunicaciones	grado:
¿Por qué?	
Los técnicos monitorean y controlan la conectividad de los usuarios con la red	
activo: [CCTRL_CTI] Cuarto de Control	grado:
¿Por qué?	

Posee los elementos que le permiten mantener el funcionamiento continuo al equipo	
activo: Usuarios	grado:
¿Por qué?	
Para la comunicación de datos y acceso a Internet	

[HW] Equipamiento Informático (hardware)	
código: ROUTER_DTI	nombre: Router
descripción:	Equipo activo que permite el direccionamiento de los paquetes de datos de la Sede
Responsable del llenado:	Franklin Carrasco
Fecha de llenado:	6 de octubre 2014
responsable: Técnico Redes 1 - Líder	
ubicación: Data center	
número: 11	

tipo

( )	[host] grandes equipos	
( )	[mid] equipos medios	
( )	[pc] informática personal	
( )	[mobile] informática móvil	
( )	[pda] agendas personales	
( )	[easy] fácilmente reemplazable	
( )	[data] que almacena datos	
( )	[peripheral] periféricos	
	( )	[print] medios de impresión
	( )	[scan] escáneres
	( )	[crypto] dispositivos criptográficos
(X)	[network] soporte de la red	
	( )	[modem] módems
	( )	[hub] concentradores
	( )	[switch] conmutadores
	(X)	[router] encaminadores
	( )	[bridge] pasarelas
	( )	[firewall] cortafuegos

( ) [pabx] centralita telefónica		
Valoración		
dimensión	valor	justificación
[I]	9	Permitir el direccionamiento de los datos sin interrupciones o intercepciones
[C]		
[A_D]	9	Es necesario identificar al usuario de TI que accede al equipo
[T_D]	9	Es necesario saber las actividades que realiza el usuario de TI en el equipo
Dependencias de activos inferiores (hijos)		
activo: [REDES_DTI] Administradores de infraestructura y telecomunicaciones		grado:
¿Por qué?		
Los técnicos monitorean y controlan el direccionamiento de los datos en la red		
activo: [CCTRL_CTI] Cuarto de Control		grado:
¿Por qué?		
Posee los elementos que le permiten mantener el funcionamiento continuo del equipo		
activo: Usuarios		grado:
¿Por qué?		
Para la comunicación de datos y acceso a Internet		

[HW] Equipamiento Informático (hardware)	
código: WLC_DTI	**nombre:** Controladora de red inalámbrica
descripción:	Controladora de red inalámbrica, empleada para la conexión y administración de los Puntos de Acceso inalámbricos de la Sede
Responsable del llenado:	Franklin Carrasco
Fecha de llenado:	6 de octubre 2014
responsable: Técnico Redes 1 - Líder	
ubicación: Data center	
número: 12	
tipo ( ) [host] grandes equipos	

( )	[mid] equipos medios	
( )	[pc] informática personal	
( )	[mobile] informática móvil	
( )	[pda] agendas personales	
( )	[easy] fácilmente reemplazable	
( )	[data] que almacena datos	
( )	[peripheral] periféricos	
	( )	[print] medios de impresión
	( )	[scan] escáneres
	( )	[crypto] dispositivos criptográficos
(X)	[network] soporte de la red	
	( )	[modem] módems
	( )	[hub] concentradores
	( )	[switch] conmutadores
	( )	[router] encaminadores
	( )	[bridge] pasarelas
	( )	[firewall] cortafuegos
( )	[pabx] centralita telefónica	

Valoración		
dimensión	valor	justificación
[I]	3	Permitir la conectividad única de los APS de la Sede
[C]		
[A_D]	7	Es necesario identificar al usuario de TI que accede al equipo
[T_D]	7	Es necesario saber las actividades que realiza el usuario de TI en el equipo

Dependencias de activos inferiores (hijos)	
activo: [REDES_DTI] Administradores de infraestructura y telecomunicaciones	grado:
¿Por qué?	
Los técnicos monitorean y controlan la conectividad de los APS en la red Inalámbrica	
activo: [CCTRL_CTI] Cuarto de Control	grado:
¿Por qué?	
Posee los elementos que le permiten mantener el funcionamiento continuo del equipo	
activo: Usuarios	grado:
¿Por qué?	

Para la comunicación de datos y acceso a Internet a través de la red inalámbrica

[HW] Equipamiento Informático (hardware)	
código: WAP_DTI	**nombre:** Punto de Acceso Inalámbrico
descripción:	Conjunto de Puntos de Acceso inalámbricos empleados para la transmisión segura de la información por la red inalámbrica de la Sede
Responsable del llenado:	Franklin Carrasco
Fecha de llenado:	6 de octubre 2014
responsable: Técnico Redes 1 - Líder	
ubicación: Data center	
número: 13	

tipo

- ( ) [host] grandes equipos
- ( ) [mid] equipos medios
- ( ) [pc] informática personal
- ( ) [mobile] informática móvil
- ( ) [pda] agendas personales
- ( ) [easy] fácilmente reemplazable
- ( ) [data] que almacena datos
- ( ) [peripheral] periféricos
  - ( ) [print] medios de impresión
  - ( ) [scan] escáneres
  - ( ) [crypto] dispositivos criptográficos
- (X) [network] soporte de la red
  - ( ) [modem] módems
  - ( ) [hub] concentradores
  - ( ) [switch] conmutadores
  - ( ) [router] encaminadores
  - ( ) [bridge] pasarelas
  - ( ) [firewall] cortafuegos
- ( ) [pabx] centralita telefónica

Valoración		
dimensión	valor	justificación
[I]	7	Paso de datos sin interrupciones o intercepciones
[C]		
[A_D]	7	Es necesario identificar al usuario de TI que accede al equipo
[T_D]	7	Es necesario saber las actividades que realiza el usuario de TI en el equipo
Dependencias de activos inferiores (hijos)		
activo: [REDES_DTI] Administradores de infraestructura y telecomunicaciones		grado:
¿Por qué?		
Los técnicos monitorean y controlan la conectividad de los usuarios con la red inalámbrica		
activo: Usuarios		grado:
¿Por qué?		
Para la comunicación de datos y acceso a Internet a través de la red inalámbrica		

e) [E] Equipamiento - [COM]Comunicaciones

[COM] Redes de comunicaciones	
código: LAN_DTI	nombre: Red LAN
descripción:	Red de área local de la Sede
Responsable del llenado:	Franklin Carrasco
Fecha de llenado:	6 de octubre 2014
responsable: Técnico Redes 1 - Líder	
ubicación: Campus Universitario	
número: 1	
tipo ( ) [PSTN] red telefónica ( ) [ISDN] RDSI (red digital) ( ) [X25] X25 (red de datos)	

( )	[ADSL] ADSL	
( )	[pp] punto a punto	
( )	[radio] red inalámbrica	
( )	[sat] satélite	
(X)	[LAN] red local	
( )	[MAN] red metropolitana	
( )	[Internet] internet	
( )	[vpn] red privada virtual	
Valoración		
dimensión	valor	justificación
[I]	7	Evitar la captura intermedia de datos
[C]		
[A_D]	7	Identificar a los usuario que acceden a la red
[T_D]	7	Monitorear y controlar la actividades de cada usuario en la red
Dependencias de activos inferiores (hijos)		
activo: [PROXS_DTI] Servidor Proxy Firewall		grado:
¿Por qué?		
para el acceso y direccionamiento de los datos		
activo: [ROUTER_DTI] Router		grado:
¿Por qué?		
Para el direccionamiento de los datos en las redes		
activo: [SWITCH_DTI] Switch		grado:
¿Por qué?		
Conexión de acceso de las estaciones de trabajo a la red LAN		
activo: [CABLE_DTI] Cableado de Datos		grado:
¿Por qué?		
Conectividad entre las estaciones de trabajo a la red LAN		
activo: Estudiantes, personal administrativo y docente		grado:
¿Por qué?		
Para el acceso a los servicios de comunicación y envío de datos		

[COM] Redes de comunicaciones		
código: WLAN_DTI	**nombre:** Red LAN Inalámbrica	
descripción: Red de área local inalámbrica de la Sede		
Responsable del llenado: Franklin Carrasco		
Fecha de llenado: 6 de octubre 2014		
responsable: Técnico Redes 1 - Líder		
ubicación: Campus Universitario		
número: 2		
tipo ( ) [PSTN] red telefónica ( ) [ISDN] RDSI (red digital) ( ) [X25] X25 (red de datos) ( ) [ADSL] ADSL ( ) [pp] punto a punto (X) [radio] red inalámbrica ( ) [sat] satélite (X) [LAN] red local ( ) [MAN] red metropolitana ( ) [Internet] internet ( ) [vpn] red privada virtual		
Valoración		
dimensión	valor	justificación
[I]	6	Evitar la captura intermedia de datos
[C]		
[A_D]	7	Identificar a los usuario que acceden a la red
[T_D]	7	Monitorear y controlar la actividades de cada usuario en la red
Dependencias de activos inferiores (hijos)		
activo: [PROXS_DTI] Servidor Proxy Firewall		grado:
¿Por qué?		
para el acceso y direccionamiento de los datos		
activo: [ROUTER_DTI] Router		grado:
¿Por qué?		
Para el direccionamiento de los datos en las redes		
activo: [HW.WLC_DTI] Controladora de red inalámbrica		grado:
¿Por qué?		
Permite la conexión de los Puntos de Acceso inalámbrico a la red WLAN		
activo: [WAP_DTI] Punto de Acceso Inalámbrico		grado:

¿Por qué?	
Conexión de acceso inalámbrico de los usuarios	
activo: Estudiantes, personal administrativo y docente	grado:
¿Por qué?	
Para el acceso a los servicios de comunicación y envío de datos	

[COM] Redes de comunicaciones		
código: INTERNET_DTI	**nombre:** Servicio de Internet	
descripción:	Red de Internet	
Responsable del llenado:	Franklin Carrasco	
Fecha de llenado: 6 de octubre 2014		
responsable: Técnico Redes 1 - Líder		
ubicación: Campus Universitario		
número: 3		
tipo ( ) [PSTN] red telefónica ( ) [ISDN] RDSI (red digital) ( ) [X25] X25 (red de datos) ( ) [ADSL] ADSL ( ) [pp] punto a punto ( ) [radio] red inalámbrica ( ) [sat] satélite ( ) [LAN] red local ( ) [MAN] red metropolitana (X) [Internet] internet ( ) [vpn] red privada virtual		
dimensión	valor	justificación
[I]	9	Los datos deben mantener su estructura original
[C]	7	Evitar intercepción de la información de la Sede
[A_D]	7	Identificar a los usuario que acceden a la red

[T_D]	7	Monitorear y controlar la actividades de cada usuario en la red
Dependencias de activos inferiores (hijos)		
activo: [INTERSUB_DTI] Servicio de Internet		grado:
¿Por qué?		
Sin el contrato del servicio con un ISP no es posible tener Internet		
activo: [PROXS_DTI] Servidor Proxy Firewall		grado:
¿Por qué?		
Se necesita para el acceso y direccionamiento de los datos		
activo: [ROUTER_DTI] Router		grado:
¿Por qué?		
Se necesita para el direccionamiento de los datos		
activo: [SWITCH_DTI] Switch		grado:
¿Por qué?		
Conexión de acceso de las estaciones de trabajo a la red LAN		
activo: [CABLE_DTI] Cableado de Datos		grado:
¿Por qué?		
Conectividad entre las estaciones de trabajo a la red LAN		
activo: Estudiantes, personal administrativo y docente		grado:
¿Por qué?		
Para el acceso a los servicios de comunicación y envío de datos		

f) [E] Equipamiento - [AUX] Elementos Auxiliares

[AUX] Equipamiento auxiliar	
código: SAI_DTI	**nombre:** Sistema de alimentación ininterrumpida
descripción:	Sistema de alimentación ininterrumpida, para resguardo del funcionamiento de los equipos de Data center en caso de interrupción eléctrica
Responsable del llenado:	Franklin Carrasco
Fecha de llenado:	6 de octubre 2014
responsable: Técnico Redes 1 - Líder	

ubicación: Campus Universitario		
número: 1		
tipo ( ) [power] fuentes de alimentación (X) [ups] sistemas de alimentación ininterrumpida ( ) [gen] generadores eléctricos ( ) [ac] equipos de climatización ( ) [cabling] cableado ( ) [robot] robots ( ) [tape] robots de cintas ( ) [disk] robots de discos ( ) [supply] suministros esenciales ( ) [destroy] equipos de destrucción de soportes de información ( ) [furniture] mobiliario: armarios, etc. ( ) [safe] cajas fuertes		
Valoración		
dimensión	valor	justificación
[I]		
[C]		
[A_D]		
[T_D]	7	Conocer la manipulación del equipo por los técnicos
Dependencias de activos inferiores (hijos)		
activo: [REDES_DTI] Administradores de infraestructura y telecomunicaciones		grado:
¿Por qué?		
Por los técnicos deben actuar de forma inmediata para mantener la funcionalidad de los equipos que se alojan en el Data center, mediante la configuración del SAI		

[AUX] Equipamiento auxiliar		
código: AC_DTI	**nombre:** Aire Acondicionado	
descripción: Sistema de enfriamiento del Data center		
Responsable del llenado: Franklin Carrasco		
Fecha de llenado: 6 de octubre 2014		
responsable: Técnico Redes 1 - Líder		
ubicación: Campus Universitario		
número: 2		
tipo ( ) [power] fuentes de alimentación ( ) [ups] sistemas de alimentación ininterrumpida ( ) [gen] generadores eléctricos (X) [ac] equipos de climatización ( ) [cabling] cableado ( ) [robot] robots ( ) [tape] robots de cintas ( ) [disk] robots de discos ( ) [supply] suministros esenciales ( ) [destroy] equipos de destrucción de soportes de información ( ) [furniture] mobiliario: armarios, etc. ( ) [safe] cajas fuertes		
Valoración		
dimensión	valor	justificación
[I]		
[C]		
[A_D]		
[T_D]	7	Conocer la manipulación del equipo por los técnicos
Dependencias de activos inferiores (hijos)		
activo: [REDES_DTI] Administradores de infraestructura y telecomunicaciones		grado:
¿Por qué?		
Los técnicos deben revisar que se mantenga la temperatura adecuada en el Data center para evitar fallas de calentamiento en los equipos		

[AUX] Equipamiento auxiliar		
código: CABLE_DTI	**nombre:** Cableado de Datos	
descripción:	Cableado de datos que forma la Red LAN de la Sede	
Responsable del llenado:	Franklin Carrasco	
Fecha de llenado:	6 de octubre 2014	
responsable: Técnico Redes 1 - Líder		
ubicación: Campus Universitario		
número: 3		
tipo		
( )	[power] fuentes de alimentación	
( )	[ups] sistemas de alimentación ininterrumpida	
( )	[gen] generadores eléctricos	
( )	[ac] equipos de climatización	
(X)	[cabling] cableado	
( )	[robot] robots	
	( )	[tape] robots de cintas
	( )	[disk] robots de discos
( )	[supply] suministros esenciales	
( )	[destroy] equipos de destrucción de soportes de información	
( )	[furniture] mobiliario: armarios, etc.	
( )	[safe] cajas fuertes	
Valoración		
dimensión	valor	justificación
[I]		
[C]		
[A_D]		
[T_D]	7	Conocer la distribución de los enlaces para evitar accesos no permitidos
Dependencias de activos inferiores (hijos)		
activo: [REDES_DTI] Administradores de infraestructura y telecomunicaciones		grado:
¿Por qué?		
Los técnicos deben monitorear y revisar la conectividad de cada usuario en la red, evitando accesos no autorizados		

g) [L] Instalaciones

[L] Instalaciones		
código: CCTRL_CTI		**nombre:** Cuarto de Control
descripción:	Cuarto de Control o Data center de la Sede	
Responsable del llenado:	Franklin Carrasco	
Fecha de llenado:	6 de octubre 2014	
responsable: Técnico Redes 1 - Líder		
ubicación: Campus Universitario		
número: 1		
tipo ( ) [site] emplazamiento ( ) [building] edificio (X) [local] local ( ) [mobile] plataformas móviles ( ) [car] vehículo terrestre: coche, camión, etc. ( ) [plane] vehículo aéreo: avión, etc. ( ) [ship] vehículo marítimo: buque, lancha, etc. ( ) [shelter] contenedores ( ) [channel] canalización		
Valoración		
dimensión	valor	justificación
[I]	9	El cuarto debe estar alejado de todo acceso a la intemperie
[C]	8	Debe mantenerse en el anonimato por seguridad de la información
[A_D]	9	Se debe restringir el acceso de toda persona al sitio
[T_D]	9	se debe evidenciar las actividades realizada en el sitio
Dependencias de activos inferiores (hijos)		
activo: [REDES_DTI] Administradores de infraestructura y telecomunicaciones		grado:
¿Por qué?		
Los técnicos de TI administran el funcionamiento de los elementos del Cuarto de Control		

h) [P] Personal

[P] Personal	
código: ADMP_DTI	**nombre:** Administradores de Sistemas informáticos - Programadores
descripción:	Técnico encargado de la administración de los sistemas informáticos y sus respectivas bases de datos
Responsable del llenado:	Franklin Carrasco
Fecha de llenado:	6 de octubre 2014
número: 1	
tipo ( ) [ue] usuarios externos ( ) [ui] usuarios internos ( ) [op] operadores (X) [adm] administradores del sistema ( ) [com] administradores de comunicaciones (X) [dba] administradores de BBDD (X) [des] desarrolladores ( ) [sub] subcontratas ( ) [prov] proveedores	

Valoración		
dimensión	valor	justificación
[I]		
[C]	9	Puede estar expuesto a solicitudes de usuarios externos, que busquen una finalidad perjudicial para la Sede
[A_D]		
[T_D]		

[P] Personal	
código: REDES_DTI	**nombre:** Administradores de infraestructura y telecomunicaciones
descripción:	Técnico encargado de administrar las redes de datos de la Sede

Responsable del llenado: Franklin Carrasco		
Fecha de llenado: 6 de octubre 2014		
número: 2		
tipo ( ) [ue] usuarios externos ( ) [ui] usuarios internos ( ) [op] operadores ( ) [adm] administradores del sistema (X) [com] administradores de comunicaciones ( ) [dba] administradores de BBDD ( ) [des] desarrolladores ( ) [sub] subcontratas ( ) [prov] proveedores		
Valoración		
dimensión	valor	justificación
[I]		
[C]	9	Puede estar expuesto a solicitudes de usuarios externos, que busquen una finalidad perjudicial para la Sede
[A_D]		
[T_D]		

[P] Personal	
código: SOPTE_DTI	**nombre:** Soporte Técnico
descripción:	Técnico encargado de dar soporte a usuarios y mantenimiento a computadoras
Responsable del llenado: Franklin Carrasco	
Fecha de llenado: 6 de octubre 2014	
número: 3	
tipo ( ) [ue] usuarios externos ( ) [ui] usuarios internos (X) [op] operadores ( ) [adm] administradores del sistema ( ) [com] administradores de comunicaciones	

( )	[dba] administradores de BBDD
( )	[des] desarrolladores
( )	[sub] subcontratas
( )	[prov] proveedores
Valoración	
dimensión	justificación
[I]	
[C]	
[A_D]	
[T_D]	

BIBLIOGRAFÍA

[1] P. A. López, Seguridad Informática, Madrid: Editex S.A., 2010.

[2] F. Ebel, J. Hennecart, S. Lasson, D. Puche, R. R. ACISSI, M. Agé, S. Baudru, N. Crocfer y (. Robert Crocfer, Seguridad informática: Ethical Hacking, Eni Ediciones, 2013.

[3] National Institute of Standards and Technology, Contingency Planning Guide for Federal Information Systems, Gaithersburg: Computer Security Division, Information Technology Laboratory, 2010.

[4] INTECO, «Instituto Nacional de Tecnologías de la Comunicación de España,» 08 08 2010. [En línea]. Available: http://www.inteco.es/icdemo/empresas/Catalogo_STIC/Busqueda_de_Soluciones/Informacion_de_categoria_1/?postAction=solutionCategoryView&idCategory=21.

[5] C. Kunthe, «ISACA - Difference between BCP and DR,» 01 02 2013. [En línea]. Available: http://www.isaca.org/Groups/Professional-English/business-continuity-disaster-recovery-planning/Pages/ViewDiscussion.aspx?PostID=72.

[6] R. J. Sandhu, Disaster Recovery Planning, Cincinnati: Muska & Lipman/Premier-Trade, 2002, p. 320.

[7] R. A. Española, «http://lema.rae.es/drae/,» 04 03 2014. [En línea]. Available: http://lema.rae.es/drae/srv/search?key=riesgo.

[8] I. R. IT, «ISACA,» 2009. [En línea]. Available: https://www.isaca.org.

[9] ISACA, «ISACA,» 2013. [En línea]. Available: http://www.isaca.org/Knowledge-Center/Standards/Documents/1202_std_Spanish_1113.pdf.

[10] P. e. I. d. l. A. E. Dirección General de Modernización Administrativa, «MAGERIT – versión 3.0. Metodología de Análisis y Gestión de Riesgos de los Sistemas de Información. Libro I- Método,» Madrid, 2012.

[11] ISO/IEC, Estándard Internacional ISO 27001, España, 2013.

[12] IBM, «IBM,» 2010. [En línea]. Available: http://www-935.ibm.com/services/es/es/it-services/analisis-de-impacto-de-negocio.html.

[13] A. d. J. A. K. M. P. R. T. A. v. d. V. T. V. Jan van Bon, Mejora Continua del Servicio Basada en ITIL V3 - Guía de Gestión, Amersfoort: Van Haren Publishing, 2008.

[14] A. Asociación Nacional de Empresas de Internet, «Comunidad de Madrid,» 21 abril 2006. [En línea]. Available: http://www.madrid.org/cs/Satellite?blobcol=urldata&blobheader=application%2Fpdf&blobheadername1=Content-Disposition&blobheadervalue1=filename%3DManual+de+introducci%C

3%B3n+a+la+seguridad+en+el+%C3%A1mbito+empresarial.pdf&blobkey=id&blobtable=MungoBlobs&bl.

[15] CCN-CERT, «CERT Gubernamental,» 2014. [En línea]. Available: https://www.ccn-cert.cni.es/publico/ens/ens/index.html?n=172.html.

[16] G. d. España, «Portal administración electrónica,» Octubre 2012. [En línea]. Available: http://administracionelectronica.gob.es/pae_Home/pae_Documentacion/pae_Metodolog/pae_Magerit.html.