ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

MAESTRÍA EN SEGURIDAD INFORMÁTICA

Tema:

"IMPLEMENTACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS TECNOLÓGICOS Y DE SEGURIDAD DE LA INFORMACIÓN A LA PLATAFORMA DE GESTIÓN ACADÉMICA DE UNA INSTITUCIÓN DE EDUCACIÓN SUPERIOR DEL ECUADOR"

PROYECTO DE TITULACIÓN

Previo a la obtención del título de

MAGÍSTER EN SEGURIDAD INFORMÁTICA APLICADA

Presentado por:

ING. LÍDICE VICTORIA HAZ LÓPEZ
LSI. JACINTO GEOVANNY CERVANTES BUSTOS

GUAYAQUIL – ECUADOR

AÑO: 2017

AGRADECIMIENTO

Agradezco a Dios, mi guía y protección en toda mi vida. A mis padres, hermanos y demás familiares que hicieron posible que llegue al cumplimiento de este objetivo. A los profesores de la maestría, en especial a la directora del proyecto, por sus directrices técnicas que permitieron concluir exitosamente este trabajo. A las autoridades de la institución de educación superior que nos abrió las puertas para la ejecución de este proyecto.

Jacinto Geovanny Cervantes Bustos

AGRADECIMIENTO

Quiero agradecer a mis padres por el apoyo y la confianza depositada en mí, durante todo este tiempo de formación académica y a mi tutora por el soporte y la ayuda brindada durante el desarrollo de este proyecto. A mis amigos y compañeros de maestría, Geovanny Cervantes y Víctor Contreras con quienes formé un gran equipo de trabajo, y que gracias a su apoyo, y conocimientos hicieron de esta experiencia una de las más especiales de mi vida. Y a todas las personas que ayudaron directa e indirectamente en la realización de este trabajo.

Lídice Victoria Haz López

DEDICATORIA

A Dios, a mis padres, hermanos y sobrinos.

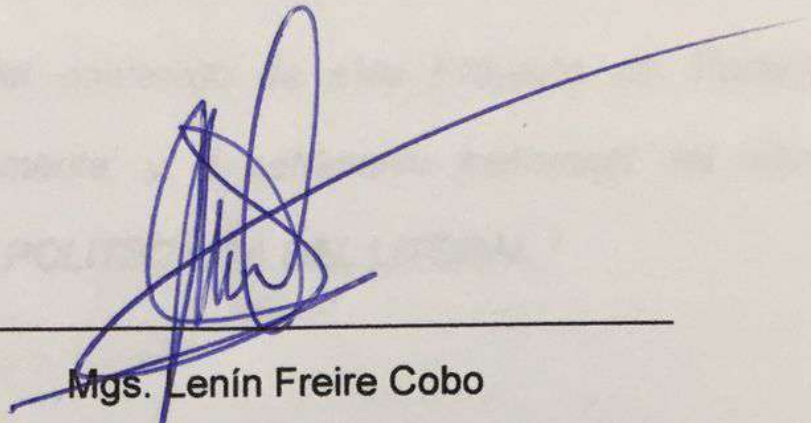
Jacinto Geovanny Cervantes Bustos

DEDICATORIA

A mi madre que ha sabido formarme con buenos sentimientos, hábitos y valores, lo cual me ha ayudado a salir adelante en todos los momentos de mi vida.

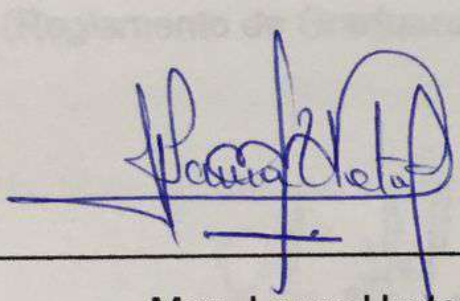
Lídice Victoria Haz López

TRIBUNAL DE SUSTENTACIÓN



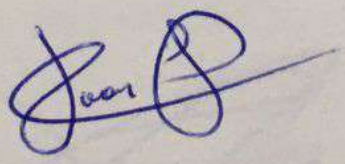
Mgs. Lenín Freire Cobo

DIRECTOR MSIA



Mgs. Laura Ureta Arreaga

DIRECTORA DEL PROYECTO DE TITULACIÓN



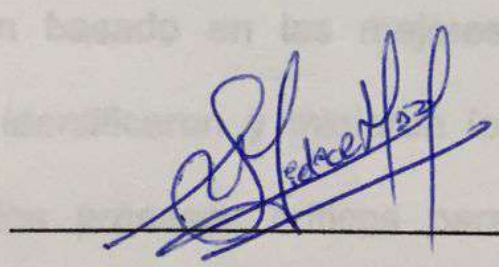
Mgs. Juan Carlos García Plúa

MIEMBRO DEL TRIBUNAL

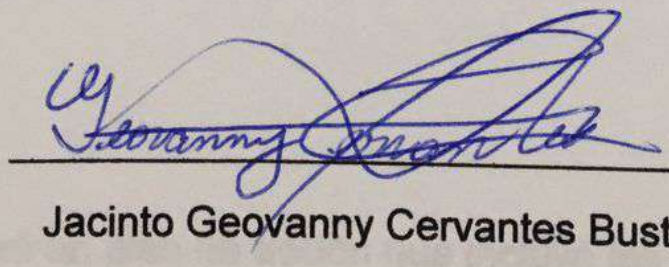
DECLARACIÓN EXPRESA

"La responsabilidad del contenido de este Proyecto de Titulación, nos corresponde exclusivamente; y el patrimonio intelectual del mismo a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL."

(Reglamento de Graduación de la ESPOL)



Lídice Victoria Haz López



Jacinto Geovanny Cervantes Bustos

RESUMEN

Este documento presenta un trabajo técnico administrativo para implantar un proceso para la identificación, medición, control y monitoreo del riesgo tecnológico y de seguridad de la información, que permita prevenir y reducir niveles de pérdida por la materialización de este tipo de riesgos en una institución de educación superior.

Se definió un proceso para la gestión del riesgo tecnológico y de seguridad de la información basado en las mejores prácticas a nivel nacional e internacional; se identificaron y midieron los riesgos sobre los activos de información de dos procesos críticos para la institución y que podrían provocar afectaciones materiales, financieras, operativas y de imagen, determinando cualitativamente su probabilidad de ocurrencia e impacto.

Además, se elaboró un plan de acción que incluyó los controles de mitigación para contrarrestar los efectos de los riesgos identificados así como su probabilidad de ocurrencia, un presupuesto estimado y el análisis de la conveniencia económica de implementar las contramedidas.

Se realizó un análisis de los principales mecanismos que permitan la retroalimentación de la gestión de riesgos y asegurar razonablemente la ejecución de los controles de mitigación.

Finalmente, se muestran los resultados obtenidos de la aplicación del proceso de gestión de riesgos definido, los efectos generados y el impacto en la administración de las tecnologías de la información en la institución de educación superior.

.

ÍNDICE GENERAL

ABREVIATURAS Y SIMBOLOGÍA

AS/NZS	Estándar Australiano y de Nueva Zelanda
CEAACES	Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior
CNT	Corporación Nacional de Telecomunicaciones
COSO	Committee of Sponsoring Organizations of the Treadway Commission (Comité de Organizaciones Patrocinadoras de la Comisión Treadway)
FODA	Fortalezas, oportunidades, debilidades y amenazas.
I	Impacto
I (USD)	Impacto económico
IEC	International Electrotechnical Commission (Comisión Internacional Electrotécnica)
ISACA	Information Systems Audit and Control Association (Asociación de Auditoría y Control de Sistemas de Información)
ISO	International Organization for Standarization (Organización Internacional de Normalización)
ITGI	Information Technology Governance Institute (Gobernanza de las Tecnologías de la Información)
LOES	Ley Orgánica de Educación Superior
OMC	Organización Mundial del Comercio

P	Probabilidad de ocurrencia
PGRTI	Proceso de gestión de riesgos de tecnología y seguridad de la información
PMTI	Periodo máximo tolerable de interrupción
R	Riesgo
R (USD)	Valor en riesgo
SI	Seguridad de la información
TI	Tecnologías de la información
TIC	Tecnologías de la información y comunicación
UPS	Uninterruptible Power Supply (sistema de alimentación ininterrumpida)

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

INTRODUCCIÓN

Son instituciones del Sistema de Educación Superior las universidades, escuelas politécnicas; y, los institutos superiores técnicos, tecnológicos, pedagógicos, de artes y los conservatorios superiores, tanto públicos como particulares, debidamente evaluados y acreditados, conforme la Ley Orgánica de Educación Superior [1]. En Ecuador existen 60 instituciones de educación superior entre universidades, escuelas politécnicas públicas y particulares.

El sistema de educación superior tiene como finalidad la formación académica y profesional con visión científica y humanista; la investigación científica y tecnológica; la innovación, promoción, desarrollo y difusión de los saberes y las culturas; la construcción de soluciones para los problemas del país, en relación con los objetivos del régimen de desarrollo.

A partir del 29 de agosto de 2011, el Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior (CEAACES), ejerce la rectoría de la política pública para el aseguramiento de la calidad de la educación superior del Ecuador a través de procesos de evaluación,

acreditación y categorización en las instituciones de educación superior, en concordancia con el numeral 2, artículo 353 de la Constitución [2].

Las normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos expedidas por la Contraloría General del Estado [3], sirven como marco de referencia para que las instituciones del Estado establezcan y pongan en funcionamiento su propio control interno; también señala que: *"El control interno está orientado a cumplir con el ordenamiento jurídico, técnico y administrativo, promover eficiencia y eficacia de las operaciones de la entidad y garantizar la confiabilidad y oportunidad de la información, así como la adopción de medidas oportunas para corregir las deficiencias de control"* [3].

En el numeral 300. Evaluación de riesgos de las normas de control interno antes indicadas, se menciona que las autoridades de la institución son los responsables de efectuar el proceso de administración de riesgos.

Uno de los procesos más importantes que deben definirse y controlarse en cualquier tipo de institución es el proceso de gestión de riesgos, ya que las

organizaciones podrían estar expuestas a pérdidas significativas al no realizar un adecuado manejo de los riesgos en las actividades y procesos críticos afectando el normal funcionamiento de las operaciones y a la consecución de sus objetivos.

El presente proyecto se aplicará en una institución de educación superior del Ecuador, se trata de una universidad de prestigio y su fin principal es formar profesionales comprometidos con la sociedad, brindar servicios académicos de alta calidad, fomentar la investigación; y, adoptar y generar conocimientos científicos y tecnológicos.

La implementación del proceso de gestión de riesgos tecnológicos y de seguridad de la información permitirá a la universidad controlar en un nivel razonable los riesgos de tecnología de la información, obteniendo el mayor grado de mitigación posible, es decir, que sea capaz de identificar y controlar las amenazas y vulnerabilidades, de tal forma que se disminuya el impacto del riesgo en caso de que este se materialice. Las instituciones deben controlar los riesgos sin alterar significativamente sus características de estructura y funcionalidad, y permitir regresar a su estado original una vez que el evento de riesgo ha terminado.

El primer paso para gestionar los riesgos es conocer e identificar los procesos, los activos de información que soportan a los procesos así como las potenciales amenazas y vulnerabilidades que pueden afectarlos y ocasionar pérdidas a la institución, determinando las causas y efectos en caso de que el evento ocurra, generando la matriz de riesgos donde se identifique la probabilidad y consecuencias de cada riesgo con la finalidad de clasificarlos y priorizarlos según su impacto, por último es necesario que se generen planes de acción o planes de contingencia para mitigar o eliminar los riesgos identificados en caso de que sucedan. Esto principalmente, cuando se pone en peligro la continuidad de las operaciones normales de la universidad como consecuencia de la ocurrencia de un evento.

Una adecuada gestión de riesgos permite asegurar la continuidad de los servicios tecnológicos de la organización. En el presente trabajo, se han aplicado normativas y estándares nacionales e internacionales como ISO 31000 Gestión del Riesgo. Principios y Directrices; ISO/IEC 27005 Gestión del Riesgo en la Seguridad de la Información; ISO 22301 Gestión de la Continuidad de Negocio; el *"Modelo de Evaluación Institucional de Universidades y Escuelas Politécnicas"* elaborado por el CEAACES [4]; las normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos

expedidas por la Contraloría General del Estado [3], entre otros. Cada una de estas normativas especifica los requisitos para implementar o adoptar buenas prácticas que permitan mantener un sistema para gestionar la seguridad de los servicios de TI y mitigación de riesgos, con el objetivo de que se protejan los procesos y los activos de la institución en caso de ocurrir incidentes que provoquen interrupciones en las actividades.

Este proyecto de titulación se desarrolla en seis capítulos que enfocan: Generalidades, marco conceptual, definición del proceso de gestión del riesgo operativo para el factor tecnología y seguridad de la información, aplicación del proceso de gestión del riesgo, plan de acción para controlar los riesgos identificados y resultados obtenidos de la aplicación del proceso de gestión de riesgos.

En el primer capítulo, Generalidades, se plantean los antecedentes, la descripción del problema, la solución propuesta, los objetivos generales y específicos y la metodología de desarrollo del proceso de gestión de riesgos tecnológicos y de seguridad de la información.

En el segundo capítulo, se plantean las definiciones que constituyen el marco conceptual relacionado a la gestión del riesgo operativo en el nivel de tecnología y seguridad de la información, así como el marco regulatorio nacional e internacional aplicado en el desarrollo de este estudio.

En el tercer capítulo, se conoce el contexto de la organización; se recopila la información con el objeto de definir el proceso de gestión del riesgo operativo para el factor tecnología y seguridad de la información; se desarrolla la metodología o proceso a seguir en donde se responde ¿cómo hacerlo?, ¿con qué instrumentos?, ¿cómo se procesará y analizará la información?; se determina la matriz de riesgo operativo y sus criterios de evaluación de riesgo.

En el cuarto capítulo, se describe el procedimiento para la aplicación del proceso de gestión del riesgo, se analiza la información y el diagnóstico de los procesos críticos, se identifican y valoran los riesgos de tecnología de la información y se elabora el mapa de riesgos.

En el quinto capítulo, se diseñan los planes de acción para controlar los riesgos identificados por actividad a fin de mitigarlos, según los procesos

críticos de la universidad e implementación de actividades de monitoreo de estos controles.

Finalmente, en el sexto capítulo, se detallan los resultados obtenidos de la aplicación del proceso de gestión de riesgos de TI, sus efectos e impactos generados en la institución.

Adicionalmente, se adjuntan las referencias bibliográficas consultadas para la realización del presente proyecto y los anexos elaborados.

CAPÍTULO 1

1. GENERALIDADES

1.1 Antecedentes

El marco legal que regula las actividades de las instituciones de educación superior son: la Constitución [2], Ley Orgánica de Educación Superior (LOES) y su Reglamento [1], Código Orgánico de Planificación y Finanzas Públicas, y las Normas de Control Interno expedidas por la Contraloría General del Estado [3].

La Disposición Transitoria constitucional vigésima establece que en el plazo de cinco años a partir de la entrada en vigencia de la Constitución, todas las instituciones de educación superior, así como sus carreras, programas y posgrados deberán ser evaluados

y acreditados conforme a la ley. En caso de no superar la evaluación y acreditación, quedarán fuera del Sistema de Educación Superior [2].

El artículo 95 de la Ley Orgánica de Educación Superior (LOES), señala entre otros que *"La Acreditación es una validación de vigencia quinquenal realizada por el Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior, para certificar la calidad de las instituciones de educación superior, de una carrera o programa educativo, sobre la base de una evaluación previa (…)"* [1].

El artículo 96 del cuerpo legal antes mencionado, dispone que: *"El Aseguramiento de la Calidad de la Educación Superior, está constituido por el conjunto de acciones que llevan a cabo las instituciones vinculadas con este sector, con el fin de garantizar la eficiente y eficaz gestión, aplicables a las carreras, programas académicos, a las instituciones de educación superior y también a los consejos u organismos evaluadores y acreditadores"*.

El Consejo de Evaluación, Acreditación y Aseguramiento de la Calidad de la Educación Superior (CEAACES), ejerce la rectoría de la política pública para el aseguramiento de la calidad de la educación superior del Ecuador a través de procesos de evaluación, acreditación y categorización en las instituciones de educación superior, en concordancia con el numeral 2, artículo 353 de la Constitución del Ecuador [2].

El *"Modelo de Evaluación Institucional de Universidades y Escuelas Politécnicas"*, elaborado en septiembre de 2015 por el CEAACES, define criterios y subcriterios de calidad de la educación superior mediante atributos que son medidos a través de indicadores.

Este modelo define el criterio "Organización", que considera los procesos para establecer, monitorizar y evaluar la consecución de los objetivos; dentro de este criterio se establece el subcriterio "Gestión de la calidad" con el fin de evaluar políticas, mecanismos, recursos y procedimientos para promover una cultura de calidad; y, un indicador cualitativo denominado "Sistema de información" como mecanismo para garantizar la disponibilidad de información suficiente, exacta, oportuna y asequible para los miembros

involucrados y constituye un elemento fundamental de la planificación y de la toma de decisiones.

Además, se incluye el criterio “Recursos e infraestructura”, que propone entre otros evaluar las características de las tecnologías de la información determinando que sean adecuadas para garantizar el desarrollo de las actividades de la comunidad académica; en el mismo se establece el subcriterio “Tecnologías de la información y comunicación” para analizar los sistemas, plataformas y herramientas tecnológicas; y, los indicadores “Conectividad” tendiente a garantizar la conectividad a la internet y “Plataforma de gestión académica” para asegurar la disponibilidad, confiabilidad y transparencia de los resultados y la información obtenidos del sistema informático y procesos de gestión académicos [4].

Las normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos expedidas por la Contraloría General del Estado, sirven como marco de referencia para que las instituciones del Estado establezcan y pongan en funcionamiento su propio control interno; también señala que: *“El control interno está*

orientado a cumplir con el ordenamiento jurídico, técnico y administrativo, promover eficiencia y eficacia de las operaciones de la entidad y garantizar la confiabilidad y oportunidad de la información, así como la adopción de medidas oportunas para corregir las deficiencias de control".

En el numeral 300. Evaluación de riesgos de las normas de control interno antes indicadas, menciona entre otros que: *"… la máxima autoridad, el nivel directivo y todo el personal de la entidad serán responsables de efectuar el proceso de administración de riesgos, que implica la metodología, estrategias, técnicas y procedimientos, a través de los cuales las unidades administrativas identificarán, analizarán y tratarán los potenciales eventos que pudieran afectar la ejecución de sus procesos y el logro de sus objetivos"* [3].

Las instituciones de educación superior podrían estar expuestas a pérdidas significativas de información al no realizar una adecuada gestión de riesgos en las actividades y procesos críticos de la plataforma que soporta la gestión académica, afectando a la disponibilidad, confiabilidad, integridad y transparencia de los

resultados y la información obtenida; y, a la consecución de los objetivos institucionales.

Esta situación obliga a que las instituciones de educación superior implementen un proceso para gestionar los riesgos tecnológicos y de seguridad de la información que podrían afectar a la disponibilidad, confiabilidad, exactitud, transparencia de la información de sus plataformas de gestión académica, asegurando razonablemente el cumplimiento de los criterios, subcriterios e indicadores antes mencionados que son evaluados por el CEAACES y las normas de control interno de la Contraloría General del Estado.

El presente trabajo de titulación se aplica en una institución de educación superior del Ecuador, la cual es una universidad de prestigio y su fin principal es formar profesionales comprometidos con la sociedad, brindar servicios académicos de alta calidad, fomentar la investigación; y, adoptar y generar conocimientos científicos y tecnológicos.

La Dirección de Tecnologías de la Información y Comunicación es la responsable de la administración de la plataforma tecnológica de la universidad y la máxima autoridad ejecutiva está interesada en definir un proceso de gestión de riesgos tecnológicos que permita relevar la matriz de riesgos con principal énfasis en los riesgos tecnológicos y de seguridad de la información, considerando que parte importante del proceso académico se apalanca en la tecnología de la información. Partiendo del hecho de que el proceso de gestión de riesgos es eminentemente preventivo, el área espera disminuir la probabilidad de ocurrencia y el impacto producto de la posible materialización de algún riesgo tecnológico o de seguridad de la información que no se haya gestionado.

1.2 Descripción del problema

Actualmente, el entorno complejo, dinámico y competitivo en el que deben desenvolverse las instituciones, han llevado a que se tecnifiquen y automaticen sus procesos, implementando estrategias que permitan mejorar la calidad de los productos o servicios que ofrecen a la comunidad.

Estos cambios se producen debido a las exigencias del entorno, los nuevos modelos organizacionales, los requisitos establecidos por los usuarios, los cambios regulatorios impuestos por las entidades de control que buscan generar valor agregado a los productos y servicios mejorando su calidad; sin embargo, todo cambio por menor que sea, siempre implica un riesgo; por lo que existe la necesidad de garantizar la disponibilidad y operatividad de los servicios que demanda la comunidad académica, evitando interrupciones y escenarios que puedan ocasionar pérdidas o afectar la reputación de la institución.

Para las instituciones de educación superior, existe la necesidad de mantener la continuidad de los servicios tecnológicos, como los sistemas informáticos que son herramientas que facilitan la gestión académica. Su importancia radica en que estos sistemas permiten soportar los principales procesos de la universidad relacionados con matriculación, planificación académica, calificaciones, promociones, entre otros; permitiendo que sus servicios funcionen correctamente tanto para los usuarios internos como externos.

Actualmente, en la institución no se encuentran definidos formalmente los procesos tecnológicos y de seguridad que se encuentran bajo la responsabilidad de la Dirección de Tecnologías de la Información y Comunicación, lo que dificulta identificar los riesgos tecnológicos que podrían tener estos procesos así como la falta de ejecución de los mismos.

En el año 2016 han ocurrido eventos de riesgo tecnológico que se materializaron y la última vez provocaron pérdida de información de la plataforma de gestión académica por lo que se tomaron medidas reactivas para restaurar la información de algunos días, afectando la productividad del personal docente. Además, existen ciertos reportes gerenciales con errores en la plataforma de gestión académica, mismos que son corregidos de forma manual en la base de datos, incrementando el riesgo tecnológico y de seguridad.

Para disminuir los incidentes de tecnología, eventos de fallas de equipos u otros siniestros que puedan dañar los servicios tecnológicos, es necesario que se realice un análisis y evaluación de riesgos, a los que se exponen todos los servicios informáticos e

infraestructuras y comunicaciones tecnológicas, con el objetivo de mitigar o eliminar la presencia de estos riesgos.

1.3 Solución propuesta

El presente trabajo de titulación tiene como fin principal implementar un proceso de gestión de riesgos operativos, que pueda ser aplicado al factor tecnología de la información que permita disminuir la exposición a los riesgos tecnológicos y de seguridad de la información, asegurando razonablemente el cumplimiento de los indicadores referentes a: sistema de información, conectividad y plataforma de gestión académica evaluados por el CEAACES, así como a las normas de control interno de la Contraloría General del Estado relacionadas a la evaluación de riesgos y a las mejores prácticas internacionales.

Por lo antes indicado, surge la necesidad de desarrollar e implementar un proceso para la gestión del riesgo tecnológico y seguridad de la información, que permita identificar, medir, controlar y monitorear el riesgo, para mitigar la probabilidad e impacto de posibles eventos que pueden afectar las actividades de los

procesos que son soportados en la plataforma de gestión académica.

Se elaboró una matriz de riesgos tecnológicos que incluye los riesgos de seguridad de la información, basada en información histórica de los principales eventos de riesgo que han generado pérdidas así como un análisis de los mismos para los principales procesos críticos soportados en la plataforma de gestión académica; y, con ello proponer planes de acción con controles que ayuden a prevenir, detectar o corregir dichos eventos.

El estudio inició con la revisión de información bibliográfica para el desarrollo del marco conceptual de la gestión del riesgo operativo, así como de acuerdos, leyes y normativas vigentes nacionales e internacionales relacionadas con la gestión de este tipo de riesgo para fundamentar y diseñar el proceso propuesto, tales como: ISO 31000 Gestión del Riesgo. Principios y Directrices; ISO/IEC 27005 Gestión del Riesgo en la Seguridad de la Información; Modelo de Evaluación Institucional de Universidades y Escuelas Politécnicas del CEAACES; Normas de control interno expedidas por la Contraloría General del Estado, entre otros.

El proceso propuesto consta de las siguientes fases:

1. Identificación
2. Medición
3. Control
4. Monitoreo

Posteriormente, en la institución de educación superior, se analizó y recopiló información para la implementación del proceso de gestión de riesgos tecnológicos y de seguridad de la información de la plataforma de gestión académica, mediante la técnica de encuestas y entrevistas al personal involucrado en los procedimientos del área de TI, a los jefes de las unidades administrativas y a la máxima autoridad ejecutiva de la institución y con la observación directa, partiendo del inventario de procesos críticos y activos de información de la universidad.

Además, se recopiló la siguiente información inicial:

- Carta de aceptación por parte de la máxima autoridad ejecutiva de la institución.
- Mapa de procesos.

- Organigramas.
- Inventario de procesos soportados en la plataforma de gestión académica, así como su clasificación.
- Inventario de activos de información asociados a los procesos soportados en la plataforma de gestión académica.

Los resultados obtenidos en el proyecto, fueron:

- Definición formal del proceso de gestión de riesgos tecnológicos y de seguridad de la información alineado al plan estratégico institucional de excelencia de la institución.
- Matriz y mapa de riesgos tecnológicos y de seguridad de la información, identificados en los procesos más importantes.
- Propuesta del plan de acción de controles para la mitigación de los riesgos identificados, incluido el presupuesto inicial tentativo para su implementación.
- Definición de las actividades para el monitoreo de la ejecución de controles que permiten constatar su aplicación.

1.4 Objetivo general

Implementar un proceso para la identificación, medición, control y monitoreo del riesgo tecnológico y de seguridad de la información, que permita prevenir y reducir niveles de pérdida por la materialización de estos riesgos en la institución de educación superior, mediante la aplicación de normativas y estándares nacionales e internacionales.

1.5 Objetivos específicos

- Conocer los conceptos y definiciones referentes a la gestión del riesgo tecnológico, conforme a estándares, normas y leyes nacionales e internacionales.
- Definir un proceso para la gestión del riesgo tecnológico y de seguridad de la información, que incluya las etapas de administración y control de este tipo de riesgos.
- Implementar el proceso de gestión de riesgos para identificar y medir los riesgos que pudieran llegar a generar pérdidas financieras en la institución, por daños en la infraestructura tecnológica o violaciones a la seguridad informática que afecten

a la confiabilidad y disponibilidad inmediata de información relevante.

- Elaborar un plan de acción que defina controles que permitan tratar adecuada y eficientemente los riesgos identificados y elevarlo a conocimiento de la máxima autoridad ejecutiva de la institución, para su posterior aprobación.
- Establecer los mecanismos de monitoreo que permitan la retroalimentación a la gestión de los riesgos y aseguren razonablemente la ejecución de los controles que mitigan los riesgos tecnológicos y de seguridad de la información.

1.6 Metodología

El presente trabajo corresponde a la modalidad de investigación de proyecto factible, pues tiene como objetivo la ejecución de una propuesta, define el proyecto factible como "*un estudio que consiste en la investigación, elaboración y desarrollo de una propuesta de un modelo operativo viable para, requerimientos o necesidades de organizaciones o grupos sociales*" [5].

En el desarrollo de este trabajo se emplearon técnicas cualitativas para la compresión y descripción de los procesos críticos del negocio ubicándolos como parte del conocimiento del contexto real de la organización, además se utilizaron técnicas como la observación, entrevistas y la recopilación documental [6, 7].

El método de la observación científica, fue utilizado como un instrumento de análisis, que permitió describir los procesos de la universidad y entender las actividades y el comportamiento de las personas que laboran en la institución según el cargo que desempeñan, obteniendo datos confiables correspondientes a conductas, eventos y/o situaciones perfectamente identificadas e insertas en el contexto laboral analizado. Esta técnica permite conocer la realidad mediante la percepción directa de los objetos y fenómenos identificados y analizados.

Para la recopilación de la información se utilizó la técnica de entrevistas, para lo cual, se diseñaron cuestionarios dirigidos a diferentes colaboradores de la institución, según sus funciones, y posteriormente se analizaron y validaron dichos resultados con los obtenidos en la observación.

Estos instrumentos permitieron recolectar información específica para la elaboración de la matriz y mapa de riesgos tecnológicos de los procesos críticos identificados en la universidad, así como también, la recopilación de información sobre los factores externos e internos que inciden en el uso de las tecnologías de información y comunicación del personal.

Los cuestionarios que se utilizaron en las entrevistas fueron diseñados con 10 preguntas entre abiertas y cerradas, que estaban relacionadas con los objetivos planteados en este proyecto, las entrevistas fueron realizadas en forma directa e individual al personal responsable de los procesos críticos soportados en la plataforma de gestión académica, un total de 8 colaboradores, entre ellos: coordinador de gestión del rectorado, director de tecnologías, secretaría académica, director de carrera, decano de facultad, desarrollador de software, asistente de tecnologías y responsable de infraestructura tecnológica.

La recopilación documental, fue desarrollada mediante la selección de información fundamentada en la investigación bibliográfica, de campo, descriptiva y explicativa del tema en estudio, lo cual permitió ampliar el conocimiento, usando fuentes primarias y secundarias de información. Se consultó sobre normas y estándares nacionales e internacionales como ISO 31000 Gestión del Riesgo. Principios y Directrices; ISO/IEC 27005 Gestión del Riesgo en la Seguridad de la Información; ISO 22301 Gestión de la Continuidad de Negocio; Modelo de Evaluación Institucional de Universidades y Escuelas Politécnicas del CEAACES; Normas de control interno expedidas por la Contraloría General del Estado, entre otros.

Finalmente, como metodología de desarrollo se definieron las siguientes fases:

Tabla 1. Metodología de desarrollo del proceso de gestión de riesgos

Fases	Actividades
Fase 1:	Planteamiento del proyecto: Generalidades y marco conceptual.
	Desarrollo del proceso para la gestión de riesgo operativo: tecnologías y seguridad de la información.
Fase 2:	Levantamiento de información de los procesos soportados en la plataforma gestión académica.
	Identificación y análisis de procesos importantes.

Fases	Actividades
Fase 3:	Elaboración de matriz y mapa de riesgos tecnológicos.
Fase 4:	Elaboración de propuesta de plan de acción.
Fase 5:	Documentación de procedimientos.

CAPÍTULO 2

2. MARCO CONCEPTUAL

2.1 Administración de riesgos

El propósito de la administración de riesgos es garantizar la supervivencia de la institución, minimizando los costos asociados con los riesgos, siendo el riesgo más común al que se enfrentan las organizaciones: el no cumplimiento de sus objetivos y metas.

La administración del riesgo empresarial (Enterprise Risk Management-ERM) es el proceso que permite a la alta gerencia de una empresa u organización administrar los riesgos a los que está expuesta de acuerdo al nivel de riesgo que están dispuestos a aceptar, según sus objetivos estratégicos.

Es un proceso iterativo que se ejecuta secuencialmente generando una mejora continua en la toma de decisiones. La administración de riesgos es definida también, como un método lógico y sistemático en el que se establece el contexto, identifica, analiza, evalúa, trata, monitorea y comunica los riesgos asociados con una actividad, función, proceso o procedimiento de manera que permita a las organizaciones minimizar pérdidas y maximizar oportunidades.

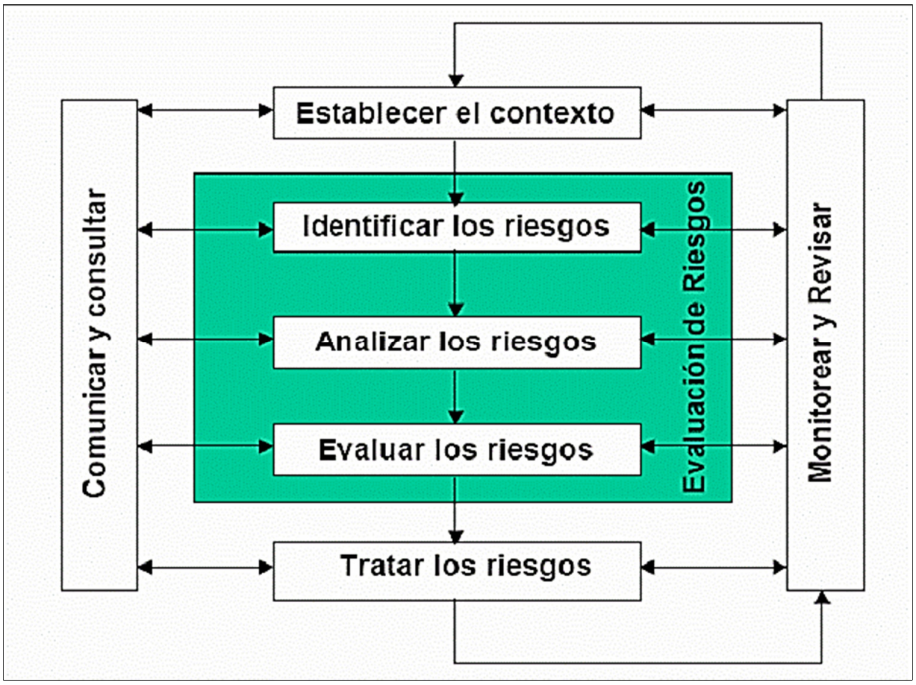


Figura 2.1. Proceso de administración de riesgos

El proceso de administración de riesgos según la norma australiana AS/NZS 4360:2004, establece cómo se debe llevar a cabo el análisis de los diferentes riesgos que potencialmente podrían afectar a la institución, sus procesos, infraestructura o cualquier actividad en general [8].

El impacto de la administración de riesgos relacionada con las tecnologías, se la puede definir como la posibilidad de que ocurra un evento vinculado con TI y que afecta significativamente con la consecución de los objetivos del negocio.

La máxima autoridad ejecutiva de la institución debe asegurar que se cumplan los objetivos de la universidad, dirigiendo y administrando las actividades de TI, obteniendo un balance efectivo entre el manejo de riesgos y los beneficios encontrados. Para esto, se necesita identificar las actividades y procesos más importantes o críticos que deben ser ejecutados sin interrupciones, los mismos que permiten el progreso hacia el cumplimiento de las metas y objetivos determinando su nivel de dependencia con los procesos de TI.

El proceso de administración de riesgos tecnológicos conlleva a identificar los riesgos potenciales a los que está expuesta la infraestructura de TI de la universidad. Una vez identificados son inventariados y analizados según el impacto potencial que tienen sobre el funcionamiento de los procesos y la forma en que estos podrían ser afectados. La administración de riesgos tecnológicos es evitar que por situaciones derivadas del uso de la tecnología se produzcan pérdidas económicas, impacto social, daño ambiental o afectación de las operaciones de la institución.

Finalmente, entre los beneficios que genera una eficiente administración de riesgos, tenemos:

- Facilita el logro de los objetivos de la institución.
- Hace a la organización más segura y consciente de sus riesgos.
- Mejora continua del sistema de control interno.
- Optimiza la asignación de recursos.
- Aprovechamiento de oportunidades.
- Fortalece la cultura de autocontrol.
- Mayor estabilidad ante cambios del entorno.
- Prioriza y establece niveles de riesgo para las actividades, procesos y recursos críticos.

- Pasa de un enfoque de mitigar el riesgo a prevenir proactivamente las fallas.
- Prepararse adecuadamente para las auditorías de los entes de control.

2.1.1 Definición de riesgos

El riesgo constituye una falta de conocimiento sobre futuros eventos o acontecimientos adversos que podrían afectar el cumplimiento de los objetivos. También se puede referir a riesgo cuando la consecuencia sea positiva para el cumplimiento del objetivo, algunos autores lo definen como oportunidad [9].

El **riesgo** se define como el grado de incertidumbre sobre la ocurrencia de un evento que pueda interrumpir el normal desarrollo de las funciones de una institución y afectar el logro de sus objetivos.

También puede definirse como la combinación de la probabilidad de que se produzca un evento y sus consecuencias negativas. Los factores que lo componen son la amenaza y la vulnerabilidad.

La **amenaza** es la posibilidad de ocurrencia de cualquier tipo de evento o acción que puede producir un daño (material o inmaterial) sobre los elementos de un sistema. Es un peligro que está latente, pero que todavía no ocurre, y que sirve como aviso para prevenir la posibilidad de que suceda.

La **vulnerabilidad** son las características y las circunstancias de una organización, sistema o bien que los hacen susceptibles a los efectos dañinos de una amenaza (grado o nivel de destrucción). Es la capacidad y posibilidad de un sistema de responder o reaccionar a una amenaza o de recuperarse de un daño.

Las vulnerabilidades están en directa interrelación con las amenazas porque si no existe una amenaza, tampoco existe la vulnerabilidad o no tiene importancia, porque no ocasiona ningún daño.

Riesgo = Amenaza x Vulnerabilidad, ó

Riesgo = Probabilidad x Impacto.

El **riesgo inherente** es el riesgo intrínseco de cada actividad, sin tener en cuenta los controles que se hayan implementado en la institución. El riesgo inherente es propio del trabajo o proceso, que no puede ser eliminado del sistema; es decir, en todo trabajo o proceso se encontrarán riesgos para las personas o para la ejecución de la actividad en sí misma.

El **riesgo residual** es aquel riesgo que subsiste, después de haber implementado controles. El riesgo residual refleja el riesgo remanente una vez que se han implementado de manera eficaz las acciones planificadas por la alta administración para mitigar el riesgo inherente.

El **riesgo tecnológico** es la pérdida por daños, interrupción, alteración o fallas derivadas del uso o dependencia de tecnologías de la información en la prestación de los servicios de tecnologías de la información y comunicación.

Es importante mencionar que el nivel de riesgo al que está expuesto una organización, no puede ser eliminado en su totalidad. Por lo que, se debe buscar un equilibrio entre el nivel de recursos y mecanismos que es preciso dedicar para minimizar o mitigar los riesgos y un cierto nivel de confianza que se puede considerar suficiente (nivel de riesgo aceptable).

2.1.2 Importancia de la administración de riesgos en instituciones públicas

En toda organización es necesario disponer de una herramienta que garantice la correcta evaluación de los riesgos, a los que están expuestos los procesos, procedimientos y actividades que soportan las tecnologías

de la información; y, que a través de operaciones de control, se pueda evaluar el desempeño y seguridad del entorno informático.

El uso de la tecnología es una de las estrategias más comunes utilizadas por cualquier tipo de organización, lo que ha incrementado la dependencia del uso de información y canales electrónicos dentro de las instituciones. Esto, ha permitido que la tecnología deje de ser un elemento pasivo y se convierta en un activo importante para la operación de los procesos organizacionales, tal como se muestra en la figura 2.2. [10,11].

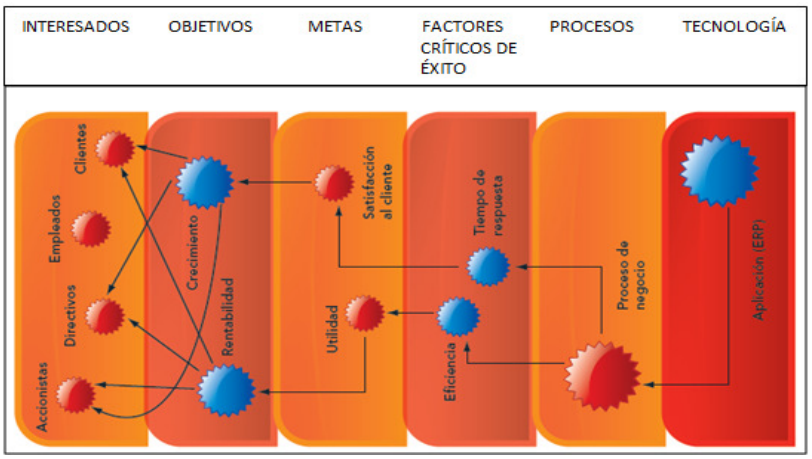


Figura 2.2. Relación de la TI con los procesos organizacionales

Es así, que la tecnología es parte de los procesos institucionales y su funcionamiento no puede aislarse de los demás elementos del proceso.

Para una institución de educación superior es importante mejorar su calidad para sobresalir dentro de las instituciones de su tipo, siendo un factor importante para este objetivo la implantación de nuevas estrategias, técnicas y herramientas que permitan mejorar aspectos como: planeación, administración, gestión y operación, tecnología, entre otros.

Uno de los principales problemas dentro del entorno informático es que existe una inadecuada gestión de riesgos tecnológicos, por lo que se definen los siguientes aspectos que ayudan a mejorar la administración de riegos:

- La evaluación de los riesgos inherentes a los procesos informáticos.
- La evaluación de las amenazas o causas de los riesgos.

- Los controles utilizados para minimizar las amenazas de los riesgos.
- La asignación de responsables a los procesos informáticos.
- La evaluación de los elementos del análisis de riesgos.

La participación de los interesados (“stakeholders”), es importante para obtener un mayor beneficio en relación a la gestión de los riesgos tecnológicos, pues la mayoría de sus actividades son ejecutadas sólo por personal de TI. Para cumplir con el objetivo deseado es necesario que todos los involucrados en los procesos administrativos de la institución participen en la gestión de los riesgos [11].

El riesgo tecnológico debe ser considerado por todos los involucrados, lo cual permitirá realizar un análisis más eficiente sobre el impacto que pueda tener y la probabilidad de ocurrencia dentro de los procesos y con ello lograr un mayor conocimiento para su administración.

Existen ciertos riesgos asociados al uso de las TI dentro del entorno organizacional, estos pueden ser daños causados en forma accidental o intencional por los empleados, o también debido a intentos deliberados de intrusos que desean acceder a los datos de la institución de forma ilegal para sacar provecho o causar daño a la información.

En esa situación, la institución puede llegar a quedar seriamente comprometida con su activo más valioso que es la información. Es por ello, imprescindible contar con estrategias y herramientas que permitan evaluar y reconocer todos los riesgos asociados con el uso de las TI, con el objetivo de minimizar tales riesgos.

Es importante, que se realice un análisis del contexto de la institución que permita conocer su situación y los riesgos típicos que se presentan en el uso de las TI, es decir, cuáles son las amenazas más frecuentes.

Dentro de los principales riesgos tecnológicos, se incluyen el error humano, que es identificado como la principal amenaza en los sistemas tecnológicos, por lo que es necesario contar con parámetros bien definidos en los procedimientos de seguridad, los mismos que deben ser ejecutados sigilosamente por los empleados, de lo contrario se podría llegar a perder información valiosa para la universidad.

Ante esta situación, surge la necesidad de conocer ¿cuáles son los tipos de riesgos o eventos a los que está expuesta la institución?; pues no existe una respuesta específica para esta pregunta, esto depende de sus características, del contexto en el que se desenvuelve, del tipo de tecnología que esté utilizando y de los procesos a los que esté soportando. Sin embargo, existen algunos criterios o guías que se pueden utilizar sobre los riesgos tecnológicos, como la proporcionada por el ITGI (Information Technology Governance Institute), descritos en la tabla 2 [12,13].

Tabla 2. Guía de riesgos de la ITGI

Clasificación del riesgo	Descripción
Seguridad y acceso	Información confidencial o sensitiva disponible a personas que no tienen la autorización apropiada para obtenerla.
Integridad	Información no confiable, ya sea porque no está autorizada, está incompleta o es inexacta.
Pertinencia	No obtener la información correcta para los procesos, en el tiempo preciso para tomar las acciones apropiadas.
Disponibilidad	Imposibilidad de acceder a un servicio.
Infraestructura	La organización no cuenta con la infraestructura tecnológica que soporte de manera efectiva las necesidades actuales y futuras del negocio.

Estos riesgos están completamente relacionados con la tecnología y su impacto puede ser directo para la organización, como ya se mencionó: la tecnología es un factor importante para la operación normal de la institución.

2.1.3 Riesgos en instituciones de educación superior

En el proceso de administración de riesgos es necesario conocer los riesgos inherentes a los que se exponen este

de tipo de instituciones, así como aquellos que pueden ser asumidos y controlados; sin embargo, siempre existirá la posibilidad de que estos se materialicen aunque se encuentren controlados (fallas o insuficiencias en los procesos, personas, sistemas internos, tecnología, eventos externos imprevistos, entre otros). Es necesario conocer y aplicar un correcto y óptimo criterio para la transferencia de riesgos a compañías que puedan administrar estos peligros sabiendo qué y cómo transferir; este proceso es parte fundamental para una buena administración de riesgos.

En el numeral 300 Evaluación del Riesgo, del acuerdo No. 039-CG de 14 de diciembre de 2009 referente a las *"Normas de Control Interno para las Entidades, Organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos"*, se indica entre otros lo siguiente: *"La máxima autoridad establecerá los mecanismos necesarios para identificar, analizar y tratar los riesgos a los que está expuesta la organización para el logro de sus objetivos"*. Además, se detallan las fases para

la gestión del riesgo, las mismas que son: identificación, valoración, plan de mitigación y respuesta al riesgo.

2.2 Riesgo operativo

2.2.1 Definición de riesgo operativo

El riesgo operativo es la posibilidad de que se ocasionen pérdidas financieras debido a fallas en los procesos, personas, sistemas internos y a causa de acontecimientos externos [14].

El riesgo operativo incluye el riesgo legal pero excluye la posibilidad de pérdidas originadas por cambios inesperados en el entorno político, económico y social así como los riesgos estratégicos y de reputación [14].

El riesgo tecnológico es un componente clave del riesgo operacional, principalmente en las instituciones altamente automatizadas y que dependen en gran medida de la tecnología de la información para mantener en operación

los procesos críticos, tal como se señaló en 2.1.2. En este contexto, el riesgo tecnológico se considera un elemento importante para la gestión del riesgo operativo.

2.2.2 Factores de riesgo operativo

Los factores de riesgo operativo son la causa primaria o el origen de un evento de riesgo, y son [14]:

- Procesos: Conjunto de actividades que transforman insumos en productos o servicios con valor para el usuario, sea interno o externo. Se encuentran definidos de conformidad con la estrategia y las políticas de la institución.
- Personas: Es el capital humano que labora en la organización.
- Tecnología de la Información: Conjunto de herramientas y métodos empleados para llevar a cabo la administración de la información. Incluye el hardware, software, sistemas operativos, sistemas de administración de bases de datos, redes, multimedia, servicios asociados, entre otros.

- Eventos externos: Eventos ajenos al control de la organización, tales como fallas en los servicios públicos, desastres naturales, atentados y otros actos delictivos.

2.2.3 Eventos de riesgo operativo

Basándonos en las fuentes de pérdidas identificadas por el Comité de Supervisión Bancaria de Basilea [14], se han definido los eventos de riesgo operativo que también podrían afectar a las actividades administrativas de una institución de educación superior, los que se detallan a continuación:

- Fraude interno: Errores intencionados en la información sobre registros y calificaciones, robos por parte de empleados, inadecuada utilización de información confidencial, falsificación de calificaciones, falsificación de títulos, destrucción maliciosa de activos, etc.
- Fraude externo: robo, falsificación, perjuicios por intrusión en los sistemas informáticos, etc.
- Relaciones laborales y seguridad en el ambiente de trabajo: solicitud de indemnizaciones por parte de los

empleados, violación a las normas laborales de seguridad e higiene, organización de actividades laborales, acusaciones de discriminación, responsabilidades generales, etc.

- Prácticas con los usuarios, servicios y convenios: abusos de confianza, mal manejo de información confidencial de estudiantes y empleados, etc.
- Daños a activos físicos: terrorismo, vandalismo, pérdidas por desastres naturales, etc.
- Alteraciones en la actividad y fallos en los sistemas: fallas del hardware o del software, problemas en las telecomunicaciones, interrupción de servicios públicos, etc.
- Ejecución, entrega y procesamiento: errores en el ingreso de datos, documentación legal incompleta, acceso no autorizado a las calificaciones de los estudiantes, etc.

2.2.4 Normas y estándares internacionales para la gestión de riesgos: ISO 31000 e ISO 27005

ISO 31000:2009 Gestión del Riesgo – Principios y Directrices

La norma ISO 31000:2009 fue preparada por el Comité ISO, Consejo de gestión técnica del grupo de trabajo sobre la gestión de riesgos.

Esta norma establece principios y directrices genéricas sobre la gestión del riesgo, puede ser utilizada por cualquier tipo de organización ya que no es específica para ninguna industria o sector y no es certificable.

Incluye un marco de referencia como un componente clave para el éxito de la gestión del riesgo, mismo que se muestra a continuación [15].

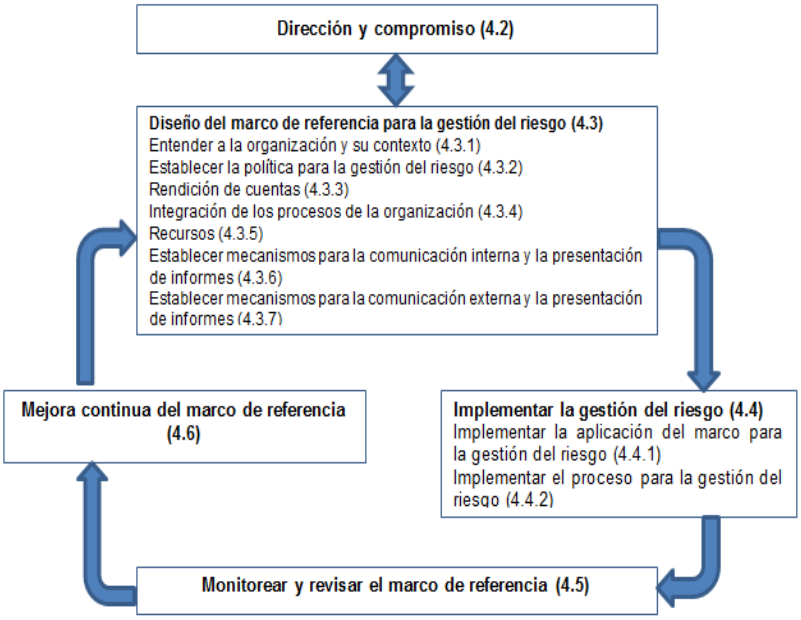


Figura 2.3. Relación entre componentes del marco de referencia

De acuerdo a lo indicado en esta norma, el marco de referencia mostrado debe adaptarse conforme a las necesidades de la institución e incluir:

Dirección y compromiso: La continuidad de la gestión del riesgo requiere el compromiso de la alta dirección, así como de la planificación estratégica y rigurosa para lograr el compromiso a todo nivel.

Diseño del marco de referencia: Es necesario entender el contexto de la organización; establecer la política para la gestión del riesgo; definir los responsables de la rendición de cuentas; incluir la gestión del riesgo en los procesos de la organización; asignar los recursos adecuados; establecer los mecanismos para la comunicación interna y externa; y, la presentación de informes.

Implementar la gestión del riesgo: Implementar el marco de referencia definiendo tiempo, estrategia, aplicarlo en los procesos de la organización, cumpliendo con los requisitos legales y reglamentarios; e implementar el proceso mediante un plan para la gestión del riesgo en todos los niveles y las funciones necesarias.

Monitorear y revisar el marco de referencia: Se debe medir el desempeño, progreso y desviaciones de la gestión del riesgo así como efectuar revisiones para determinar si las acciones realizadas son adecuadas, presentar informes y revisar la eficacia del marco de referencia para la gestión del riesgo.

Mejora continua del marco de referencia: Se deben tomar decisiones para mejorar el marco de referencia, política y plan para la gestión del riesgo.

Además, indica que el proceso para la gestión del riesgo debería ser parte integral de la gestión, estar incluido en la cultura y las prácticas, y estar adaptado a los procesos de negocio de la organización.

El proceso incluye las actividades que se muestran en el siguiente gráfico y que serán detalladas a continuación [15]:

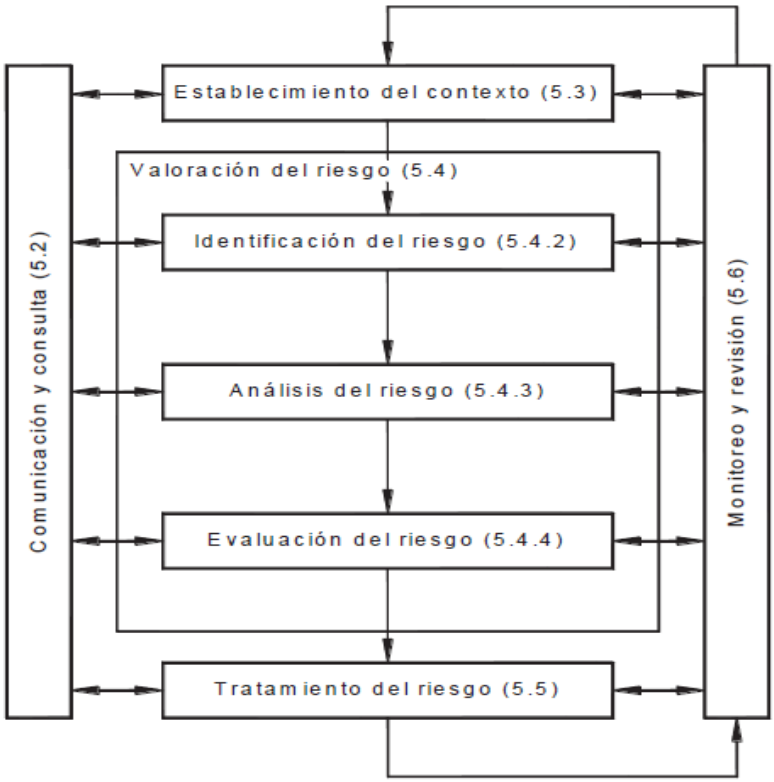


Figura 2.4. Proceso para la gestión del riesgo

Comunicación y consulta: Misma que debe estar presente durante todas las etapas y con las partes involucradas internas y externas, definiendo planes para la comunicación y consulta.

Establecimiento del contexto: Establecer el contexto externo, interno y del proceso para la gestión del riesgo; y, definir los criterios del riesgo.

Valoración del riesgo: Mediante la identificación, análisis y evaluación del riesgo.

Tratamiento del riesgo: Valorar el tratamiento del riesgo; definir el riesgo residual tolerable; valorar la eficacia del tratamiento del riesgo; seleccionar las opciones para el tratamiento del riesgo; preparar e implementar los planes para el tratamiento del riesgo.

Monitoreo y revisión: Monitorear el proceso de gestión del riesgo para garantizar eficacia y eficiencia de los controles, mejorar la valoración del riesgo, analizar y aprender lecciones, detectar cambios en el contexto de la organización e identificar riesgos emergentes.

Registro del proceso para la gestión del riesgo: Mantener trazabilidad de las actividades del proceso para mejorar los métodos y las herramientas, así como del proceso global.

ISO/IEC 27005:2012 Tecnología de la Información – Técnicas de Seguridad – Gestión del Riesgo en la Seguridad de la Información

Esta norma brinda directrices para la gestión del riesgo de la seguridad de la información en una institución, alineándose a los requisitos de un sistema de gestión de seguridad de la información (SGSI) de acuerdo a la norma ISO/IEC 27001. Es aplicable a todas las organizaciones que deseen gestionar los riesgos que pueden comprometer su seguridad de la información.

Establece que la gestión del riesgo de la seguridad de la información debería ser parte integral de todas las actividades de la gestión de la seguridad de la información y se debería aplicar a la implementación y funcionamiento de un SGSI. También señala que debe ser un proceso continuo [16].

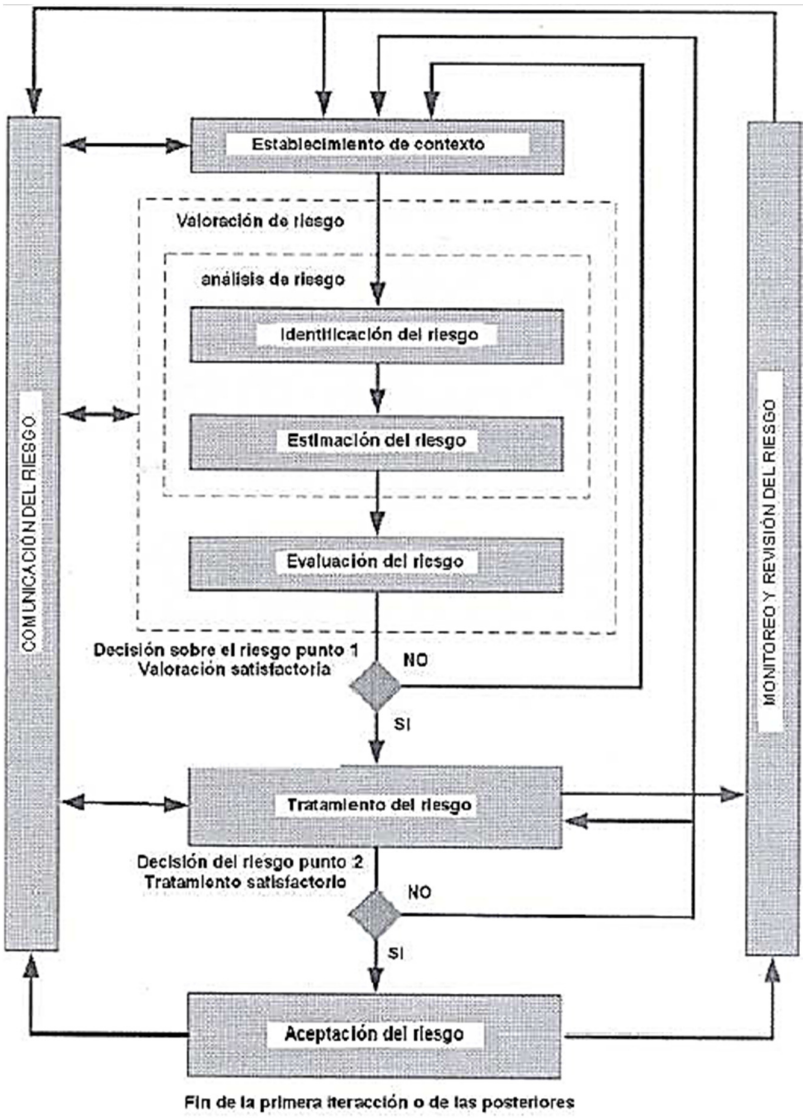


Figura 2.5. Proceso de gestión del riesgo de SI

Como se muestra en la figura anterior, el proceso de gestión del riesgo de seguridad de la información puede ser iterativo.

Primero, se establece el contexto; luego se realiza una valoración del riesgo; si ésta valoración brinda suficiente información para definir las acciones para el tratamiento del riesgo a fin de llevarlo a un nivel aceptable, termina esta actividad y se sigue con el tratamiento del riesgo, caso contrario, se realiza otra iteración de valoración del riesgo.

A continuación, se describe de forma general las actividades del proceso de gestión de riesgos de seguridad de la información conforme a la norma ISO/IEC 27005:2012:

Comunicación del riesgo: Se debería establecer un plan de comunicación interno y externo de los riesgos de seguridad de la información aplicable para todas las etapas del proceso.

Establecimiento del contexto: Conocer la información de la organización para establecer el contexto de la gestión del riesgo de seguridad de la información, estableciendo criterios básicos, de evaluación y aceptación del riesgo de seguridad de la información que son necesarios su gestión;

definir el alcance y límites así como la organización para que opere el proceso.

Valoración del riesgo: Los riesgos se deberían identificar, describir cuantitativa o cualitativamente y priorizarse en función de los criterios de evaluación y los objetivos de la institución.

Tratamiento del riesgo: Se deben seleccionar controles para reducir, retener, evitar o transferir los riesgos así como definir un plan para el tratamiento de los mismos.

Aceptación del riesgo: Se debería tomar formalmente la decisión de aceptar los riesgos y las responsabilidades de esta decisión e indicando la justificación para aquellos que no satisfacen los criterios de aceptación y que hayan sido aceptados.

Monitoreo y revisión: Los riesgos y sus factores deberían ser monitoreados y revisados para identificar cambios en el contexto de la organización y su estado para tener una visión general del riesgo.

2.2.5 Normas de control interno para la evaluación de riesgos de instituciones públicas

En las *"Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos"*, expedidas por la Contraloría General del Estado mediante acuerdo No. 039-CG de 16 de noviembre de 2009, se dispone que *"La máxima autoridad establecerá los mecanismos necesarios para identificar, analizar y tratar los riesgos a los que está expuesta la organización para el logro de sus objetivos (…)"* y detalla las principales actividades para la gestión de riesgos institucionales, que se indican a continuación:

300-01 Identificación de riesgos.- *"Los directivos de la entidad identificarán los riesgos que puedan afectar el logro de los objetivos institucionales debido a factores internos o externos, así como emprenderán las medidas pertinentes para afrontar exitosamente tales riesgos"*.

300-02 Plan de mitigación de riesgos.- *"Los directivos de las entidades del sector público y las personas jurídicas de derecho privado que dispongan de recursos públicos,*

realizarán el plan de mitigación de riesgos desarrollando y documentando una estrategia clara, organizada e interactiva para identificar y valorar los riesgos que puedan impactar en la entidad impidiendo el logro de sus objetivos".

300-03 Valoración de los riesgos.- *"La valoración del riesgo estará ligada a obtener la suficiente información acerca de las situaciones de riesgo para estimar su probabilidad de ocurrencia, este análisis le permitirá a las servidoras y servidores reflexionar sobre cómo los riesgos pueden afectar el logro de sus objetivos, realizando un estudio detallado de los temas puntuales sobre riesgos que se hayan decidido evaluar"*.

300-04 Respuesta al riesgo.- *"Los directivos de la entidad identificarán las opciones de respuestas al riesgo, considerando la probabilidad y el impacto en relación con la tolerancia al riesgo y su relación costo/beneficio"*.

CAPÍTULO 3

3. DEFINICIÓN DEL PROCESO DE GESTIÓN DEL RIESGO OPERATIVO PARA EL FACTOR TECNOLOGÍA Y SEGURIDAD DE LA INFORMACIÓN

3.1 Contexto de la institución de educación superior

La universidad es una institución de educación superior, con personería jurídica de derecho público, con autonomía académica, administrativa, financiera y orgánica, sin fines de lucro, pluralista y abierta a todas las corrientes y formas del pensamiento universal, financiada principalmente por el Estado ecuatoriano y forma del sistema de educación superior ecuatoriano. Fue creada mediante Ley expedida por el Congreso Nacional en la década de los noventa, es decir, casi 20 años de vida institucional.

En el año 2013, el CEAACES mediante resolución administrativa acreditó a la universidad por el periodo de cinco años, al haber cumplido los estándares de calidad establecidos.

La universidad se rige por el siguiente marco normativo:

- Constitución de la República del Ecuador.
- Ley Orgánica de Educación Superior (LOES)
- Reglamento a la Ley Orgánica de Educación Superior
- Código Orgánico de Planificación y Finanzas Públicas
- Normas de Control Interno para las Entidades, Organismos del Sector Público y de las Personas Jurídicas de Derecho Privado que Dispongan de Recursos Públicos.

3.1.1 Misión

Formar profesionales comprometidos con la sociedad, en base a una alta calidad académica, a la investigación, la generación de conocimientos respetando y promoviendo la identidad nacional.

3.1.2 Visión

Ser una institución de educación referente en el Ecuador, por sus competencias académicas de investigación científica y tecnológica y con espíritu innovador y crítico, así como por la responsabilidad social de sus actores internos y externos.

3.1.3 Objetivos estratégicos

- Promover la relevancia y excelencia de los programas de pregrado y posgrado, mediante la calidad de la docencia y la formación de profesionales con sólidas bases científicas, técnicas y humanistas, que respondan a las necesidades de desarrollo local, regional y nacional.

- Fortalecer la investigación para generar conocimiento, a través de proyectos de investigación, producción científica, tecnológica e innovación que contribuyan al desarrollo sostenible de la sociedad y del país.

- Desarrollar programas y proyectos de vinculación con la sociedad, alineados a la docencia e investigación que contribuyan al desarrollo local, regional y nacional.

- Realizar una gestión institucional de calidad y eficiente orientada a fortalecer los procesos académicos y de investigación.

3.1.4 Estructura organizativa

La universidad tiene la siguiente estructura orgánica funcional [17]:

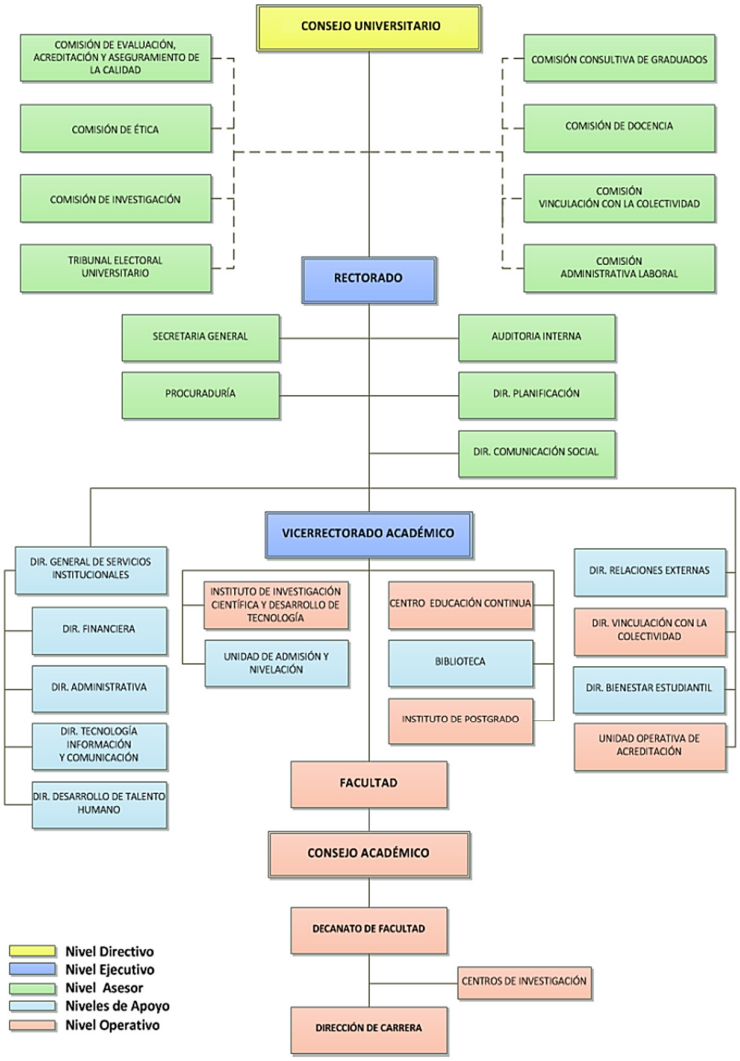


Figura 3.6. Estructura orgánica funcional

El gobierno institucional de la universidad está conformado de la siguiente manera:

Tabla 3. Gobierno de la universidad

Tipo	Organismo/ Autoridad	Descripción
Organismos de Cogobierno	Consejo Superior Universitario	Es el órgano colegiado superior que ostenta la máxima autoridad de la institución, cuya misión será la de analizar, aprobar e implementar políticas y normas para el adecuado desenvolvimiento de las funciones de docencia, investigación, vinculación y gestión administrativa.
	Consejo Académico de Facultad	Es un organismo de cogobierno que decide, dirige y coordina en los ámbitos: académico, de investigación, de gestión e infraestructura de las facultades.
Autoridades Ejecutivas	Rector / Rectora	Es la máxima autoridad ejecutiva de la universidad y su representante legal, judicial y extrajudicial; presidirá el Consejo Superior Universitario. Es responsable de la dirección de la institución en el campo académico, de investigación, administrativo, financiero y de vinculación con la colectividad.
	Vicerrector Académico / Vicerrectora Académica	Tiene como misión: dirigir, coordinar, supervisar y evaluar la gestión académica y de investigación, así como el desarrollo de programas,

Tipo	Organismo/ Autoridad	Descripción
		proyectos y planes de formación profesional de grado y postgrado.
Autoridades Académicas	Decanos/ Decanas de Facultad	Es la autoridad académica de la facultad, responsable de la aplicación y cumplimiento de las directrices y políticas que impartan los órganos superiores.
	Director / Directora del Instituto Investigación Científica y Desarrollo Tecnológico	Es el responsable de proponer, coordinar y ejecutar, los planes, políticas y programas de investigación, ciencia, tecnología e innovaciones de la universidad, así como sobre la adecuada interrelación entre la investigación y la docencia de pregrado y postgrado.
	Director / Directora del Instituto de Posgrado	Es responsable de planificar, supervisar y evaluar, con carácter interdisciplinario e interinstitucional, programas de doctorado (equivalente a Ph.D.), programas de maestría y de especialización, que respondan a las necesidades del desarrollo institucional, de la región y del país.
	Gestores Académicos	Directores de Carrera, Director de Educación Continua, de Vinculación con la Colectividad, de la

Tipo	Organismo/ Autoridad	Descripción
		Unidad Operativa de Acreditación y de los Centros de Investigación de Facultades.

3.1.5 Contexto internacional

La institución ha identificado tendencias a nivel mundial que impactarán la educación superior hasta el 2020, en lo relacionado a:

Político: Macropolíticas que facilitan el intercambio de bienes y servicios y que garantizan la propiedad intelectual, dentro de la Organización Mundial del Comercio (OMC); mayor presencia de los países asiáticos; crisis en países de la Unión Europea; protección del medio ambiente.

Económico: Globalización; bajo crecimiento económico de los países europeos; nueva arquitectura financiera mundial; desarrollo humano sustentable; mayor producción; producción de transgénicos.

Educativo: Educación en línea y aplicación de nuevas tecnologías; redes de universidades mundiales, regionales y nacionales; incremento de la demanda de estudios de cuarto nivel; educación centrada en el aprendizaje y en el estudiante; visión humanística y tecnológica; educación dual (educación-trabajo); mayor autonomía en el aprendizaje de los estudiantes; flexibilidad curricular; aseguramiento de la calidad de la educación; movilidad académica internacional; educación multidisciplinaria y transdisciplinaria.

Científico y tecnológico: Desarrollo de fuentes de energía alternativas renovables; aplicación creciente de la biotecnología y nanotecnología; mayor inversión en investigación, desarrollo e innovación; generación y aplicación de nuevas tecnologías de la información y comunicación; redes universitarias de investigación.

Ambientales: Creciente demanda de productos agrícolas orgánicos; desarrollo y uso de tecnologías limpias para la explotación y manejo de recursos naturales; desarrollo sustentable; manejo adecuado del agua.

3.1.6 Contexto regional

Categorización de las universidades en la región; variación de la demanda de estudios de educación superior; los requerimientos de nuevas carreras afines a los problemas del entorno; repercusión de la tasa de admisión en función del proceso de admisión determinada por la LOES.

3.1.7 Contexto nacional

La institución ha identificado factores a nivel nacional, que influenciarán a la educación superior hasta el 2020, en lo relacionado a:

Político: Gratuidad de la educación pública hasta el tercer nivel; Plan Nacional del Desarrollo y del Buen Vivir; políticas de inclusión social; libre acceso a la información pública (Ley de Transparencia).

Económico: Desarrollo interno; nacionalización de los sectores estratégicos; desarrollo de la infraestructura vial, puertos y aeropuertos; cambio de la matriz productiva; mayor endeudamiento de la población; bioturismo; protección a la producción nacional.

Social: Priorización e incremento de la inversión social por parte del gobierno; regulación para la Inclusión de las personas con capacidades especiales en el mercado laboral; democratización al acceso de los servicios sociales; la responsabilidad social de la educación superior, como un bien público.

Educativo: Bachillerato general unificado; flexibilidad curricular a nivel universitario; alto grado de especialización en la docencia universitaria; aseguramiento de la calidad de la educación; control de las universidades por parte del Estado; movilidad estudiantil; educación centrada en la solución de problemas.

Científicas y Tecnológicas: Prioridad en la investigación; servicios virtuales administrativos y educativos; Ciudad del Conocimiento (Yachay); desarrollo del bioconocimiento.

Ambientales: Derechos de la naturaleza consagrados en la Constitución; reforzamiento de los estudios de impacto ambiental; mantiene el uso indebido de agrotóxicos; explotación de recursos naturales con responsabilidad; optimización del uso del agua para mejorar la huella hídrica

de la producción; remediación de los ríos contaminados por la minería.

3.1.8 Contexto interno

La universidad dentro de su plan estratégico vigente [17], ha definido su análisis situacional mediante la técnica del FODA (fortalezas, oportunidades, debilidades y amenazas), específicamente para la gestión administrativa de los procesos académicos ha determinado lo siguiente:

- Fortalezas: Plataforma informática con servicios en línea a disposición de estudiantes y docentes; acreditación; cultura de planificación y evaluación; sistema informático para planificación institucional; infraestructura administrativa; aplicación informática para la gestión bibliotecaria.
- Oportunidades: Leyes, normas, procedimientos y el Plan Nacional del Buen Vivir permiten alinear los objetivos y postulados de la planificación institucional; avances tecnológicos; facilidad de acceso a redes de comunicación e información.

- Debilidades: Carencia de cultura en atención y servicio; falta de actualización de manual de procesos y procedimientos; falta automatización de procesos académicos y administrativos; reglamentación interna no está en función de normativa nacional; servicio de internet limitado; fallas recurrentes en el sistema de internet y conectividad; carencia de innovación tecnológica; Infraestructura tecnológica no adecuada.
- Amenazas: Normas rígidas impuestas por el Ministerio de Finanzas; fallos electrónicos y fallas eléctricas; inseguridad de la comunicación unificada; inseguridad ciudadana.

3.2 Recopilación de información

La gestión de riesgos tecnológicos y de seguridad de la información se aplicará a los procesos que son soportados por la plataforma de gestión académica de la universidad.

3.2.1 Organigrama de la Dirección de Tecnologías de la Información y Comunicación

A continuación se muestra el organigrama y principales funciones de la Dirección de TIC [18]:

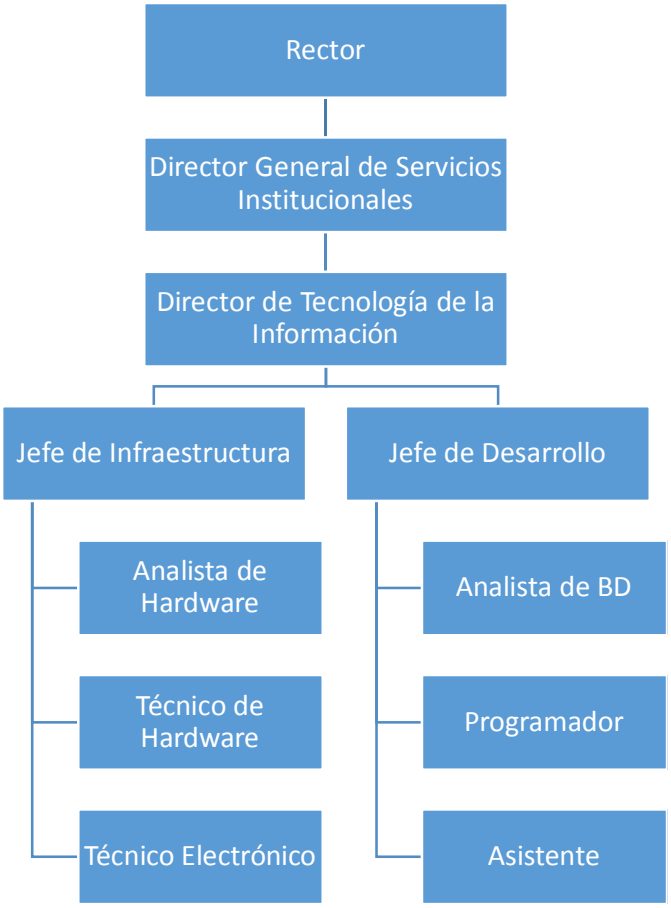


Figura 3.7. Organigrama de la Dirección de TIC

Tabla 4. Principales funciones de la Dirección de TIC

Cargo	Descripción
Director de Tecnología de la Información y Comunicación	Dirigir la ejecución de las actividades de soporte técnico y de mantenimiento de equipos informáticos, tecnologías de la información y comunicaciones; y apoyar en la gestión del sistema de aseguramiento de la calidad de las carreras y programas de educación superior.
Jefe de Infraestructura	Coordinar y supervisar actividades de soporte técnico y de mantenimiento de equipos informáticos, tecnologías de la información y comunicaciones, e informar sobre las mejoras a incorporar en los productos y servicios institucionales.
Analista de Hardware	Ejecutar actividades de soporte técnico y de mantenimiento de equipos informáticos, tecnologías de la información y comunicaciones; e informar sobre las mejoras a incorporar en los productos y servicios institucionales.
Técnico de Hardware y Técnico Electrónico	Ejecutar actividades de soporte técnico y de mantenimiento de equipos informáticos, tecnologías de la información y comunicaciones; e informar sobre

Cargo	Descripción
	las mejoras a incorporar en los productos y servicios institucionales.
Jefe de Desarrollo	Administrar, controlar, gestionar y dirigir soluciones informáticas e informar sobre las mejoras continuas para incorporar en los productos y servicios informáticos institucionales.
Analista de Bases de Datos	Administrar y diseñar las bases de datos institucionales y velar por la seguridad y respaldo de la información.
Programador	Desarrollar, implementar y mantener los sistemas de información.
Asistente	Ejecución y mantenimiento documental de todos los sistemas desarrollados. Soporte a usuarios en sistemas y redes.

3.2.2 Proceso de gestión académica

De las reuniones mantenidas con el personal de la Dirección de Tecnologías de la Información y Comunicación de la institución así como con personal de la Secretaría Académica, se constató que existe un macroproceso

conocido como “gestión académica”, conformado por varios procesos y subprocesos, mismos que se detallan a continuación [18]:

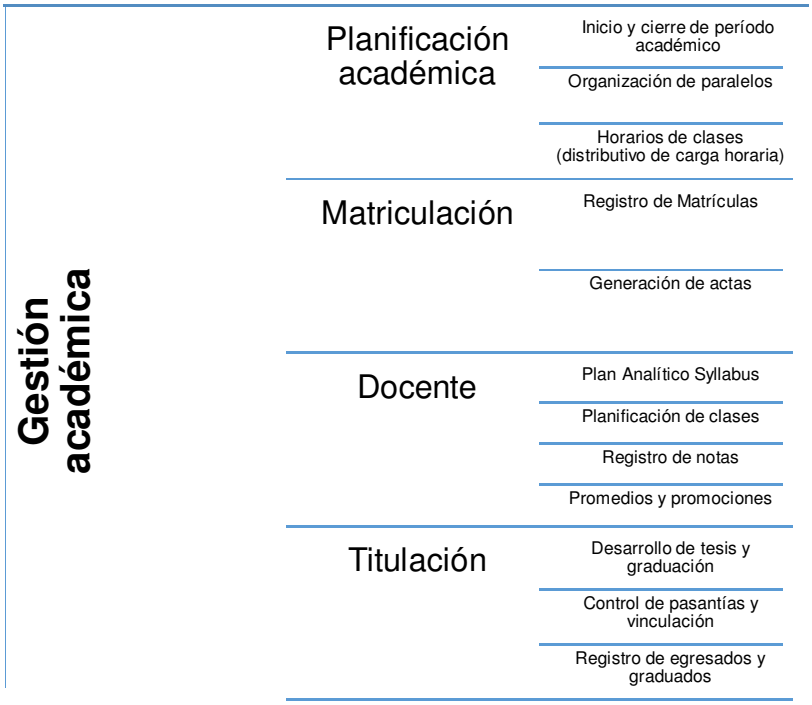


Figura 3.8. Macroproceso de Gestión Académica

3.2.3 Política institucional de gestión de riesgos tecnológicos

A la fecha de este trabajo, no existe una política institucional formalizada para la gestión de riesgos que incluya al riesgo tecnológico y de seguridad de la información.

No obstante de lo antes mencionado, en el plan estratégico institucional [17] se señala que para el eje estratégico denominado “Generación de valor distintivo a través de gestión administrativa” alineado al objetivo estratégico tendiente a realizar una gestión institucional de calidad y eficiente, se indica que para el año 2017 se realizará la formulación e implementación del plan de contingencias y emergencias bajo la responsabilidad de un Comité de Gestión de Riesgos.

Se considera necesario crear una política institucional de gestión de riesgos, misma que debe ser aprobada por el Consejo Universitario.

3.3 Proceso de gestión del riesgo operativo para el factor tecnología

Para definir las etapas del proceso de gestión de riesgo operativo, es necesario relacionar los lineamientos establecidos en las normas ISO 27005 e ISO 31000, que tratan sobre la gestión del riesgo y seguridad de la información.

El proceso de gestión del riesgo de tecnologías y seguridad de la información, que se ha denominado “PGRTI” se define en cuatro fases genéricas que a su vez contienen subprocesos que pueden ser aplicados según el entorno y la actividad que desarrolla la organización.

La fase uno corresponde a la definición y comprensión de la organización y su contexto. La fase dos establece los macroprocesos para la administración de los riesgos de TI. La fase tres especifica los planes de acción para mitigar y gestionar los riesgos identificados, y por último la fase cuatro corresponde al proceso de retroalimentación y mejoramiento de los resultados obtenidos en las fases previas.

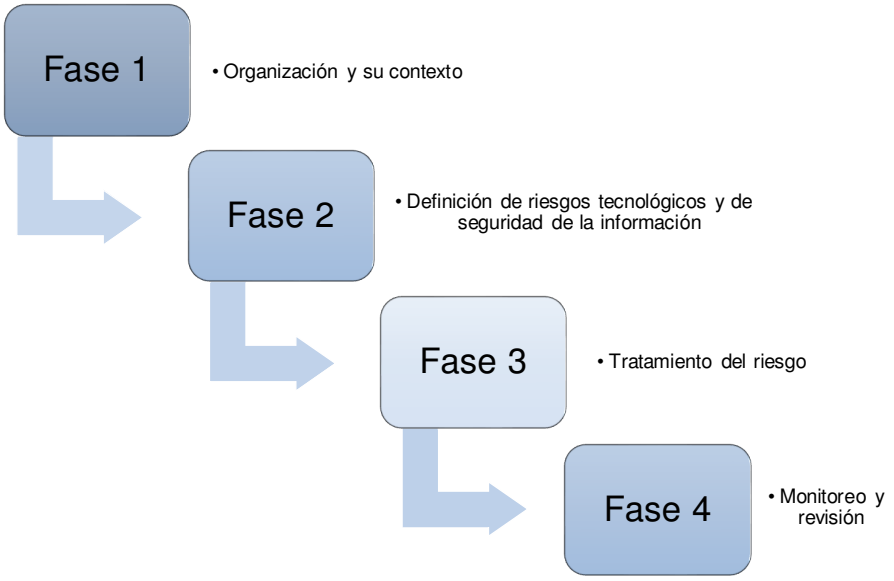


Figura 3.9. Fases del proceso de gestión del riesgo operativo

A continuación se indican las principales características del proceso de gestión de riesgo de tecnología y seguridad de la información.

Tabla 5. Características proceso gestión de riesgos de TI y SI

Logo	Macroproceso: Gestión de Riesgos
	Proceso: Gestión de Riesgo de Tecnología y Seguridad de la Información
	Tipo de proceso: Habilitante o de apoyo
	Código del proceso: PGRTI
Propósito:	Gestionar los riesgos tecnológicos que pudieran llegar a generar pérdidas financieras en la institución, por daños en la infraestructura tecnológica o violaciones a la seguridad informática que afecten a la confiabilidad y disponibilidad inmediata de información relevante.
Entradas (prerrequisitos):	• Inventario de procesos y subprocesos • Inventario de activos de información asociados a

	los procesos.
Recursos:	• Matriz de riesgos de TI
Periodicidad de ejecución:	Al menos una vez al año o cuando existan cambios importantes en la infraestructura tecnológica.
Políticas:	• Se utilizará únicamente el formato de la matriz de riesgos definida en este proceso. • Los informes de cumplimiento de la política serán presentados en el mes de marzo de cada año. • Los niveles de impacto financiero serán determinados por la Dirección Financiera. • Los impactos operativos serán determinados por la Dirección de Planificación. • Cualquier cambio en el proceso, deberá ser aprobado por el Consejo Superior Universitario.
Salidas:	• Matriz y mapa de riesgos tecnológicos. • Plan de acción de controles para la mitigación de riesgos.
Tipo de cliente:	Interno ☒ Externo ☐
Responsables:	• Director de Planificación • Director de Tecnologías de la Información y Comunicación • Dueños de procesos • Auditoría Interna • Consejo Superior Universitario
Marco legal:	"Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos", expedidas por la Contraloría General del Estado mediante acuerdo No. 039-CG de 16 de noviembre de 2009.
Indicador de cumplimiento:	• Matriz de riesgos de TI actualizada. • # controles implementados / # controles aprobados. • # riesgos con umbral menor o igual al máximo tolerado. • # informes de cumplimiento presentados / # informes solicitados.
Excepciones:	No aplica.

Este proceso ha sido dividido en etapas o fases, mismos que se explicarán en este capítulo.

3.4 Definición de las etapas del proceso de gestión del riesgo de tecnologías y seguridad de la información (PGRTI)

Fase 1: entender a la organización y su contexto

Todo proceso de administración del riesgo operativo parte del conocimiento del contexto de la organización, es decir, entender su misión, visión, objetivos, cultura organizacional, organigrama, marco regulatorio que debe cumplir, macro procesos, políticas institucionales, procesos críticos, productos y servicios que brinda.

Lo más importante en esta fase, es entender la interrelación existente entre los procesos institucionales con los riesgos de los activos de TI que soportan la ejecución y funcionamiento adecuado de dichos procesos. Esto debido a que un proceso puede depender de más de una aplicación y a su vez una aplicación puede depender de más de un equipo tecnológico, generando un mayor riesgo en aquellos activos de los que dependen principalmente los procesos críticos.

Figura 3.10. Relación entre la actividad principal y procesos de TI

Debe existir un inventario de los activos de información asociados a cada uno de los procesos, principalmente de aquellos considerados como críticos, indicando: el responsable, custodio, valoración del activo en términos de su integridad, confidencialidad y disponibilidad así como a qué parte de la institución afecta.

En esta fase, el resultado principal es definir un mapa de procesos críticos de la organización en el que se identifiquen dos tipos de riesgos:

Nivel de criticidad por cada proceso institucional: Esta clasificación le sirve a los dueños de los procesos para conocer cómo éstos afectan a la operación de la institución.

Riesgo de TI por cada uno de los activos: La identificación y medición de este riesgo permite a la Dirección de TIC de la institución generar acciones para mitigar los riesgos a los que están expuestos y determinar cuál es la gestión que se debe aplicar.

Logo	**Proceso de Gestión de Riesgo de Tecnología de Información**	**Revisado**	**Código** PGRTI-001
	Fase 1: Entender la organización y su contexto	**Elaborado** Octubre / 2016	**Versión** 1.0

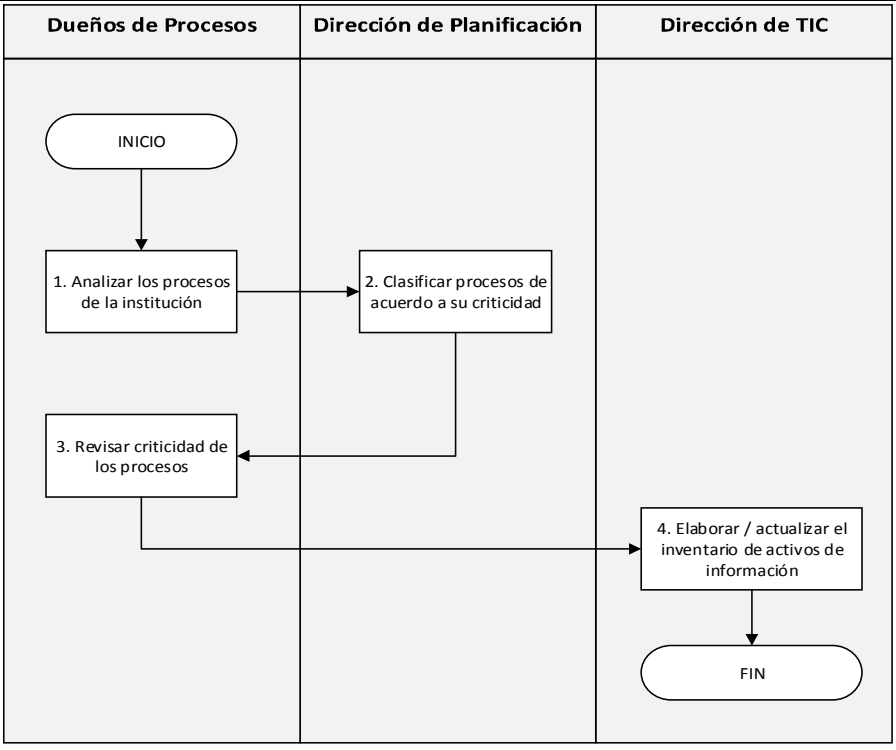


Figura 3.11. Fase 1: Entender la organización y su contexto

Fase 2: definición de riesgos tecnológicos y de seguridad de la información

La fase de definición de riesgos tecnológicos corresponde a un proceso sistemático para determinar el riesgo realizando las siguientes actividades:

a. Identificación de riesgos: determinar a qué amenazas están expuestos los activos relevantes para la organización.
b. Definición de criterios de evaluación del riesgo: es definir los criterios que se considerarán para la evaluación de riesgo, por ejemplo: criticidad del proceso, valoración de activos, niveles de protección actuales, amenazas e impactos.
c. Análisis del riesgo: evaluar el impacto, definido como el daño sobre el activo derivado de la materialización de la amenaza, y determinar qué controles están implementados y su nivel de eficacia frente al riesgo.
d. Evaluación del riesgo: estimar el riesgo, estableciendo el impacto ponderado con la probabilidad de ocurrencia de la amenaza.

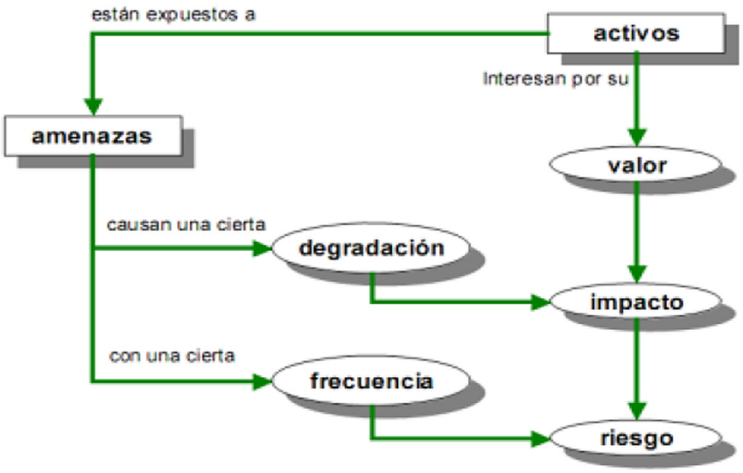


Figura 3.12. Definición de riesgos de TI y SI [19]

a. Identificación de riesgos

Dentro del riesgo operativo, se encuentra el riesgo tecnológico que también es un riesgo de la institución asociado al uso, propiedad, operación, participación, influencia y adopción de la tecnología de la información.

Para poder identificar los riesgos operativos, se debe ejecutar la fase uno, en la que se elabora un inventario de los procesos de la institución agrupados por tipos: gobernantes o estratégicos; productivos; y, habilitantes o de apoyo. Además, se deben

identificar los procesos críticos, es decir, los que son vitales para la continuidad de las operaciones de la organización.

A continuación, se muestran las tablas de categorías para la valoración de activos en términos de seguridad, el nivel de protección que posean así como a qué parte de la institución afectan [20, 21].

Tabla 6. Valor del activo en términos de seguridad

Valor del activo	Descripción
1	Poca pérdida o daño.
2	Pérdida o daño menor.
3	Pérdida o daño medio, los procesos pueden verse afectados negativamente, sin llegar a fallar o causar su interrupción.
4	Pérdida o daño serio o considerable y los procesos pueden fallar o interrumpirse.
5	Altas pérdidas monetarias, daño a un individuo o a la sociedad, imagen, privacidad, y/o proceso. Los procesos dependientes fallarán.

Tabla 7. Niveles de protección del activo

Vulnerabilidad del activo	Valor
Sin protección	0.9
Poca protección	0.7
Protección media	0.5
Protección aceptable	0.3
Fuertemente protegido	0.1

Tabla 8. Elementos de la institución afectados

Elementos de la institución
1. Física
2. Red / telecomunicaciones
3. Plataformas
4. Bases de datos
5. Aplicaciones
6. Información / documentos
7. Personas

Una vez definidos los procesos y activos de información asociados, los dueños de los procesos identificarán las amenazas que pueden afectar a los activos de información que los soportan. Este es un trabajo especializado, pues es necesario conocer las vulnerabilidades que tienen los activos y cómo éstas pueden ser explotadas.

b. Definición de criterios de evaluación de riesgo

Como criterios de evaluación de riesgos se han considerado:

- La criticidad de los procesos.
- La valoración de los activos de información, en términos de su seguridad.
- El nivel de protección que tiene el activo.
- Las amenazas y agentes de amenazas.
- El impacto: en personas, material, económico, de procesos e imagen/reputación.

El criterio de aceptación del riesgo se encuentra definido en:

- Umbral medio: 1.8
- Umbral alto: 3.6
- Criterio de aceptación: 1.8

Los activos que hayan sido evaluados y mantengan un nivel de riesgo hasta 1.8, no requerirán un plan de tratamiento de riesgo, sin embargo, deberán ser plenamente identificados y

monitoreados periódicamente. Es decir, el criterio para aceptar el riesgo es el umbral medio (1.8).

c. Análisis del riesgo

En esta fase del proceso se deben identificar los agentes de amenazas, es decir, los entes que se encuentran interesados en explotar las vulnerabilidades de los activos de la información, por ejemplo: personal interno, proveedor/contratista, hackers, entre otros; también se debe estimar la probabilidad de su existencia, el nivel de interés y el nivel de capacidad del agente de amenaza. Para el efecto, se utilizarán las siguientes escalas de valoración [10,20].

Tabla 9. Valoración del agente de amenaza (probabilidad)

Valor	Probabilidad de existencia	Nivel de interés	Nivel de capacidad
0.9	Es casi seguro que existe	El interés es incontrolable	Los recursos son superiores
0.7	Es muy posible que exista	Se genera mucho interés	Cuenta con muchos recursos
0.5	Es probable que exista	Se genera regular interés	Los recursos son regulares
0.3	Es poco probable que exista	Se genera poco interés	Cuenta con muy pocos recursos

Valor	Probabilidad de existencia	Nivel de interés	Nivel de capacidad
0.1	Es casi imposible que exista	Casi no se genera interés	Los recursos son casi nulos

Al finalizar esta etapa del proceso, se debe obtener un listado de las principales amenazas y agente de amenazas, que permitirán obtener la probabilidad de ocurrencia del riesgo identificado y analizado (amenaza), considerando la siguiente tabla [20, 21].

Tabla 10. Probabilidad de ocurrencia

Valor	Probabilidad de ocurrencia
0.9	Casi seguro
0.7	Alta
0.5	Mediana
0.3	Baja
0.1	Casi imposible

d. Evaluación del riesgo

En esta fase del proceso, se determinará el daño ocasionado por los riesgos identificados y el nivel de riesgo de su materialización, multiplicando la probabilidad de ocurrencia por el impacto.

A fin de determinar el impacto, se utilizará la siguiente tabla que detalla las ponderaciones para los tipos de daños: personas, material, económico, de procesos e imagen/reputación [20, 21].

Tabla 11. Ponderación del impacto

Valor	Impacto	Personas	Material	Económico	Procesos	Imagen / Reputación
10	Catastrófico	Muertes	Pérdidas graves no recuperables	Entre $675,000 y $900,000	Afectación de procesos críticos que no pueden reanudarse en menos de cinco días	Difusión a nivel internacional
8	Alto	Heridos graves	Pérdidas recuperables a largo plazo	Entre $450,000 y $675,000	Afectación de procesos críticos que pueden reanudarse en menos de cinco días	Difusión a nivel de todo el país
6	Regular	Lesiones con incapacidad	Pérdidas leves no recuperables	Entre $225,000 y $450,000	Afectación de varios proceso no críticos	Difusión a nivel provincial
4	Mínimo	Lesiones moderadas	Pérdidas leves	Entre $90,000 y $225,000	Afectación de un proceso no crítico	Difusión dentro de la universidad
2	Ninguno	Sin lesiones	Sin pérdidas materiales	Menor de $90,000	Sin afectación	Difusión dentro de la unidad administrativa

Al final de la fase, se obtendrán los niveles de riesgo de cada amenaza identificada, en función de la siguiente escala.

Tabla 12. Niveles de riesgo

Nivel	Descripción
< = 1.8	BAJO
> 1.8 y < = 3.6	MEDIO
> 3.6	ALTO

Así mismo, se obtendrá el mapa de riesgos de TI y de seguridad de la información, similar al que se muestra en el siguiente gráfico.

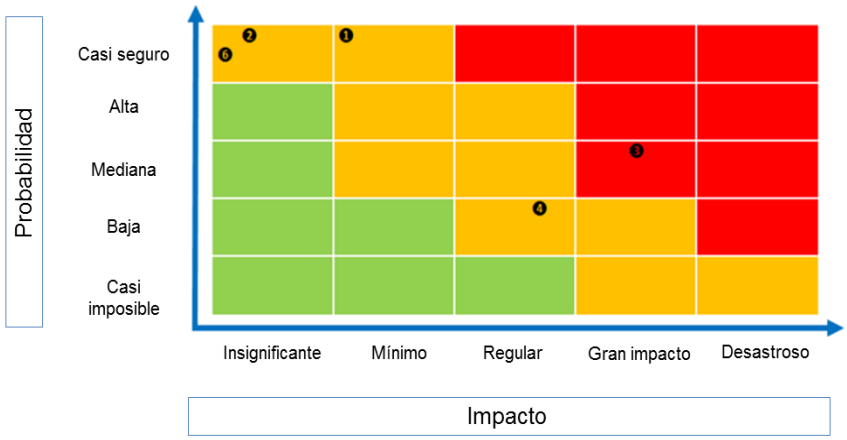


Figura 3.13. Mapa de riesgos

Logo	Proceso de Gestión de Riesgo de Tecnología de Información	Revisado	Código PGRTI-002
	Fase 2: Definición de riesgos de TI y seguridad de la información	Elaborado Octubre / 2016	Versión 1.0

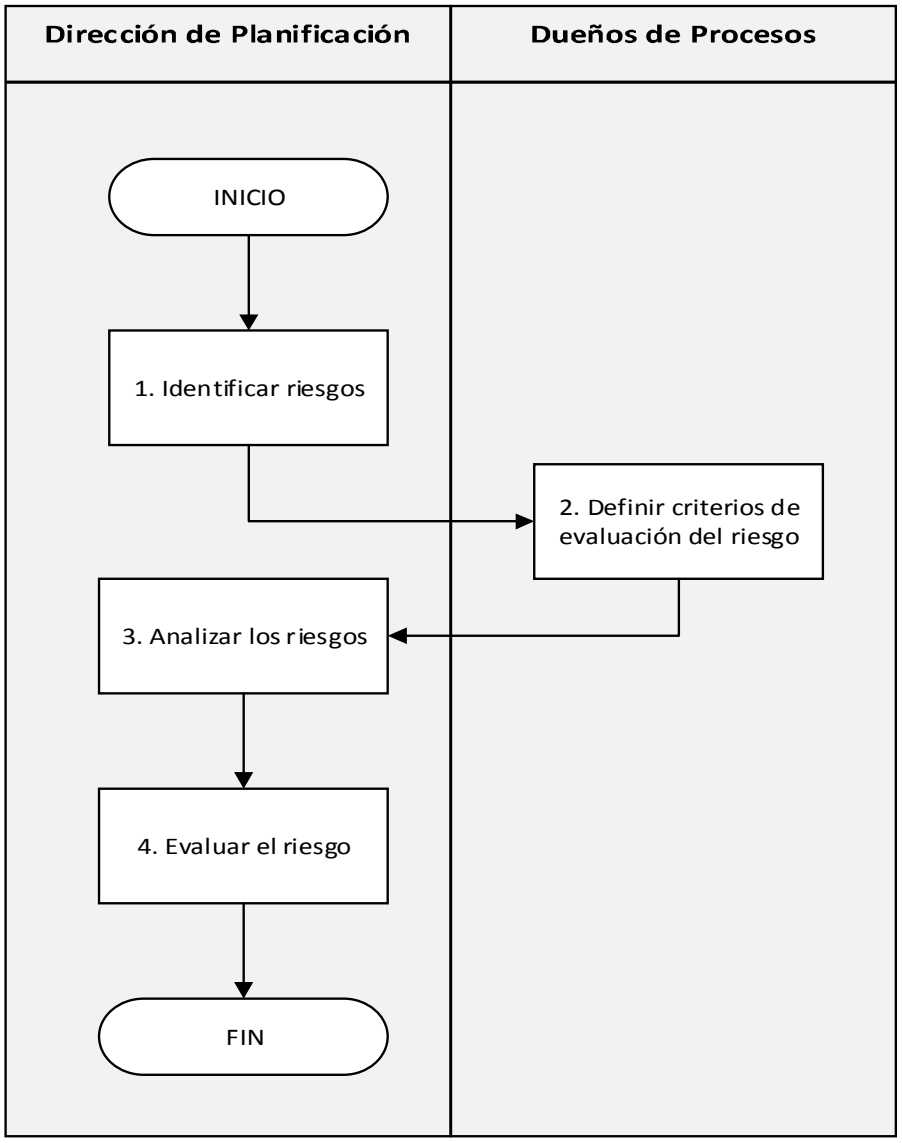


Figura 3.14. Fase 2: Definición de riesgos deTI y SI

Fase 3: Tratamiento del riesgo (respuesta al riesgo)

El tratamiento del riesgo consiste en tomar acciones para mitigar los riesgos tecnológicos y llevarlos a niveles de tolerancia aceptables. La estrategia de mitigación de riesgos y la respuesta a los mismos, dependerá del apetito al riesgo que tenga la institución.

Para este proceso, se ha definido al umbral 1.8 (probabilidad por impacto) como el umbral aceptable de tolerancia al riesgo, es decir, los activos con niveles de riesgo superiores a este umbral, deberán contar con un control para mitigarlos.

La estrategia de tratamiento del riesgo [22] que se aplicará, será:

- Aceptar: Cuando el nivel de riesgo es menor o igual a 1.8.
- Evitar: No implementar la actividad o proceso.
- Transferir: Compartir el riesgo con alguien más, por ejemplo: seguros.
- Mitigar: Implementar controles para reducir la probabilidad o el impacto del riesgo.

El objetivo con el plan de tratamiento de riesgos es llevar los riesgos a niveles mínimos aceptables.

Figura 3.15. Riesgo residual

Nota: el riesgo residual mínimo aceptable será 1.8

En esta fase se debe asignar la prioridad de implementación de los controles en función del nivel de riesgo; además, se debe realizar un análisis costo / beneficio para proponer y aprobar los controles previo a su implementación.

Logo	Proceso de Gestión de Riesgo de Tecnología de Información	Revisado	Código PGRTI-003
	Fase 3: Tratamiento del riesgo (respuesta al riesgo)	Elaborado Octubre / 2016	Versión 1.0

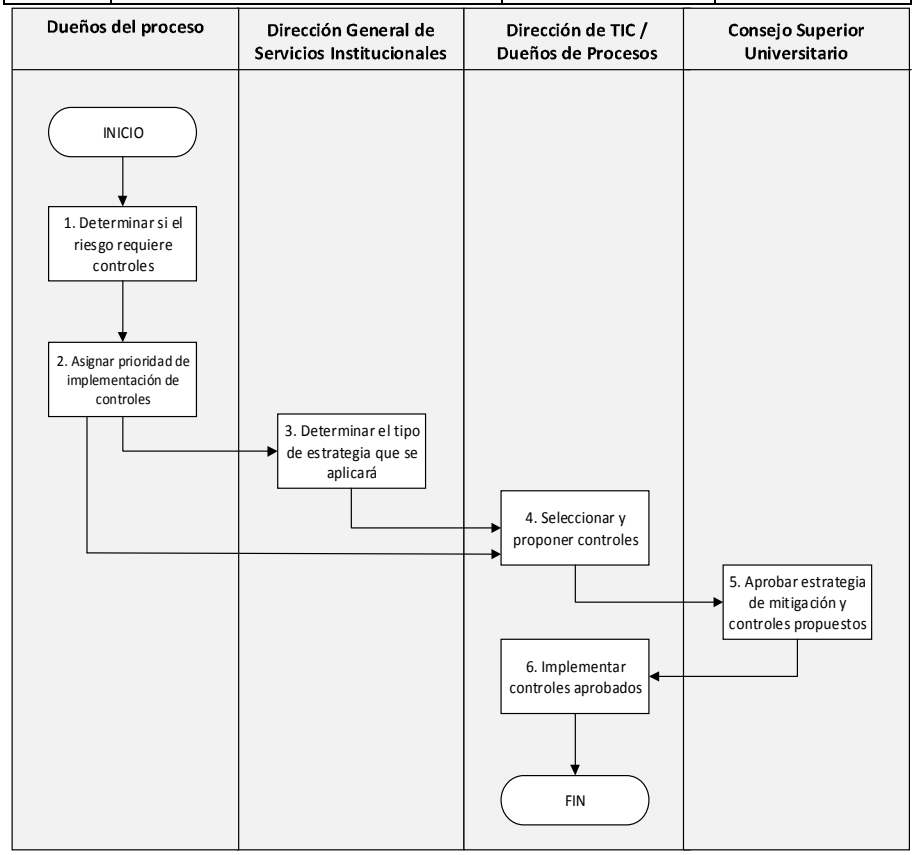


Figura 3.16. Fase 3: Tratamiento del riesgo

Fase 4: Monitoreo y revisión

La última fase dentro del proceso de administración de riesgos es el monitoreo de la ejecución de los controles y definición de indicadores que permitan constatar la aplicación y efectividad de los mismos.

Estos indicadores deben ser definidos formalmente y establecer un rango de tolerancia para considerarlos efectivos. Además, debe existir un esquema de informes de cumplimiento de los mismos.

Así mismo, se debe evaluar el grado de cumplimiento de las políticas del proceso de gestión de riesgos de TI (PGRTI) y la efectividad de los controles e informar al Consejo Superior Universitario.

El Consejo Superior Universitario determinará si es necesario definir una nueva estrategia de mitigación de riesgos y tomará decisiones a partir de los informes recibidos.

Logo	Proceso de Gestión de Riesgo de Tecnología de Información	Revisado	Código PGRTI-004
	Fase 4: Monitoreo y revisión	Elaborado Octubre / 2016	Versión 1.0

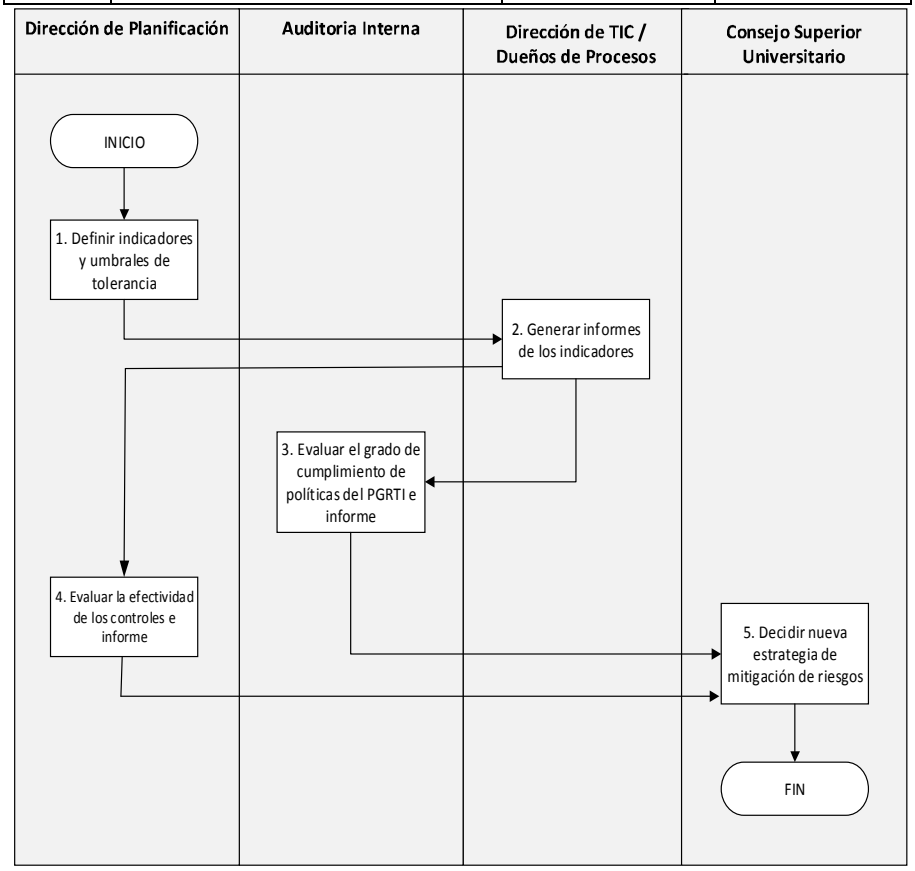


Figura 3.17. Fase 4: Monitoreo y revisión

3.5 Matriz de riesgo operativo: factor tecnología y seguridad de la información

El producto resultante del PGRTI será una matriz consolidada de los riesgos tecnológicos y de seguridad de la información que

plasme los criterios de evaluación descritos a lo largo del proceso así como los niveles de riesgo luego del tratamiento de los mismos (ver anexo A: Formato de matriz de riesgos tecnológicos y de seguridad de la información [20, 21]).

CAPÍTULO 4

4. APLICACIÓN DEL PROCESO DE GESTIÓN DEL RIESGO (PGRTI) A LOS PROCESOS SOPORTADOS EN LA PLATAFORMA DE GESTIÓN ACADÉMICA

4.1 Análisis de información

Para llevar a cabo la implementación del proceso de gestión de riesgos de tecnología y seguridad de la información, la institución de educación superior hizo entrega de la siguiente información:

- Mapa de procesos
- Inventario de los procesos soportados por la plataforma de gestión académica.
- Inventario de activos asociados a los procesos.

4.1.1 Mapa de procesos

A continuación, se muestra el mapa de procesos de la universidad [23], mismo que se encuentra orientado a lograr la satisfacción de los clientes internos y externos, brindando servicios educativos, de investigación y vinculación con la colectividad.

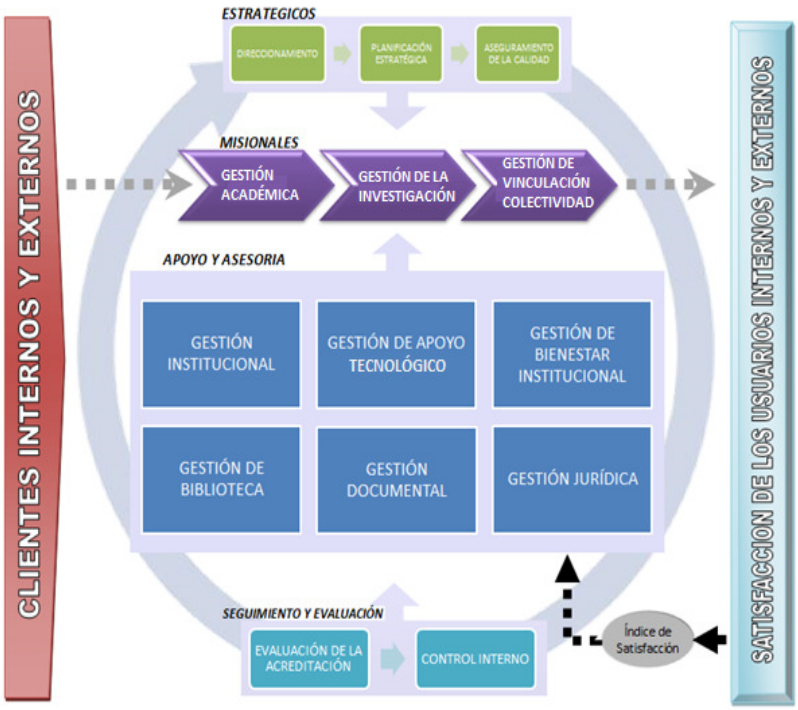


Figura 4.18. Mapa de procesos de la universidad

La institución ha clasificado sus procesos en:

- Procesos estratégicos: Proporcionan direccionamiento y son ejecutados por la alta administración de la universidad.
- Procesos misionales: Corresponden a los procesos productivos orientados al cumplimiento de las políticas y estrategias relacionadas con la calidad de los servicios educativos ofrecidos por la institución, es decir, contribuyen al logro de los objetivos institucionales.
- Procesos de apoyo y asesoría: Apoyan o soportan a los procesos estratégicos y misionales, proporcionan personal competente, reducen riesgos del trabajo, mantienen condiciones de operatividad y funcionamiento, coordinan y mantienen la eficacia del desempeño administrativo y optimización de recursos.
- Procesos de seguimiento y evaluación: Orientados al control interno y evaluación de los procesos antes mencionados.

4.1.2 Inventario de los procesos del macroproceso de gestión académica

De la revisión efectuada, se determinaron los procesos que forman parte del macroproceso de gestión académica que se detallan en el anexo B.

Estos procesos se relacionan principalmente con la gestión académica de la universidad enfocados al aseguramiento de la calidad mediante procesos estratégicos de selección y contratación docente; el proceso misional de docencia que permite toda la gestión de matriculación y planificación de las materias y la distribución de la carga horaria así como la evaluación y actualización de programas microcurriculares; asimismo se ha definido el proceso de titulación de los estudiantes mediante actividades de control de tesis, pasantías, vinculación con la colectividad y registro de egresados y graduados.

Los procesos en mención se encuentran apalancados en varios sistemas de información que la institución de

educación superior ha implementado y que son administrados por los dueños de procesos y por la Dirección de Tecnologías de la Información y Comunicación. Entre los principales sistemas, podemos mencionar a: Sistema en línea para el ingreso de Syllabus, planes de clases y calificaciones (SYSWEB); Sistema de Gestión Docente y el Sistema Académico, los mismos que en su conjunto forman parte de la plataforma de gestión académica de la universidad.

4.2 Diagnóstico y selección de procesos críticos

Para el diagnóstico y definición de los procesos críticos que se incluyeron en el presente trabajo, se organizaron talleres en coordinación con la Dirección de Planificación y los dueños de los procesos misionales o productivos, es decir, los procesos que deben ejecutarse aún en periodos de contingencia para asegurar razonablemente las actividades administrativas de la institución. Los procesos identificados como críticos son:

- MSO-DC-PA Planificación académica, mismo que permite:
  - Iniciar y cerrar el periodo académico.
  - Registrar docentes en la plataforma.

  - Definir horarios de clase.
  - Organizar paralelos.
  - Evaluar y actualizar los programas microcurriculares.
  - Administrar políticas y estrategias del proceso de evaluación académica.
  - Planificación y ejecución de evaluación docente.
- MSO-DC-MT Matriculación, cuyo objetivo principal es la matriculación del estudiante en un período académico.

Para esta definición, la universidad consideró el tipo de proceso, periodo máximo tolerable de interrupción, tiempo de recuperación objetivo y punto de recuperación objetivo a fin de determinar el nivel de criticidad e importancia para la institución.

En el anexo C se muestran los procesos críticos que son soportados por la plataforma informática de gestión académica y que han sido seleccionados como parte del alcance del presente trabajo.

4.3 Inventario de activos asociados a los procesos críticos seleccionados

Luego de reuniones mantenidas con personal clave de los procesos de planificación académica y matriculación, tales como: Secretaria Académica, Planificación Institucional, Director de Tecnologías y personal del área de Tecnología, se determinó que los activos de información asociados a los procesos son los que se muestran a continuación:

Tabla 13. Inventario de activos de información

Id. Proceso	Id. Activo	Activo de información	Descripción	Clasificación (crítico/no crítico)	Funcionario Responsable	Funcionario que Resguarda
MSO-DC-PA	1001	SERVIDOR DE PRODUCCIÓN HP BLADE c3000	Servidor físico que contiene a los demás servidores virtuales.	Crítico	Vicerrector Académico	Jefe de Infraestructura Tecnológica
	1002	SER-PRO-WEB	Portal web de la institución: contiene el sistema SYSWEB, planificación microcurricular, registro de calificaciones, control de planes de clases, evaluación docente, matriculación en línea.	Crítico	Vicerrector Académico	Jefe de Infraestructura Tecnológica
	1003	WEBSERVICES	Contiene servicio web con información de calificaciones de estudiantes	Crítico	Jefe de Desarrollo	Jefe de Infraestructura Tecnológica
	1004	SERVIDOR DE BASE DE DATOS	Servidor que contiene la base de datos de los sistemas académicos y administrativos	Crítico	Vicerrector Académico	Jefe de Infraestructura Tecnológica
	1005	SERVIDOR DE APLICACIONES	Servidor que contiene las aplicaciones web de la institución	Crítico	Jefe de Desarrollo	Jefe de Infraestructura Tecnológica
	1006	SERVIDOR DE RESPALDOS	Servidor que contiene los respaldos de las diferentes páginas web de la institución y base de datos	Crítico	Jefe de Infraestructura Tecnológica	Director de Tecnología de la Información

Id. Proceso	Id. Activo	Activo de información	Descripción	Clasificación (crítico/no crítico)	Funcionario Responsable	Funcionario que Resguarda
	1007	SWITCH CISCO (SW-CORE)	Dispositivo que contiene configuración de la red interna de la institución. Switch principal para acceso a la LAN e internet.	Crítico	Analista de Hardware	Jefe de Infraestructura Tecnológica
	1008	SWITCH CISCO (SW-CORE) - CONTINGENCIAS	Dispositivo que contiene configuración de la red interna de la institución. switch principal para acceso a la LAN e internet (contingencias)	No crítico	Analista de Hardware	Jefe de Infraestructura Tecnológica
	1009	ROUTER CISCO CNT 1	Dispositivo de red para el acceso a internet	Crítico	Analista de Hardware	Jefe de Infraestructura Tecnológica
	1010	ROUTER CISCO CNT 2	dispositivo de red para el acceso a internet	No crítico	Analista de Hardware	Jefe de Infraestructura Tecnológica
	1011	ARCHIVO FÍSICO DE OFICIOS / CORREOS ELECTRÓNICOS QUE CONTIENEN EL CALENDARIO ACADÉMICO APROBADO POR EL VICERRECTORADO ACADÉMICO	Contiene el documento / correo electrónico con información de la planificación académica de la universidad	No crítico	Vicerrector Académico	Asistente TIC
	1012	ARCHIVO FÍSICO DE ACTAS DE CALIFICACIONES POR ASIGNATURAS Y POR CARRERA	Contiene el respaldo en físico de calificaciones por asignaturas y por carrera	Crítico	Director de Carrera	Secretaria de Carrera
	1013	ARCHIVO FÍSICO DE OFICIOS CON RESOLUCIONES DE CONSEJO UNIVERSITARIO POR EXCEPCIONES	Contiene las resoluciones de consejo universitario para aplicar excepciones en períodos académicos	No crítico	Miembros del Consejo Universitario	Asistente TIC
	1014	ARCHIVO FÍSICO DE PROGRAMAS MICROCURRICULARES POR ASIGNATURA Y CARRERA	Contiene el sílabo de asignaturas por carreras	No crítico	Docente	Secretaria de Carrera
	1015	SER-PRO-DNS	Servidor de nombres de dominio (DNS)	Crítico	Jefe de Infraestructura Tecnológica	Jefe de Infraestructura Tecnológica
	1016	EJECUTABLE DEL SISTEMA ACADÉMICO – INTRANET	Ejecutable del sistema académico que se copia en cada equipo de secretarias y directores de carrera, decanos de cada facultad y vicerrector académico	Crítico	Vicerrector Académico	Jefe de Desarrollo

Id. Proceso	Id. Activo	Activo de información	Descripción	Clasificación (crítico/no crítico)	Funcionario Responsable	Funcionario que Resguarda
	1017	SER-PRO-CDSTD	Servidor Active Directory. Control de acceso a usuarios estudiantes	No crítico	Jefe de Infraestructura Tecnológica	Jefe de Infraestructura Tecnológica
	1018	SER-PRO-CD	Servidor Active Directory. control de acceso a usuarios-personal de la institución	Crítico	Jefe de Infraestructura Tecnológica	Jefe de Infraestructura Tecnológica
	1019	PFS-BOR-PRINC	Control de seguridad perimetral freeBsd – firewall	Crítico	Jefe de Infraestructura Tecnológica	Jefe de Infraestructura Tecnológica
	1020	SER-DHCP-LINUX	Control y asignación de direcciones IP a PC	Crítico	Jefe de Infraestructura Tecnológica	Jefe de Infraestructura Tecnológica
	1021	CENTRO DE CÓMPUTO	Centro de cómputo	Crítico	Jefe de Infraestructura Tecnológica	Director de Tecnología de la Información
MSO-DC-MT	1001	SERVIDOR DE PRODUCCIÓN HP BLADE c3000	Servidor físico que contiene a los demás servidores virtuales.	Crítico	Vicerrector Académico	Jefe de Infraestructura Tecnológica
	1002	SER-PRO-WEB	Portal web de la institución: contiene el sistema SYSWEB, planificación microcurricular, registro de calificaciones, control de planes de clases, evaluación docente, matriculación en línea.	Crítico	Vicerrector Académico	Jefe de Infraestructura Tecnológica
	1003	WEBSERVICES	Contiene servicio web con información de calificaciones de estudiantes	Crítico	Jefe de Desarrollo	Jefe de Infraestructura Tecnológica
	1004	SERVIDOR DE BASE DE DATOS	Servidor que contiene la base de datos de los sistemas académicos y administrativos	Crítico	Vicerrector Académico	Jefe de Infraestructura Tecnológica
	1005	SERVIDOR DE APLICACIONES	Servidor que contiene las aplicaciones web de la institución	Crítico	Jefe de Desarrollo	Jefe de Infraestructura Tecnológica
	1006	SERVIDOR DE RESPALDOS	Servidor que contiene los respaldos de las diferentes páginas web de la institución y base de datos	Crítico	Jefe de Infraestructura Tecnológica	Director de Tecnología de la Información
	1007	SWITCH CISCO (SW-CORE)	Dispositivo que contiene configuración de la red interna de la institución. Switch principal para acceso a la LAN e internet.	Crítico	Analista de Hardware	Jefe de Infraestructura Tecnológica
	1008	SWITCH CISCO (SW-CORE) - CONTINGENCIAS	Dispositivo que contiene configuración de la red interna de la institución. Switch principal para acceso a la LAN e internet (contingencias)	No crítico	Analista de Hardware	Jefe de Infraestructura Tecnológica
	1009	ROUTER CISCO CNT 1	Dispositivo de red para el acceso a internet	Crítico	Analista de Hardware	Jefe de Infraestructura Tecnológica
	1010	ROUTER CISCO CNT 2	Dispositivo de red para el acceso a internet	No crítico	Analista de Hardware	Jefe de Infraestructura Tecnológica

Id. Proceso	Id. Activo	Activo de información	Descripción	Clasificación (crítico/no crítico)	Funcionario Responsable	Funcionario que Resguarda
	1017	SER-PRO-CDSTD	Servidor Active Directory. Control de acceso a usuarios estudiantes	No crítico	Jefe de Infraestructura Tecnológica	Jefe de Infraestructura Tecnológica
	1018	SER-PRO-CD	Servidor Active Directory. control de acceso a usuarios-personal de la institución	Crítico	Jefe de Infraestructura Tecnológica	Jefe de Infraestructura Tecnológica
	1019	PFS-BOR-PRINC	control de seguridad perimetral freeBsd – firewall	Crítico	Jefe de Infraestructura Tecnológica	Jefe de Infraestructura Tecnológica
	1020	SER-DHCP-LINUX	Control y asignación de direcciones IP a PC	Crítico	Jefe de Infraestructura Tecnológica	Jefe de Infraestructura Tecnológica
	1022	ARCHIVO FÍSICO DE OFICIOS CON RESOLUCIONES DEL CONSEJO UNIVERSITARIO	Contiene resoluciones para aplicar excepciones en matriculación	No crítico	Miembros Consejo Universitario	Asistente TIC
	1023	OFICIO/EMAIL ESTADO DE CALIFICACIONES POR CARRERA	Documento / email de confirmación de ingreso de calificaciones	No crítico	Director Carrera	Asistente TIC
	1024	CORREO ELECTRÓNICO Office 365 EN LA NUBE	Correo electrónico institucional	No crítico	Jefe de Infraestructura Tecnológica	Director de Tecnología de la Información
	1025	ARCHIVO FÍSICO DE SOLICITUDES PRE-IMPRESAS PARA MATRICULACIÓN	Contiene solicitudes pre-impresas con la información del estudiante	No crítico	Secretaria de Carrera	Secretaria de Decanato
	1026	ARCHIVO FÍSICO DE COMPROBANTES DE MATRÍCULA	Contiene el registro de la matricula	Crítico	Secretaria de Carrera	Secretaria de Decanato
	1027	ARCHIVO FÍSICO DE COMPROBANTES DE PAGO	Contiene el registro de pago por arrastre o repetición de asignaturas	Crítico	Secretaria de Carrera	Tesorera
	1028	ARCHIVO FÍSICO DE FÍCHA DE ESTUDIANTE	Contiene ficha del estudiante y su información académica	Crítico	Secretaria de Carrera	Secretaria de Decanato

4.4 Identificación de riesgos tecnológicos y de seguridad de la información de procesos críticos seleccionados por la institución

Para la identificación de los riesgos tecnológicos y de seguridad de la información de los procesos críticos seleccionados por la institución, se aplicó lo indicado en la *"Fase 2: definición de riesgos tecnológicos y de seguridad de la información"*, numeral 3.4, del capítulo 3 de este documento.

Mediante un taller efectuado con las autoridades de la institución, se valoraron los activos de información de los procesos críticos seleccionados en términos de su integridad, confidencialidad y disponibilidad, el nivel de protección existente sobre estos activos así como a qué parte de la institución afectan, aplicando el método de criterio ponderado mediante lo establecido en las tablas números 6, 7 y 8, literal a., Fase 2, numeral 3.4, capítulo 3 de este trabajo.

Posteriormente, se definió un listado de las posibles amenazas que podrían afectar a los activos de información asociados a los procesos críticos, los mismos que fueron analizados para conocer las vulnerabilidades y la posibilidad de su explotación. Las amenazas fueron clasificadas considerando si las mismas son causadas por: la naturaleza, los humanos, errores u omisiones, y fallas de la tecnología; además, se determinó a qué parte de la

institución afectan, para poder definir los escenarios de riesgo (activo versus amenazas). A continuación, se muestra el listado de las amenazas analizadas y que pueden afectar a uno o varios de los activos de información de los procesos críticos:

Tabla 14. Amenazas analizadas

				Elementos afectados (Tabla 8)						
Clasificación	**No. referencia amenaza**	**Amenaza**	**Agente de amenaza**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
Causados por la naturaleza	1001	Incendio	Material (falla)	✓	✓	✓	✓	✓	✓	✓
	1002	Sismo	Natural	✓						✓
	1003	Polvo	Natural	✓	✓	✓				
	1004	Huracán / Tormenta	Natural	✓	✓	✓				✓
	1005	Inundación	Natural	✓	✓	✓			✓	✓
	1006	Rayos	Natural	✓	✓	✓	✓	✓	✓	✓
	1007	Tsunami	Natural	✓	✓	✓	✓	✓	✓	✓
	1008	Temperaturas excesivamente altas	Natural	✓						✓
	1009	Epidemias	Natural							✓
Causados por humanos	1010	Materiales peligrosos o contaminantes (explosiones)	Empleado sin experiencia	✓	✓	✓	✓	✓	✓	✓
	1011	Atentado / terrorismo	Grupo subversivo	✓	✓	✓	✓	✓	✓	✓
	1012	Sabotaje	Personal descontento	✓	✓	✓	✓	✓	✓	
	1013	Código malicioso	Hacker		✓	✓	✓	✓		
	1014	Fraude	Proveedor / Contratista				✓	✓	✓	
	1015	Fraude	Personal descontento				✓	✓	✓	
	1020	Robo	Delincuencia organizada	✓	✓	✓				
	1021	Robo	Proveedor / Contratista	✓			✓		✓	

				Elementos afectados (Tabla 8)						
Clasificación	**No. referencia amenaza**	**Amenaza**	**Agente de amenaza**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
	1022	Incumplimiento de contrato	Proveedor / Contratista		✓	✓	✓	✓		
	1023	Insolvencia del contratista	Proveedor / Contratista		✓	✓				
	1024	Acceso no autorizado	Personal descontento		✓	✓	✓	✓	✓	
	1025	Acceso no autorizado	Empleado sin experiencia		✓	✓	✓	✓	✓	
	1026	Acceso no autorizado	Proveedor / Contratista		✓	✓	✓	✓	✓	
	1027	Acceso no autorizado	Ex-empleado		✓	✓	✓	✓	✓	
	1028	Modificación no autorizada de información	Personal descontento		✓	✓	✓	✓	✓	
	1029	Modificación no autorizada de información	Empleado sin experiencia		✓	✓	✓	✓	✓	
	1030	Modificación no autorizada de información	Proveedor / Contratista		✓	✓	✓	✓	✓	
	1031	Modificación no autorizada de información	Ex-empleado		✓	✓	✓	✓	✓	
	1032	Ingeniería social	Ex-empleado						✓	✓
	1033	Ingeniería social	Script Kiddies						✓	✓
	1034	Crackeo de contraseñas	Hacker		✓	✓	✓	✓		
Causados por errores u omisiones	1016	Interrupción energía eléctrica	Material (falla)		✓	✓	✓	✓		
	1017	Variaciones de voltaje	Material (falla)		✓	✓	✓	✓		
	1018	Chantaje / Extorsión	Delincuencia organizada							✓
	1019	Robo	Personal descontento	✓			✓		✓	
	1035	Respaldos defectuosos	Empleado sin experiencia		✓	✓	✓	✓		
	1036	Servicios de red o enlace tercerizados sin control	Proveedor / Contratista		✓					
	1037	Negación de servicio	Empleado sin experiencia		✓	✓	✓	✓		
	1038	Fallas estructurales del edificio	Empleado sin experiencia	✓	✓	✓	✓	✓	✓	✓
	1039	Filtraciones de agua	Material (falla)	✓	✓	✓	✓	✓	✓	
	1040	Limitado espacio en centro de cómputo	Empleado sin experiencia	✓	✓	✓				
Causados por fallas de la	1041	Virus en las redes o	Hacker		✓	✓	✓	✓		

				Elementos afectados (Tabla 8)						
Clasificación	**No. referencia amenaza**	**Amenaza**	**Agente de amenaza**	**1**	**2**	**3**	**4**	**5**	**6**	**7**
tecnología		computadoras								
	1042	Virus en las redes o computadoras	Personal descontento		✓	✓	✓	✓		
	1043	Virus en las redes o computadoras	Empleado sin experiencia		✓	✓	✓	✓		
	1044	Fallas de hardware en los equipos	Material (falla)		✓	✓				
	1045	Discos defectuosos	Material (falla)			✓	✓	✓		
	1046	Periféricos o componentes defectuosos	Material (falla)		✓	✓				
	1047	UPS defectuoso o sin mantenimiento	Empleado sin experiencia		✓	✓	✓	✓		
	1048	UPS defectuoso o sin mantenimiento	Personal descontento		✓	✓	✓	✓		
	1049	UPS defectuoso o sin mantenimiento	Material (falla)		✓	✓	✓	✓		

Para la evaluación de las amenazas también se hizo la valoración del agente de amenaza (probabilidad de ocurrencia), conforme a los criterios establecidos en la tabla 9 del proceso de gestión del riesgo de tecnologías y seguridad de la información (PGRTI) definido en el capítulo 3.

4.5 Matriz de riesgo operativo del factor tecnología y seguridad de la información

La matriz de riesgo operativo del factor tecnología y seguridad de la información contiene el análisis de las diferentes amenazas valorando su probabilidad de ocurrencia; el impacto en personas, material, económico, de procesos e imagen/reputación, conforme a lo establecido en el proceso de gestión del riesgo de tecnologías y seguridad de la información (PGRTI) definido en el capítulo 3; se determinaron los escenarios de riesgo, es decir, el cruce de información de las amenazas versus los activos que podrían ser afectados si se materializa la explotación de sus vulnerabilidades, obteniendo el nivel de riesgo multiplicando la probabilidad de ocurrencia y el impacto.

La matriz de riesgos se obtuvo al sumar la valoración de probabilidad de ocurrencia de las amenazas con el nivel de vulnerabilidad de los activos y obteniendo un promedio; este promedio fue multiplicado por el valor máximo del impacto en personas, material, económico, de procesos e imagen/reputación, que podría conducir a la materialización del riesgo, obteniendo un valor entre 0 y 10.

Producto de esta evaluación, se determinó que las principales amenazas que provocan un riesgo alto (> 3.6) sobre varios activos de información, son:

Tabla 15. Amenazas de riesgo alto

Amenaza	Descripción de la amenaza	Agente de amenaza
1013	Código malicioso	Hacker
1020	Robo	Delincuencia organizada
1029	Modificación no autorizada de información	Empleado sin experiencia
1028	Modificación no autorizada de información	Personal descontento
1031	Modificación no autorizada de información	Ex–empleado
1041	Virus en las redes o computadoras	Hacker
1012	Sabotaje	Personal descontento
1042	Virus en las redes o computadoras	Personal descontento
1011	Atentado / terrorismo	Grupo subversivo
1038	Fallas estructurales del edificio	Empleado sin experiencia
1030	Modificación no autorizada de información	Proveedor / Contratista
1035	Respaldos defectuosos	Empleado sin experiencia
1002	Sismo	Natural
1019	Robo	Personal descontento
1048	UPS defectuoso o sin mantenimiento	Personal descontento
1015	Fraude	Personal descontento
1016	Interrupción energía eléctrica	Material (falla)
1017	Variaciones de voltaje	Material (falla)
1037	Negación de servicio	Empleado sin experiencia
1043	Virus en las redes o computadoras	Empleado sin experiencia

Las principales amenazas que provocan un riesgo medio (>= 1.8 y <= 3.6) sobre los activos de información de los procesos seleccionados, son:

Tabla 16. Amenazas de riesgo medio

Amenaza	Descripción de la amenaza	Agente de amenaza
1001	Incendio	Material (falla)
1007	Tsunami	Natural
1034	Crackeo de contraseñas	Hacker
1021	Robo	Proveedor / Contratista
1036	Servicios de red o enlace tercerizados sin control	Proveedor / Contratista
1008	Temperaturas excesivamente altas	Natural
1044	Fallas de hardware en los equipos	Material (falla)
1045	Discos defectuosos	Material (falla)
1010	Materiales peligrosos o contaminantes (explosiones)	Empleado sin experiencia
1025	Acceso no autorizado	Empleado sin experiencia
1047	UPS defectuoso o sin mantenimiento	Empleado sin experiencia
1024	Acceso no autorizado	Personal descontento
1027	Acceso no autorizado	Ex-empleado
1032	Ingeniería social	Ex-empleado
1033	Ingeniería social	Script Kiddies
1005	Inundación	Natural
1014	Fraude	Proveedor / Contratista
1004	Huracán / Tormenta	Natural
1006	Rayos	Natural
1003	Polvo	Natural
1026	Acceso no autorizado	Proveedor / Contratista
1039	Filtraciones de agua	Material (falla)
1022	Incumplimiento de contrato	Proveedor / Contratista
1023	Insolvencia del contratista	Proveedor / Contratista
1049	UPS defectuoso o sin mantenimiento	Material (falla)

Las principales amenazas que provocan un nivel de riesgo bajo (< 1.8) sobre los activos de información de los procesos críticos seleccionados, son:

Tabla 17. Amenazas de riesgo bajo

Amenaza	Descripción de la amenaza	Agente de amenaza
1046	Periféricos o componentes defectuosos	Material (falla)
1040	Limitado espacio en centro de	Empleado sin experiencia

Amenaza	Descripción de la amenaza	Agente de amenaza
	cómputo	

Cabe mencionar que las amenazas de riesgo bajo no fueron consideradas para el tratamiento del riesgo, debido a que el riesgo mínimo aceptable definido en la metodología indicada en el capítulo 3, es aquel cuyo producto de probabilidad e impacto sea menor a 1.8.

Es necesario indicar que no se han considerado las amenazas que atentan directamente con las personas, ya que estas deben ser tratadas en un plan de continuidad del negocio.

A continuación, se muestra el mapeo de los cuarenta y siete (47) riesgos evaluados en términos de su probabilidad de ocurrencia e impacto sobre los activos de información y procesos críticos asociados.

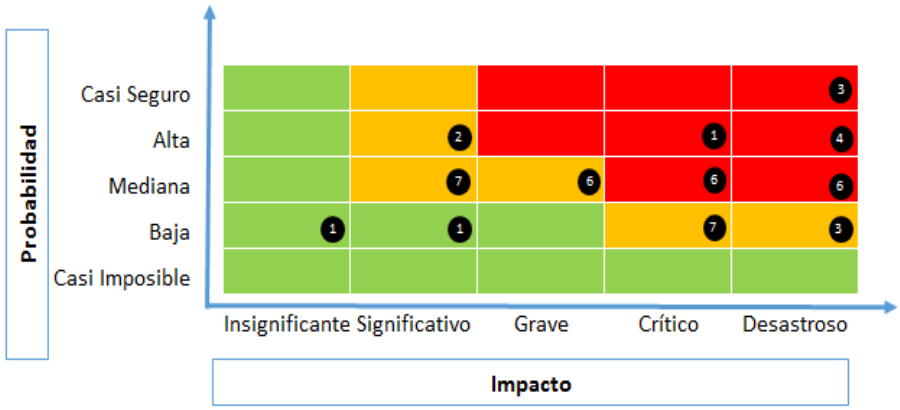


Figura 4.19. Mapa de riesgos institucionales

CAPÍTULO 5

5. PLAN DE ACCIÓN PARA CONTROLAR LOS RIESGOS IDENTIFICADOS

5.1 Plan de acción por riesgo, según los procesos críticos seleccionados

Debido a que es la primera vez que se realiza este tipo de análisis en la institución, considerando que la gestión de riesgos es un proceso continuo y que debe ejecutarse periódicamente, y dado el presupuesto anual para tecnología de la información, se seleccionaron las 20 amenazas evaluadas como riesgo alto y que se encuentran detalladas en la tabla 15 del capítulo 4.

Para cada una de las amenazas y dependiendo de los activos de información de los procesos críticos seleccionados, se determinaron los controles que se deben implementar para poder mitigar estos riesgos.

En el anexo D de este trabajo, se detallan los controles propuestos y su relación con 40 controles del “Anexo A” de la norma ISO/IEC 27001:2013.

El plan de acción para la aplicación de los controles propuestos, se elaboró tomando como referencia el nivel de criticidad de los activos de información en términos de su integridad, confidencialidad y disponibilidad. Utilizando los valores de las tablas 6 y 18, los funcionarios responsables y que resguardan cada activo determinaron el nivel de criticidad de los mismos.

Tabla 18. Niveles de criticidad

Valor	Nivel de criticidad
< = 5	Bajo
> 5 y < = 10	Medio
> 10	Alto

En la tabla 19 se muestran los veintiocho (28) activos de información ordenados por su nivel de criticidad, en términos de su seguridad.

Tabla 19. Activos de información y nivel de criticidad

Id. Activo	Activo de información	Descripción	Confidencialidad	Integridad	Disponibilidad	Total	Nivel de criticidad
1016	EJECUTABLE DEL SISTEMA ACADÉMICO – INTRANET	EJECUTABLE DEL SISTEMA ACADÉMICO QUE SE COPIA EN CADA EQUIPO DE SECRETARIAS Y DIRECTORES DE CARRERA, DECANOS DE CADA FACULTAD Y VICERRECTOR ACADÉMICO	5	5	5	15	Alto
1019	PFS-BOR-PRINC	CONTROL DE SEGURIDAD PERIMETRAL FreeBSD – FIREWALL	4	5	4	13	Alto
1001	SERVIDOR DE PRODUCCIÓN HP BLADE c3000	SERVIDOR FÍSICO QUE CONTIENE A LOS DEMÁS SERVIDORES VIRTUALES.	3	5	4	12	Alto
1004	SERVIDOR DE BASE DE DATOS	SERVIDOR QUE CONTIENE LA BASE DE DATOS DE LOS SISTEMAS ACADÉMICOS Y ADMINISTRATIVOS	2	5	5	12	Alto
1002	SER-PRO-WEB	PORTAL WEB DE LA INSTITUCIÓN: CONTIENE EL SISTEMA SYSWEB, PLANIFICACIÓN MICROCURRICULAR, REGISTRO DE CALIFICACIONES, CONTROL DE PLANES DE CLASES, EVALUACIÓN DOCENTE, MATRICULACIÓN EN LÍNEA.	3	4	5	12	Alto

Id. Activo	Activo de información	Descripción	Confidencialidad	Integridad	Disponibilidad	Total	Nivel de criticidad
1005	SERVIDOR DE APLICACIONES	SERVIDOR QUE CONTIENE LAS APLICACIONES WEB DE LA INSTITUCIÓN	3	4	5	12	Alto
1017	SER-PRO-CDSTD	SERVIDOR ACTIVE DIRECTORY. CONTROL DE ACCESO A USUARIOS ESTUDIANTES	5	3	4	12	Alto
1018	SER-PRO-CD	SERVIDOR ACTIVE DIRECTORY. CONTROL DE ACCESO A USUARIOS-PERSONAL DE LA INSTITUCIÓN	5	3	4	12	Alto
1003	WEBSERVICES	CONTIENE SERVICIO WEB CON INFORMACIÓN DE CALIFICACIONES DE ESTUDIANTES	2	5	4	11	Alto
1028	ARCHIVO FÍSICO DE FICHA DE ESTUDIANTE	CONTIENE FICHA DEL ESTUDIANTE Y SU INFORMACIÓN ACADÉMICA	1	5	5	11	Alto
1012	ARCHIVO FÍSICO DE ACTAS DE CALIFICACIONES POR ASIGNATURAS Y POR CARRERA	CONTIENE EL RESPALDO EN FÍSICO DE CALIFICACIONES POR ASIGNATURAS Y POR CARRERA	1	5	4	10	Medio
1021	CENTRO DE CÓMPUTO	CENTRO DE CÓMPUTO	2	2	5	9	Medio
1015	SER-PRO-DNS	SERVIDOR DE NOMBRES DE DOMINIO (DNS)	3	3	3	9	Medio
1024	CORREO ELECTRÓNICO Office 365 EN LA NUBE	CORREO ELECTRÓNICO INSTITUCIONAL	3	3	3	9	Medio
1027	ARCHIVO FÍSICO DE COMPROBANTES DE PAGO	CONTIENE EL REGISTRO DE PAGO POR ARRASTRE O REPETICIÓN DE ASIGNATURAS	1	5	3	9	Medio

Id. Activo	Activo de información	Descripción	Confidencialidad	Integridad	Disponibilidad	Total	Nivel de criticidad
1007	SWITCH CISCO (SW-CORE)	DISPOSITIVO QUE CONTIENE CONFIGURACION DE LA RED INTERNA DE LA INSTITUCIÓN. SWITCH PRINCIPAL PARA ACCESO A LA LAN E INTERNET.	2	2	4	8	Medio
1020	SER-DHCP-LINUX	CONTROL Y ASIGNACION DE DIRECCIONES IP A PC	2	2	4	8	Medio
1026	ARCHIVO FÍSICO DE COMPROBANTES DE MATRÍCULA	CONTIENE EL REGISTRO DE LA MATRICULA	1	3	3	7	Medio
1011	ARCHIVO FÍSICO DE OFICIOS / CORREOS ELECTRÓNICOS QUE CONTIENEN EL CALENDARIO ACADÉMICO APROBADO POR EL VICERRECTORADO ACADÉMICO	CONTIENE EL DOCUMENTO / CORREO ELECTRÓNICO CON INFORMACION DE LA PLANIFICACIÓN ACADÉMICA DE LA UNIVERSIDAD	1	2	3	6	Medio
1013	ARCHIVO FÍSICO DE OFICIOS CON RESOLUCIONES DE CONSEJO UNIVERSITARIO POR EXCEPCIONES	CONTIENE LAS RESOLUCIONES DE CONSEJO UNIVERSITARIO PARA APLICAR EXCEPCIONES EN PERÍODOS ACADÉMICOS	1	2	3	6	Medio
1022	ARCHIVO FÍSICO DE OFICIOS CON RESOLUCIONES DEL CONSEJO UNIVERSITARIO	CONTIENE RESOLUCIONES PARA APLICAR EXCEPCIONES EN MATRICULACIÓN	1	2	3	6	Medio
1006	SERVIDOR DE RESPALDOS	SERVIDOR QUE CONTIENE LOS RESPALDOS DE LAS DIFERENTES PÁGINAS WEB DE LA INSTITUCIÓN Y BASE DE DATOS	1	2	2	5	Bajo
1009	ROUTER CISCO CNT 1	DISPOSITIVO DE RED PARA EL ACCESO A INTERNET	1	3	1	5	Bajo
1010	ROUTER CISCO CNT 2	DISPOSITIVO DE RED PARA EL ACCESO A INTERNET	1	3	1	5	Bajo

Id. Activo	Activo de información	Descripción	Confidencialidad	Integridad	Disponibilidad	Total	Nivel de criticidad
1008	SWITCH CISCO (SW-CORE) - CONTINGENCIAS	DISPOSITIVO QUE CONTIENE CONFIGURACION DE LA RED INTERNA DE LA INSTITUCIÓN. SWITCH PRINCIPAL PARA ACCESO A LA LAN E INTERNET (CONTINGENCIAS)	1	1	1	3	Bajo
1014	ARCHIVO FÍSICO DE PROGRAMAS MICROCURRICULARES POR ASIGNATURA Y CARRERA	CONTIENE EL SÍLABO DE ASIGNATURAS POR CARRERAS	1	1	1	3	Bajo
1023	OFICIO/EMAIL ESTADO DE CALIFICACIONES POR CARRERA	DOCUMENTO / EMAIL DE CONFIRMACION DE INGRESO DE CALIFICACIONES	1	1	1	3	Bajo
1025	ARCHIVO FÍSICO DE SOLICITUDES PRE-IMPRESAS PARA MATRICULACIÓN	CONTIENE SOLICITUDES PRE-IMPRESAS CON LA INFORMACIÓN DEL ESTUDIANTE	1	1	1	3	Bajo

Para mitigar los riesgos se elaboró un plan de acción en el que se determinaron las tareas a realizarse, los responsables de las mismas y los recursos necesarios; este plan se muestra en el anexo E. El tiempo de implementación de la totalidad de los controles seleccionados es de 17 meses y el presupuesto para su implementación asciende a USD 58,400.00. Es preciso indicar que en este presupuesto no se consideraron los valores de los controles que a la fecha de este proyecto, ya se encuentran implementados en la institución.

5.2 Análisis del plan de acción frente a eventos que generen pérdidas por riesgo operativo: factor tecnología y seguridad de la información

Luego de haber definido el plan de acción para mitigar los riesgos de seguridad de la información, se analizó si la inversión que se debe realizar es aceptable y conveniente desde el punto de vista financiero, y con ello determinar la factibilidad de que el control sea implementado.

Para el efecto, se multiplicó la probabilidad de ocurrencia por el impacto económico del evento de riesgo (tabla 11), lo que permitió evaluar la amenaza y comparar ese resultado con el costo de implementar los controles. Si el costo de implementar las contramedidas es menor al impacto económico obtenido, se determinó que el control es aceptable [20, 21].

Además, se estimó que al aplicar los controles, la probabilidad de ocurrencia se reduciría en un 60% y al multiplicarla por el impacto total, se obtuvo un nuevo nivel del riesgo; si éste es menor que el

riesgo inicial, se concluyó que es conveniente la implementación del control.

En el anexo F “Análisis de la aplicación de controles”, se muestra el resultado de la aplicación de los criterios antes mencionados.

A continuación, se muestra el mapeo de los cuarenta y siete (47) riesgos evaluados en términos de su probabilidad de ocurrencia e impacto sobre los activos de información y procesos críticos asociados, luego de que se apliquen los controles incluidos en el plan de acción.

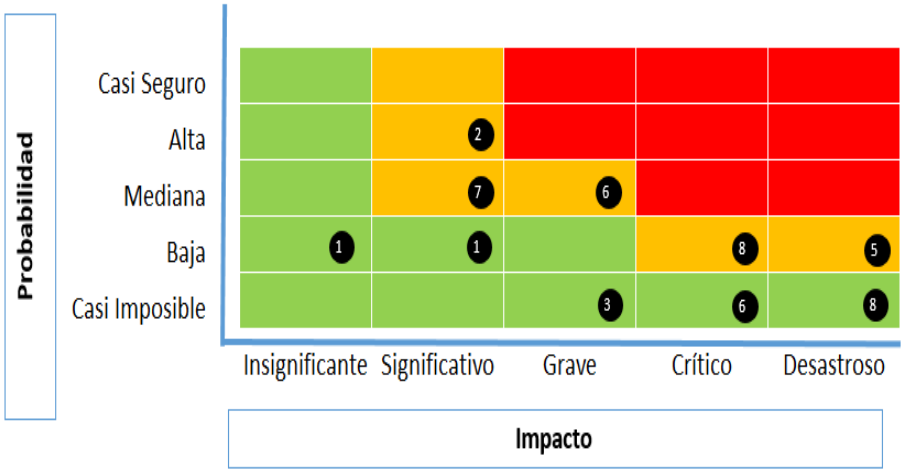


Figura 5.20. Mapa de riesgos luego de aplicar controles

5.3 Mecanismos de monitoreo para asegurar razonablemente la ejecución de controles a implementar

Para asegurar la implementación de los controles seleccionados, fue necesario definir las actividades que se deben realizar para verificar su eficacia y cumplimiento, los responsables del monitoreo y su periodicidad.

Las actividades de monitoreo se centran principalmente en:

- Revisiones y actualizaciones periódicas a políticas internas.
- Seguimiento periódico al cumplimiento de presupuestos.
- Evaluaciones realizadas por el Auditor Interno.
- Evaluaciones independientes por parte del Auditor Externo.
- Revisión de contratos por parte del Procurador Judicial.
- Revisiones realizadas por los propietarios de activos de información.
- Verificación de segregación de funciones.
- Revisión del cumplimiento de los acuerdos de niveles de servicio de proveedores tecnológicos.
- Informes del nivel de cumplimiento del plan de acción.
- Revisión de planes de mitigación de nuevos riesgos detectados.

El detalle de las actividades de monitoreo se muestra en el anexo G "Mecanismos de monitoreo para el cumplimiento de controles".

5.4 Actividades para asegurar que la gestión de riesgos se mantenga como un proceso continuo en el tiempo

La gestión de riesgos institucionales y la continuidad de las operaciones normales de la institución, se encuentran bajo la responsabilidad de la máxima autoridad ejecutiva y el Consejo Universitario; por lo tanto, se debe tener el apoyo y compromiso formal para que el proceso de gestión del riesgo de tecnologías y seguridad de la información, que ha sido denominado PGRTI, se ejecute conforme la periodicidad definida en el capítulo 3 de este trabajo y que sea aprobado en sesión de Consejo Universitario, además de la elaboración y aprobación formal de una política de gestión de riesgos institucionales.

Es necesario se considere cada año un rubro para la implementación de los planes de acción relacionados a la seguridad de la información y que el mismo sea agregado y aprobado en el

presupuesto anual institucional por parte de las instancias pertinentes.

La capacitación y concienciación propuestas en el plan de acción del presente capítulo, son de vital importancia para interiorizar la cultura del riesgo y prevención en la comunidad educativa; situación que coadyuvará a que el proceso de gestión de riesgos se mantenga como un proceso vivo en la institución.

Los indicadores de cumplimiento del PGRTI deben ser revisados con regularidad por parte de la Dirección de Planificación y elevarlos a conocimiento de la máxima autoridad ejecutiva y Consejo Universitario para la oportuna toma de decisiones y mantener el involucramiento de la alta administración.

CAPÍTULO 6

6. RESULTADOS OBTENIDOS DE LA APLICACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS

6.1 Estado de la gestión de riesgos tecnológicos y de seguridad de la información luego de la implementación del proceso

El proceso de gestión de riesgos tecnológicos y de seguridad de la información, no existía en la institución de educación superior en la que se aplicó este proyecto de titulación, es decir, el nivel de madurez era prácticamente nulo en este aspecto; esta fue la razón principal para que la institución acepte emprender en el mismo y consciente de que en un mundo informatizado y automatizado, la gestión del riesgo tecnológico y la seguridad de la información son aspectos que requieren una atención especializada.

A la fecha, la institución cuenta con un proceso documentado para gestionar sus riesgos tecnológicos y de seguridad de la información, lo que posibilita que la gestión de estos riesgos se mantenga como un proceso sostenible en el tiempo y ejecutado por su personal especializado.

Producto de las entrevistas realizadas con el personal técnico, financiero y administrativo de la universidad, inmerso en los procesos soportados por la plataforma de gestión académica, se logró actualizar y en ciertos casos elaborar con las áreas técnicas, los procedimientos y actividades más importantes de los dos procesos seleccionados: planificación académica y matriculación.

Existe un inventario de los principales activos de información necesarios para la ejecución de los procesos antes mencionados, esto permite tener una idea clara de lo que se requiere para que los mismos se encuentren ejecutándose, así como el grado de importancia que tienen estos activos. Así mismo, se tiene una visión clara de qué tan vulnerable es cada activo y su nivel de protección.

Las amenazas y agentes de amenazas se encuentran claramente identificados, lo que facilita tomar acciones preventivas y de forma priorizada.

La institución tiene mapeado los riesgos tecnológicos y de seguridad de la información que podrían afectar a dos de los procesos críticos; cuenta con un presupuesto tentativo y plan de acción de mitigación de los riesgos clasificados como de nivel “Alto” a fin de llevarlos en su mayoría a un nivel “Bajo” o “Medio”.

Por lo antes indicado, este proceso contribuye al cumplimiento del subcriterio “Gestión de la calidad” y al indicador cualitativo “Sistema de información”, así como al subcriterio “Tecnologías de la información y comunicación” definidos por el CEAACES en el *“Modelo de Evaluación Institucional de Universidades y Escuelas Politécnicas”*. Además, de alinearse a las normas de control interno expedidas por la Contraloría General del Estado, en lo relacionado a la administración de riesgos.

6.2 Efectos generados por la gestión de riesgos tecnológicos y de seguridad de la información

Los principales efectos generados por la implementación del proceso de gestión de riesgos tecnológicos y de seguridad de la información fueron:

- Concientizar sobre riesgos y seguridad en la alta administración, así como en el personal involucrado en este trabajo.
- Dar importancia a la gestión de riesgos tecnológicos y a la seguridad de la información, así como a la aplicación de normas internacionales para el efecto.
- Brindar apoyo a las iniciativas que permitan mitigar los riesgos identificados.
- Estar convencidos de que la aplicación del plan de acción propuesto en este trabajo, permitirá mitigar los riesgos y mejorar la gestión administrativa de la institución.
- Motivar la creación de un plan de continuidad del negocio que involucre a toda la institución así como un plan de recuperación ante desastres.
- Posibilidad de justificar la creación de un área especializada en gestión de riesgos institucionales.

6.3 Impacto en la administración de las tecnologías en la institución de educación superior

Los mayores impactos o cambios en la administración de las tecnologías de la información debido a la aplicación del proceso PGRTI, son:

- La gestión de la administración tecnológica es percibida por las autoridades como una inversión, lo que se verá reflejado en un mayor apoyo financiero para la Dirección de Tecnologías de la Información y Comunicación.
- Tener un plan de trabajo para la Dirección de Tecnologías de la Información y Comunicación, enfocado en los aspectos de mayor importancia y riesgo.
- Crear conciencia en el personal del área de Tecnologías de la Información y Comunicación, del por qué y para qué se implementan los controles o contramedidas.
- Pasar de un esquema de trabajo correctivo de “apagar incendios”, a una perspectiva preventiva y de anticiparse a los riesgos.
- Monitorear y evaluar los acuerdos de niveles de servicios mantenidos con los proveedores de TI.

- Reconocer la importancia de establecer políticas y procedimientos de tecnologías de la información y comunicación, así como para la seguridad de la información.

CONCLUSIONES Y RECOMENDACIONES

Lo detallado en los seis capítulos que conforman este documento y al terminar este proyecto, fue posible determinar las siguientes conclusiones:

1. El apoyo y compromiso formal de la alta administración son vitales al emprender un proyecto relacionado a la gestión de riesgos tecnológicos y de seguridad de la información.

2. Crear y aprobar formalmente un proceso es un factor clave para la ejecución y cumplimiento del mismo.

3. La gestión de riesgos tecnológicos y de seguridad de la información permite crear conciencia de riesgos en la alta dirección y en las unidades administrativas que participan en el mismo.

4. La creación de un proceso basado en normas y estándares internacionales mundialmente aceptados, facilita su implementación y aceptación por parte de los interesados.

5. Las herramientas utilizadas a lo largo de este trabajo, facilitan a la Dirección de Tecnologías de la Información y Comunicación, contar con los justificativos técnicos que permitan sustentar las actividades planificadas al corto y mediano plazo.

6. El análisis realizado permitió identificar y medir los riesgos tecnológicos y de seguridad que no habían sido considerados y que de materializarse, podrían afectar a la seguridad de la información de la institución.

7. Las acciones de monitoreo presentadas en el capítulo 5 harán posible conocer el nivel de maduración del proceso implantado, permitiendo fortalecer la mejora continua y ejecución del mismo.

Además, se plantean las siguientes recomendaciones:

1. Se considera necesario crear una política institucional de gestión de riesgos, misma que debe ser aprobada por el Consejo Universitario.

2. La alta dirección de la universidad debe gestionar la aprobación del presupuesto para la implementación de los controles propuestos, dado que permitirán la mitigación de los escenarios de riesgo de nivel “Alto”, es decir, que su probabilidad de ocurrencia e impacto pueden provocar daños severos a la institución.

3. La máxima autoridad ejecutiva y el Consejo Universitario deben velar para que la gestión de riesgos tecnológicos y de seguridad de la información se mantenga como un proceso “vivo” en la institución y no solo como un documento escrito de políticas y procedimientos.

4. Es necesario realizar talleres de capacitación al personal administrativo de la institución y en general a la comunidad académica relacionado a la seguridad de la información.

5. La Dirección de Planificación debería liderar el proceso de gestión de riesgos tecnológicos y de seguridad de la información, dado que ciertos controles y procedimientos para mitigar los riesgos, incluyen contramedidas para amenazas que podrían ser provocadas por personal técnico y especialista de la Dirección de Tecnologías de la Información y Comunicación.

6. El plan de acción propuesto en el capítulo 5 debe elevarse a aprobación del Consejo Universitario para su posterior ejecución.

7. Los riesgos identificados producto de los análisis de ethical hacking y auditorías informáticas internas y externas, deben ser considerados en la próxima iteración en la ejecución del proceso.

8. Analizar la factibilidad de desarrollo o adquisición de software para la administración de riesgos, con la finalidad de generar un repositorio centralizado con la información de los riesgos asociados a los procesos críticos y objetivos del negocio, incidentes o eventos de riesgo que podrían generar alguna pérdida a la institución y las métricas respectivas.

BIBLIOGRAFÍA

[1] Asamblea Nacional de Ecuador, Ley Orgánica de Educación Superior (LOES), 12 de octubre de 2010.

[2] Asamblea Nacional de Ecuador, Constitución del Ecuador, 20 de octubre de 2008.

[3] Contraloría General del Estado de Ecuador, "Normas de control interno para las entidades, organismos del sector público y personas jurídicas de derecho privado que dispongan de recursos públicos", noviembre de 2009.

[4] CEAACES, "Modelo de Evaluación Institucional de Universidades y Escuelas Politécnicas", septiembre de 2015.

[5] UPEL. Venezuela : Universidad Pedagógica Experimental Libertador, página 7, 1998.

[6] Ferrer, J., Conceptos básicos de Metodología de la Investigación, http://metodologia02.blogspot.com/p/tecnicas-de-la-investigacion.html, fecha de consulta 3 de Octubre de 2016

[7] Hernández Sampieri, C. R., *Metodología de la investigación.* México: McGraw-Hill, 2011.

[8] Comité Técnico OB007, AS/NZS 4360:2004 Administración del Riesgo, 31 de agosto de 2004.

[9] Instituto Nacional Electoral de Mexico, Metodología de Administración de Riesgos – Procesos. Sistema de control interno institucional INE, http://norma.ine.mx/documents/27912/1439180/Metodologia +de+Administracion+de+Riesgos+del+Marco+Normativo+de+Control+

Interno+del+Instituto+Nacional+Electoral/02390053-40ce-4e78-b4a6-2b3d8509a253, fecha de consulta 01 de noviembre de 2016.

[10] ISACA: Risk IT, Marco de Riesgos de TI, basado en COBIT (2009), http://www.isaca.org/Knowledge-Center/Research/Documents/Risk-IT-Framework_fmk_Spa_0610.pdf, fecha de consulta 29 de octubre de 2016.

[11] Solís Montes, G., Cobit y la Administración de Riesgos, 2008.

[12] Fuenzalida C. Raúl y Ambrosio P. Eduardo, “Riesgo Tecnológico. Su medición como prioridad para el aseguramiento tecnológico”, https://www.auditool.org/blog/auditoria-de-ti/827-riesgo-tecnologico-su-medicion-como-prioridad-para-el-aseguramiento-del-negocio, fecha de consulta octubre de 2016.

[13] Information Technology Governance Institute, “Information Risks: Whose Business Are They?”, 2005.

[14] Comité de Supervisión Bancaria de Basilea, Buenas prácticas para la gestión y supervisión del riesgo operativo, 2003.

[15] Organización Internacional de Normalización ISO, ISO 31000:2009 Gestión del Riesgo – Principios y Directrices, 2009.

[16] Organización Internacional de Normalización ISO, ISO/IEC 27005:2012 Tecnología de la Información – Técnicas de Seguridad - Gestión del Riesgo en la Seguridad de la Información, 2012.

[17] Institución de educación superior en la que se aplicó el proyecto, Plan Estratégico Institucional de Excelencia 2016 - 2020, 2016.

[18] Dirección de Tecnologías de la Información y Comunicación de la institución de educación superior en la que se aplicó el proyecto, Documentación interna de la Dirección de TIC, noviembre 2016.

[19] Olaya Tapia Jorge, Escuela Superior Politécnica del Litoral - Maestría en Seguridad Informática, material de la asignatura “Planes de Contingencia”, septiembre de 2015.

[20] Palomino Damián, Corporación Élite, material del seminario taller “Seguridad de la información ISO 27002”, noviembre de 2014.

[21] Consejo de Promoción Turística de México, Apéndice IV. A Formatos para los Productos de los procesos del MAAGTICSI, http://www.cptm.com.mx/sites/default/files/documento-de-resultados-del-analisis-de-riesgos-asi-f3_0.pdf, fecha de consulta 10 de noviembre de 2016.

[22] Committee of Sponsoring Organizations of the Treadway Commission, COSO II – ERM, 2004.

[23] Dirección de Planificación de la institución de educación superior en la que se aplicó el proyecto, Documentación interna de la Dirección de Planificación, noviembre 2016.

[24] Pró L. González J. y otros., “Tecnologías Biométricas aplicadas a la seguridad en las organizaciones”, Universidad Nacional Mayor de San Marcos, Perú, 2009.

[25] OWASP Secure Coding Practices Quick Reference Guide, https://www.owasp.org/index.php?title=File:OWASP_SCP_Quick_Reference_Guide_SPA.pdf&setlang=es, fecha de consulta 23 de enero de 2017.

[26] Desiree, Noelia – Edit, Jaquelina. Universidad Nacional del Nordeste. Facultad de Ciencias Exactas, Naturales y Agrimensura. Monografía “Seguridad Informática y Criptografía”, http://exa.unne.edu.ar/informatica/SO/Criptografia04.pdf, fecha de consulta 23 de enero de 2017.

[27] Universidad Nacional Autónoma de México, Facultad de Ingeniería, Laboratorio de redes y seguridad. http://redyseguridad.fip.unam.mx /proyectos/seguridad/ServDisponibilidad.php, fecha de consulta 23 de enero de 2017.

[28] Astudillo B. Karina, libro Hacking Ético 101, 2013.

[29] Microsoft Azure, ¿Qué es la informática en la nube? Guía para principiantes, https://azure.microsoft.com/es-es/overview/what-is-cloud-computing /, fecha de consulta 22 de enero de 2017.

[30] US-CERT United States Computer Emergency Readiness Team, https://www.us-cert.gov/ncas/tips/ST04-006, fecha de consulta 22 de enero de 2017.

[31] Organización Internacional de Normalización ISO, ISO/DIS 22313:2012 Protección y Seguridad de los Ciudadanos – Sistema de Gestión de la Continuidad del Negocio – Directrices, 2012.

[32] Laudon Kennet C. y Laudon Jane P., Sistemas de Información Gerencial – 12da. edición, Pearson 2012.

[33] Organización Internacional de Normalización ISO, ISO 9000:2015 Sistemas de Gestión de la Calidad – Fundamentos y Vocabulario, 2015.

[34] Cisco, “Lo que usted necesita saber sobre routers y switches – Conceptos generales”, http://www.cisco.com/c/dam/global/es_mx/ assets/ofertas/desconectadosanonimos/routing/pdfs/brochure_redes.pdf, fecha de consulta 22 de enero de 2017.

[35] VMWare, “Virtualización – Descripción General” http://www.vmware. com/latam/solutions/virtualization.html, fecha de consulta 22 de enero de 2017.

[36] AXELOS, Glosario y abreviaturas de ITIL Español (latinoamericano) v 1.0, 29 de julio de 2011.

[37] Real Academia Española, Diccionario de la lengua española, http://dle.rae.es, fecha de consulta 22 de enero de 2017.

[38] Uptime Institute, “Sistema de clasificación TIER”, https://es.uptimeinstitute.com/tiers, fecha de consulta 22 de enero de 2017.

[39] Firmesa S.A., “UPS online”, http://firmesa.com/productos/energia /ups-online/computer-power/sy-g-sa-series-1-3-kva, fecha de consulta 22 de enero de 2017.

GLOSARIO

Acceso biométrico: Sistema de reconocimiento estadístico de patrones que establece la autenticidad de una característica fisiológica o de comportamiento que posee un usuario [24].

Adendums: Conjunto de adiciones que se añaden después de terminada una obra escrita.

Agente de amenaza: Cualquier entidad que puede poseer un impacto negativo en el sistema. Puede ser desde un usuario malicioso que desea comprometer los controles de seguridad del sistema; sin embargo, también puede referirse al mal uso accidental del sistema o a una amenaza física como fuego o inundación [25].

Algoritmo: Es un conjunto ordenado y finito de operaciones que se utilizan para la solución de un problema. Se trata de instrucciones o reglas definidas a través de pasos secuenciales que permiten realizar una actividad o resolver un problema.

Aplicación informática: Es un programa o tipo de software que permite al usuario realizar uno o varios tipos de trabajo.

Base de datos: Colección o depósito de datos integrados, con redundancia controlada y con una estructura que refleje las interrelaciones y restricciones existentes en el mundo real.

Certificado digital: Es una garantía emitida por un tercero (autoridad certificadora) de que la firma digital ligada al certificado corresponde a la persona o institución cuyos datos se indica en el certificado. Es una credencial que relaciona un nombre con una clave pública en un paquete firmado por una tercera parte confiable, con un tiempo de validez [26].

Cifrado: Cifrar o encriptar datos significa alterarlos, generalmente mediante el uso de una clave, de modo que no sean legibles para quienes no posean dicha clave. Luego, a través del proceso de descifrado, aquellos que sí poseen la clave podrán utilizarla para obtener la información original. [36]

Código fuente: Es un texto desarrollado en un lenguaje de programación específico, el mismo que debe ser compilado o interpretado para poder ejecutarse en un ordenador.

Conectividad: Es la capacidad de un dispositivo de poder ser conectado, generalmente a un ordenador u otro dispositivo electrónico, en forma autónoma.

Confidencialidad: Propiedad de la información por la que se garantiza que está accesible únicamente a entidades autorizadas [25].

Control criptográfico: Conjunto de técnicas que permiten proteger y ocultar la información del acceso no autorizado, su intercepción, su modificación e inserción de información extra de terceras personas [26].

Crackear: Es el desarrollo y uso de programas informáticos sin autorización de su dueño, cuyo objetivo es modificar el comportamiento del software original accediendo de forma indebida al mismo [38].

Dirección IP: Número único e irrepetible con el que se identifica una computadora conectada a una red de datos que trabaja bajo el protocolo IP.

Disponibilidad: Es un servicio que garantiza que los usuarios autorizados tengan acceso a la información y a otros activos de información en el lugar, momento y forma en que son requeridos [25].

Enlace de red: Es el medio de conexión entre dos lugares con el propósito de transmitir y recibir información. Puede hacer referencia a un conjunto de componentes electrónicos, que consisten en un transmisor, un receptor y el circuito de telecomunicación de datos de interconexión.

Ethical hacking: Conjunto de técnicas de ataque para encontrar fallas de seguridad en el sistema de cómputo, realizadas con la autorización del dueño de la organización quien será el objetivo del ataque; su resultado permitirá mejorar la seguridad [25].

Firewall: Un firewall es un mecanismo de seguridad que puede ser un hardware o software que funciona como cortafuegos entre redes, permitiendo o denegando las transmisiones de una red a otra. Su uso, suele ser entre la red local y la red Internet, como dispositivo de seguridad para evitar que los intrusos puedan acceder a información confidencial [26].

Hacker: Persona experta en tecnologías informáticas, que se dedica a intervenir y/o realizar alteraciones técnicas con malas intenciones y en forma dolosa sobre un sistema informático para dañar, apropiarse, interferir, desviar, difundir, y/o destruir información que se encuentra almacenada en PC [27].

Hardening: Es el proceso de asegurar un sistema mediante la reducción de vulnerabilidades en el mismo, esto significa eliminar software, servicios, usuarios, entre otros; que son innecesarios para el sistema; así como cerrar puertos de comunicación que no estén en uso.

Hardware: Conjunto de componentes físicos del computador, es decir, todo lo que se puede ver y tocar.

Housing: Tipo de contrato en el que una empresa dedicada a la prestación de servicios informáticos se compromete a ubicar en sus instalaciones un determinado hardware propiedad del cliente y a prestar al cliente una serie de servicios adicionales como el mantenimiento del hardware, a cambio de un precio acordado.

IDS: Sistema de detección de intrusos (IDS), es un proceso o dispositivo activo que analiza la actividad del sistema y de la red por entradas no autorizadas y/o actividades maliciosas. Su objetivo es atrapar a los intrusos en el acto antes de que hagan algún daño a los recursos informáticos.

Ingeniería social: Técnica que consiste en la manipulación de las personas para que voluntariamente realicen actos que normalmente no harían. Se refiere a formas de violación que se sustentan en las debilidades de las personas más que en el software. El objetivo es engañar a la gente para que revele contraseñas u otra información que comprometa la seguridad del sistema objetivo [27].

Integridad: La seguridad de que la información es precisa, completa y válida, y no ha sido alterada por una acción no autorizada [25].

Intranet: Es una red de datos privada que está dentro de una empresa, organización o institución. Puede estar conformada por varias redes de área local interconectadas que utilizan una línea para acceder a una red de área amplia. El objetivo principal de una intranet es compartir información de la empresa y los recursos informáticos entre los empleados.

IPS: Sistema de prevención de intrusos, es un software que ejerce el control de acceso en una red informática para proteger a los sistemas computacionales de ataques y abusos.

ISP: Proveedor de servicios de Internet (Internet Service Provider), es una empresa que se encarga de conectar y dar servicio de internet a sus usuarios por algún medio (cable, inalámbrico, satelital, celular, telefónico, etc.).

Macroproceso: Proceso global, de gran alcance e impacto que generalmente es transversal a los objetivos de una unidad o área de trabajo.

Máxima autoridad ejecutiva: Persona titular o representante de más alta jerarquía de una entidad o institución del sector público o privado, sea este el máximo ejecutivo o la dirección colegiada, según lo establecido en su disposición legal o norma de creación.

Medios removibles: También conocidos como medios extraíbles, por ejemplo: memorias USB, discos duros externos, CD, entre otros.

Negación de servicio: Es un tipo de ataque computacional que tiene como objetivo hacer no operativo un servicio informático de cualquier tipo [28].

Nube: Término para referirse a la informática en la nube. Es la entrega de servicios informáticos a través de la internet [29].

Parches del sistema operativo: Son actualizaciones de programas que permiten corregir un problema o vulnerabilidad en un sistema operativo [30].

Plan de continuidad: También conocido como plan de continuidad del negocio, se refiere al conjunto de procedimientos documentados que guían a una organización para responder, recuperar, abreviar y restaurar sus operaciones a un nivel predefinido, luego de una catástrofe [31].

Plataforma de gestión académica: Sistema informático y procedimientos para la gestión de procesos académicos [4].

Plataforma informática: Arquitectura de hardware y software que permite el funcionamiento de una aplicación [32].

Procedimiento: Forma especializada de llevar a cabo una actividad o un procedimiento [33].

Proceso: Conjunto de actividades mutuamente relacionadas que utilizan las entradas para proporcionar un resultado previsto (producto o servicio) [33].

Propietario de activo: Responsable de un activo de información.

Router: Equipo de red para conectar varias redes; pueden protegen la información de amenazas a la seguridad y dar prioridad a los computadores de una red [34].

RPO: Punto de recuperación objetivo por sus siglas en inglés. Punto al cual la información utilizada por una actividad, luego de una interrupción, debe ser restaurada para habilitar o reanudar la actividad. También es conocido como la “máxima pérdida de datos” [31].

RTO: Tiempo de recuperación objetivo por sus siglas en inglés. Es el periodo de tiempo luego de un incidente, en el que una actividad, producto, recurso o servicio debe ser reanudado [31].

Servidor: Computador que está conectado a una red y proporciona funciones de software que son utilizadas por otros equipos [32].

Servidor virtual: Es un servidor donde se ejecutan varios sistemas operativos como máquinas virtuales en un único servidor físico [35].

Sistema de información: Conjunto de componentes relacionados que recolectan, procesan, almacenan y distribuyen información para apoyar los procesos de toma de decisiones y de control en una organización [32].

Sistema operativo: Software que administra los recursos y actividades de la computadora [32].

SLA/Acuerdos de niveles de servicio: Acuerdo entre el proveedor de servicios de tecnología de información y un cliente. Describe los servicios de TI, documenta los objetivos de nivel de servicio, y especifica las responsabilidades del proveedor de servicios [36].

Software: Conjunto de instrucciones programadas que coordinan y controlan el trabajo de los componentes del hardware de computadora en un sistema de información [32].

Switch: Equipo de red para conectar varios dispositivos a través de la misma red dentro de un edificio u oficina [34].

Syllabus: Compendio que abarca el contenido de una materia [37].

TIER: Sistema creado por el Uptime Institute para evaluar y clasificar de manera efectiva la infraestructura de los centros de datos, en términos de los requisitos de disponibilidad de una empresa [38].

UPS: Equipos para proteger a dispositivos críticos de daños producidos por cortes de energía, bajo voltaje, sobre voltaje, ruidos de línea, variaciones de frecuencia y transientes [39].

USB: Universal Serial Bus (bus serial universal), acrónimo del estándar IEEE 1394.

Virus: Programa de software malicioso que se une a otros programas de software o archivos de datos para ejecutarse; con frecuencia provoca fallas en el hardware y el software [32].

Webservices: O servicios web, es el conjunto de estándares universales que utilizan tecnología de internet para integrar distintas aplicaciones provenientes de diferentes fuentes sin la necesidad de utilizar codificación personalizada. Se utiliza para interconectar sistemas de distintas organizaciones o sistemas diferentes en una misma organización [32].

ANEXOS

ANEXO A: Formato de matriz de riesgos tecnológicos y de seguridad de la información

Procesos

Identificación del Proceso "Id. Proceso"	Área	Responsable del proceso	Proceso	Descripción	Actividades	Tipo	Nivel de criticidad	MTPoD	RTO	RPO
[Identificador del proceso]	*[Responsable del proceso]*	*[Cargo del responsable del proceso]*	*[Nombre del proceso]*	*[Descripción del proceso]*	*[Actividades del proceso / subprocesos]*	*Gobernante, productivo o habilitante*	*Alto, medio, bajo*	*Periodo Máximo Tolerable de Interrupción (PMTI)*	*Tiempo de Recuperación Objetivo (RTO)*	*Punto de Recuperación Objetivo (RPO) Cantidad de información que se puede perder, expresada en tiempo.*
0001	Tecnología	Jefe de Producción	Ejecución de procesos automáticos (batch)	Proceso que permite mantener la información diaria actualizada.	Ejecución de procesos. Verificación de la correcta ejecución y término.	Habilitante, de soporte o apoyo	Alto	6 horas	2 horas	4 horas

Activos

ACTIVOS						
Id. Proceso	**Id. Activo**	**Activo de información**	**Descripción**	**Clasificación (crítico/no crítico)**	**Funcionario Responsable**	**Funcionario que Resguarda**
0001	1000	SERVIDOR DE RESPALDOS (GYERESP001)	SERVIDOR QUE MANTIENE LOS RESPALDOS LOCALES DIARIOS DE LA BASE DE DATOS PRINCIPAL.	Crítico	Jefe de Producción	Jefe de Centro de Cómputo Principal
0001	1001	SERVIDOR DE PRODUCCIÓN (GYEPROD001)	SERVIDOR DE PRODUCCIÓN QUE CONTIENE EL SISTEMA PRINCIPAL DE LA COMPAÑÍA.	Crítico	Jefe de Producción	Jefe de Centro de Cómputo Principal

Probabilidad

Amenaza	Descripción de la Amenaza	Agente de la Amenaza	Activo	Descripción del Activo	Probabilidad de existencia del agente amenaza	Nivel de interés del agente amenaza	Nivel de capacidad del agente amenaza	Vulnerabilidad del activo de información	P
[Código de la amenaza]	*[Descripción de la amenaza]*	*[Descripción del agente de amenaza]*	*[Referencia del activo afectado]*	*Descripción del activo*	*[Ponderación de la Tabla 9]*	*[Ponderación de la Tabla 9]*	*[Ponderación de la Tabla 9]*	*[Ponderación de la Tabla 7]*	*[Media aritmética de las 4 columnas anteriores]*

Impacto

Personas	Material	Económico	Procesos	Imagen / Reputación	Impacto
[Ponderación de la tercera columna de la Tabla 11]	*[Ponderación de la cuarta columna de la Tabla 11]*	*[Ponderación de la quinta columna de la Tabla 11]*	*[Ponderación de la sexta columna de la Tabla 11]*	*[Ponderación de la séptima columna de la Tabla 11]*	*[Valor más alto obtenido de las 5 columnas anteriores]*

Nivel de riesgo y controles propuestos

Riesgo	RIESGO	Criterio Aceptación	¿Es necesario un control?	Prioridad	Estrategia	Controles Propuestos
[Valor producto de Probabilidad e Impacto]	*Umbral*	*[Comparar el riesgo con el criterio de aceptación]*	*[**SI** se requiere control cuando el valor de riesgo es mayor que el umbral, caso contrario anotar **NO**]*	*[Asignar sólo **SI** requiere control]*	*[Aceptar, Evitar, Transferir o Mitigar]*	*[Proponer controles y consensuarlos]*

Nivel de riesgo luego de los controles propuestos

Nivel de protección – v' (vulnerabilidad después de aplicar control)	v' (vulnerabilidad después de control)	Nivel de interés del agente amenaza	Nivel de capacidad del agente amenaza	P'	I	Riesgo'	Umbral Riesgo	Criterio Aceptación	¿Requiere control?	Prioridad	Estrategia
[Ponderación de la Tabla 7]	*[Valor resultante de la ponderación de la Tabla 7]*	*[Ponderación de la Tabla 9]*	*[Ponderación de la Tabla 9]*	*[Media aritmética de los valores v',nuevo interés y capacidad,y existencia de agente de ameenaza - [1 - v']*	*[Valor más alto que se haya obtenido del impacto]*	*[Valor resultante producto de la nueva probabilidad e impacto]*	*Umbral*	*[Comparar el valor de Riesgo' con el criterio de aceptación]*	*[**SI** se requiere control cuando el valor de riesgo es mayor que el umbral, caso contrario **NO**]*	*[Solo **SI** requiere contro]*	*[Aceptar, Evitar, Transferir o Mitigar]*

ANEXO B: Inventario de los procesos del macroproceso gestión académica

CÓDIGO	MACROPROCESO	CÓDIGO	PROCESO	CÓDIGO	SUBPROCESO	CÓDIGO	PROCEDIMIENTOS	SALIDA DEL PROCEDIMIENTO
EST	ESTRATÉGICOS	EST-AC	ASEGURAMIENTO DE LA CALIDAD	EST-AC-CA	Aseguramiento de la calidad académica	EST-AC-AC-CD	Seleccionar y contratar docente	Registro en la nómina del personal de los docentes seleccionados y contratados. Contratos/nombramientos de docentes.
MSO	MISIONALES	MSO-DC	DOCENCIA	MSO-DC-PA	Planificación académica	MSO-DC-PA-IC	Iniciar y cerrar periodo académico	Periodo académico vigente
						MSO-DC-PA-RD	Registrar docentes en plataforma	Docentes registrados en plataforma
						MSO-DC-PA-HC	Definir horarios de clase	Distribución de carga horaria
						MSO-DC-PA-OP	Organizar paralelos	Distribución de carga horaria
						MSO-DC-PA-PM	Evaluar y actualizar los programas microcurriculares	Plan analítico de syllabus
						MSO-DC-PA-EA	Administrar políticas y estrategias del proceso de evaluación académica.	Planificación de clases - Registro de notas - Promedios y promociones
						MSO-DC-PA-ED	Planificación y ejecución de evaluación docente.	Docentes evaluados.

CÓDIGO	MACROPROCESO	CÓDIGO	PROCESO	CÓDIGO	SUBPROCESO	CÓDIGO	PROCEDIMIENTOS	SALIDA DEL PROCEDIMIENTO
				MSO-DC-MT	Matriculación	MSO-DC-MT-ME	Registrar la matricula del estudiante	Inicio y cierre de período académico - Registro de matricula
MSO	MISIONALES	MSO-TT	TITULACIÓN	MSO-TT-TI	Titulación	MSO-TT-TI-TG	Dar seguimiento al desarrollo de tesis y graduación	Control de tesis
						MSO-TT-TI-SP	Controlar avance del plan de prácticas pre-profesionales	Control de pasantías y vinculación
						MSO-TT-TI-IG	Mantener actualizada la información de los graduados.	Registro de egresados y graduados

ANEXO C: Procesos soportados por la plataforma informática de gestión académica

Id. Proceso	Área	Responsable del proceso	Proceso	Descripción	Actividades	Tipo	Nivel de criticidad	MTPoD	RTO	RPO
[Identificador del proceso]	*[Responsable del proceso]*	*[Cargo del responsable del proceso]*	*[Nombre del proceso]*	*[Descripción del proceso]*	*[Actividades del proceso / subprocesos]*	*Gobernante, productivo o habilitante*	*Alto, medio, bajo*	*Periodo Máximo Tolerable de Interrupción (PMTI)*	*Tiempo de Recuperación Objetivo (RTO)*	*Punto de Recuperación Objetivo (RPO) Cantidad de información que se puede perder, expresada en tiempo.*
MSO-DC-PA	Decanato	Decano	Planificación académica	Determinar la distribución de la carga horaria y planificación microcurricular.	* Iniciar y cerrar el periodo académico. * Registrar docentes en plataforma. * Definir horarios de clase. * Organizar paralelos. * Evaluar y actualizar los programas microcurriculares. * Administrar políticas y estrategias del proceso de evaluación académica. * Planificación y ejecución de evaluación docente.	Misional: Productivo, fundamental u operativo	Alto	5 días	3 días	1 día

Id. Proceso	Área	Responsable del proceso	Proceso	Descripción	Actividades	Tipo	Nivel de criticidad	MTPoD	RTO	RPO
MSO-DC-MT	Vicerrectorado Académico	Vicerrector Académico	Matriculación	Normar las actividades generadas de la matriculación de los estudiantes de acuerdo al porcentaje de la malla curricular.	* Registrar la matrícula del estudiante.	Misional: Productivo, fundamental u operativo	Alto	4 horas	2 horas	1 día

ANEXO D: Controles propuestos

Amenaza	Descripción de la amenaza	Agente de amenaza	Estrategia	Controles Propuestos	Controles ISO 27001:2013
[Código de la amenaza]	*[Descripción de la amenaza]*	*[Descripción del agente de la amenaza]*	*[Aceptar, Evitar, Transferir o Mitigar]*	*[Mediante técnica de "Tormenta de ideas", proponer controles y consensuar los mismos en el Grupo para la asignación de valores de efectividad: alto, medio o bajo]*	*[Seleccionar y consensuar controles mediante lluvia de ideas]*
1002	Sismo	Natural	Mitigar / Transferir	Póliza de seguros, centro de cómputo alterno, respaldos externos.	A.5.1.1 Políticas para la seguridad de la información A.12.3.1 Respaldo de la información A.17.1.1 Planificación de la continuidad de la seguridad de la información A.17.1.2 Implementación de la continuidad de la seguridad de la información A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información A.17.2.1 Disponibilidad de instalaciones de procesamiento de información
1011	Atentado / terrorismo	Grupo subversivo	Mitigar / Transferir	Pólizas de seguros, centro de cómputo alterno, respaldos externos. Para el caso de los equipos de comunicación del ISP: cláusulas de contratos, acuerdos de niveles de servicio, centro de cómputo alterno.	A.5.1.1 Políticas para la seguridad de la información A.12.3.1 Respaldo de la información A.17.1.1 Planificación de la continuidad de la seguridad de la información A.17.1.2 Implementación de la continuidad de la seguridad de la información A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información A.17.2.1 Disponibilidad de instalaciones de procesamiento de información A.15.1.1 Política de seguridad de la información para las relaciones con proveedores A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores A.15.2.1 Seguimiento y revisión de los servicios de los proveedores

Amenaza	Descripción de la amenaza	Agente de amenaza	Estrategia	Controles Propuestos	Controles ISO 27001:2013
1012	Sabotaje	Personal descontento	Mitigar / Transferir	Pólizas de seguros, centro de cómputo alterno, respaldos externos. Para el caso de los equipos de comunicación del ISP: cláusulas de contratos, acuerdos de niveles de servicio, centro de cómputo alterno.	A.5.1.1 Políticas para la seguridad de la información A.12.3.1 Respaldo de la información A.17.1.1 Planificación de la continuidad de la seguridad de la información A.17.1.2 Implementación de la continuidad de la seguridad de la información A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información A.17.2.1 Disponibilidad de instalaciones de procesamiento de información A.15.1.1 Política de seguridad de la información para las relaciones con proveedores A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores A.15.2.1 Seguimiento y revisión de los servicios de los proveedores

Amenaza	Descripción de la amenaza	Agente de amenaza	Estrategia	Controles Propuestos	Controles ISO 27001:2013
1013	Código malicioso	Hacker	Mitigar	Antivirus, actualización periódica de parches del sistema operativo, monitoreo de cambios en las configuraciones, bloqueo de puertos USB, hardening, ethical hacking al menos una vez al año. Para el caso de los equipos de comunicación del ISP: cláusulas en contratos con CNT y acuerdos de niveles de servicio. Respaldos de ejecutables del sistema académico, control de versiones, control de accesos.	A.5.1.1 Políticas para la seguridad de la información A.12.2.1 Controles contra códigos maliciosos A.10.1.2 Control de llaves A.10.1.1 Política sobre el uso de controles criptográficos A.12.5.1 Instalación de software en sistemas operativos A.8.3.1 Gestión de medios removibles A.12.7.1 Controles de auditorías de sistemas de información A.18.2.1 Revisión independiente de la seguridad de la información A.15.1.1 Política de seguridad de la información para las relaciones con proveedores A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores A.15.2.1 Seguimiento y revisión de los servicios de los proveedores A.9.1.1 Política de control de acceso A.9.2.1 Registro y cancelación del registro de usuarios A.9.2.2 Suministro de acceso de usuarios A.9.2.3 Gestión de derechos de acceso privilegiado A.9.2.4 Gestión de información de autenticación secreta de usuarios A.9.2.5 Revisión de los derechos de acceso de usuarios A.9.2.6 Retiro o ajuste de los derechos de acceso A.9.3.1 Uso de información de autenticación secreta A.9.4.1 Restricción de acceso a la información A.9.4.2 Procedimiento de ingreso seguro A.9.4.3 Sistema de gestión de contraseñas A.14.2.1 Política de desarrollo A.14.2.2 Procedimientos de control de cambios en sistemas A.14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación A.14.2.4 Restricciones en los cambios a los paquetes de software A.14.2.5 Principios de construcción de los sistema seguros A.14.2.6 Ambiente de desarrollo seguro

Amenaza	Descripción de la amenaza	Agente de amenaza	Estrategia	Controles Propuestos	Controles ISO 27001:2013
1015	Fraude	Personal descontento	Mitigar	Control de accesos, IDS/IPS, respaldos, auditoria de aplicaciones, segregación de funciones, control de acceso a código fuente, control de acceso físico.	A.5.1.1 Políticas para la seguridad de la información A.10.1.1 Política sobre el uso de controles criptográficos A.10.1.2 Control de llaves A.9.1.1 Política de control de acceso A.9.1.2 Acceso a redes y a servicios en red A.9.2.1 Registro y cancelación del registro de usuarios A.9.2.2 Suministro de acceso de usuarios A.9.2.3 Gestión de derechos de acceso privilegiado A.9.2.4 Gestión de información de autenticación secreta de usuarios A.9.2.5 Revisión de los derechos de acceso de usuarios A.9.2.6 Retiro o ajuste de los derechos de acceso A.9.3.1 Uso de información de autenticación secreta A.9.4.1 Restricción de acceso a la información A.9.4.2 Procedimiento de ingreso seguro A.9.4.3 Sistema de gestión de contraseñas A.12.3.1 Respaldo de la información A.12.7.1 Controles de auditorías de sistemas de información A.11.1.2 Controles de acceso físico A.12.3.1 Respaldo de la información A.9.4.5 Control de acceso a códigos fuente de programas A.18.2.1 Revisión independiente de la seguridad de la información
1016	Interrupción energía eléctrica	Material (falla)	Mitigar	Generador eléctrico, manual de procedimientos, capacitación al personal.	A.5.1.1 Políticas para la seguridad de la información A.17.2.1 Disponibilidad de instalaciones de procesamiento de información A.12.1.1 Procedimientos de operación documentados A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información

Amenaza	Descripción de la amenaza	Agente de amenaza	Estrategia	Controles Propuestos	Controles ISO 27001:2013
1017	Variaciones de voltaje	Material (falla)	Mitigar	UPS y reguladores de voltaje.	A.5.1.1 Políticas para la seguridad de la información A.17.2.1 Disponibilidad de instalaciones de procesamiento de información
1019	Robo	Personal descontento	Mitigar / Transferir	Control de accesos, respaldos, póliza de seguros, centro de cómputo alterno.	A.11.1.2 Controles de acceso físico A.12.3.1 Respaldo de la información A.5.1.1 Políticas para la seguridad de la información A.17.2.1 Disponibilidad de instalaciones de procesamiento de información
1020	Robo	Delincuencia organizada	Mitigar / Transferir	Acceso biométrico, puerta de acero, cámaras de seguridad al interior y exterior, botón de pánico conectado a una alarma, sensor de movimiento y alertas, pólizas de seguros, cláusulas de contrato y acuerdos de niveles de servicio.	A.11.1.2 Controles de acceso físico A.5.1.1 Políticas para la seguridad de la información A.17.2.1 Disponibilidad de instalaciones de procesamiento de información A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores A.15.2.1 Seguimiento y revisión de los servicios de los proveedores

Amenaza	Descripción de la amenaza	Agente de amenaza	Estrategia	Controles Propuestos	Controles ISO 27001:2013
1028	Modificación no autorizada de información	Personal descontento	Mitigar	Controles de acceso a usuarios, IDS/IPS, respaldos de configuración e información crítica, respaldo de la información en formato digital (escaneada), cláusulas de contratos, acuerdos de niveles de servicio.	A.5.1.1 Políticas para la seguridad de la información A.9.1.1 Política de control de acceso A.9.1.2 Acceso a redes y a servicios en red A.9.2.1 Registro y cancelación del registro de usuarios A.9.2.2 Suministro de acceso de usuarios A.9.2.3 Gestión de derechos de acceso privilegiado A.9.2.4 Gestión de información de autenticación secreta de usuarios A.9.2.5 Revisión de los derechos de acceso de usuarios A.9.2.6 Retiro o ajuste de los derechos de acceso A.9.3.1 Uso de información de autenticación secreta A.9.4.1 Restricción de acceso a la información A.9.4.2 Procedimiento de ingreso seguro A.9.4.3 Sistema de gestión de contraseñas A.12.2.1 Controles contra códigos maliciosos A.12.3.1 Respaldo de la información A.15.2.1 Seguimiento y revisión de los servicios de los proveedores A.11.1.2 Controles de acceso físico

Amenaza	Descripción de la amenaza	Agente de amenaza	Estrategia	Controles Propuestos	Controles ISO 27001:2013
1029	Modificación no autorizada de información	Empleado sin experiencia	Mitigar	Capacitación al personal, controles de acceso, respaldos de configuración e información crítica, manuales de procedimientos, cláusulas de contratos, acuerdos de niveles de servicio, archivar la carpeta con documentos impresos en gavetas con cerradura, control de versiones, control de acceso a código fuente.	A.5.1.1 Políticas para la seguridad de la información A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información A.9.1.1 Política de control de acceso A.9.1.2 Acceso a redes y a servicios en red A.9.2.1 Registro y cancelación del registro de usuarios A.9.2.2 Suministro de acceso de usuarios A.9.2.3 Gestión de derechos de acceso privilegiado A.9.2.4 Gestión de información de autenticación secreta de usuarios A.9.2.5 Revisión de los derechos de acceso de usuarios A.9.2.6 Retiro o ajuste de los derechos de acceso A.9.3.1 Uso de información de autenticación secreta A.9.4.1 Restricción de acceso a la información A.9.4.2 Procedimiento de ingreso seguro A.9.4.3 Sistema de gestión de contraseñas A.12.3.1 Respaldo de la información A.12.1.1 Procedimientos de operación documentados A.12.3.1 Respaldo de la información A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores A.11.1.2 Controles de acceso físico A.9.4.5 Control de acceso a códigos fuente de programas A.14.2.2 Procedimientos de control de cambios en sistemas

Amenaza	Descripción de la amenaza	Agente de amenaza	Estrategia	Controles Propuestos	Controles ISO 27001:2013
1030	Modificación no autorizada de información	Proveedor / Contratista	Mitigar	Controles de acceso a usuarios, IDS/IPS, respaldos de configuración e información crítica, cláusulas de contratos, acuerdos de niveles de servicio, control de acceso a código fuente.	A.5.1.1 Políticas para la seguridad de la información A.9.1.1 Política de control de acceso A.9.1.2 Acceso a redes y a servicios en red A.9.2.1 Registro y cancelación del registro de usuarios A.9.2.2 Suministro de acceso de usuarios A.9.2.3 Gestión de derechos de acceso privilegiado A.9.2.4 Gestión de información de autenticación secreta de usuarios A.9.2.5 Revisión de los derechos de acceso de usuarios A.9.2.6 Retiro o ajuste de los derechos de acceso A.9.3.1 Uso de información de autenticación secreta A.9.4.1 Restricción de acceso a la información A.9.4.2 Procedimiento de ingreso seguro A.9.4.3 Sistema de gestión de contraseñas A.12.2.1 Controles contra códigos maliciosos A.12.3.1 Respaldo de la información A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores A.15.2.1 Seguimiento y revisión de los servicios de los proveedores A.11.1.2 Controles de acceso físico A.9.4.5 Control de acceso a códigos fuente de programas A.18.2.1 Revisión independiente de la seguridad de la información

Amenaza	Descripción de la amenaza	Agente de amenaza	Estrategia	Controles Propuestos	Controles ISO 27001:2013
1031	Modificación no autorizada de información	Ex-empleado	Mitigar	Controles de acceso a usuarios, IDS/IPS, respaldos de configuración e información crítica, cláusulas de contratos, acuerdos de niveles de servicio, control de acceso a código fuente.	A.5.1.1 Políticas para la seguridad de la información A.9.1.1 Política de control de acceso A.9.1.2 Acceso a redes y a servicios en red A.9.2.1 Registro y cancelación del registro de usuarios A.9.2.2 Suministro de acceso de usuarios A.9.2.3 Gestión de derechos de acceso privilegiado A.9.2.4 Gestión de información de autenticación secreta de usuarios A.9.2.5 Revisión de los derechos de acceso de usuarios A.9.2.6 Retiro o ajuste de los derechos de acceso A.9.3.1 Uso de información de autenticación secreta A.9.4.1 Restricción de acceso a la información A.9.4.2 Procedimiento de ingreso seguro A.9.4.3 Sistema de gestión de contraseñas A.12.2.1 Controles contra códigos maliciosos A.12.3.1 Respaldo de la información A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores A.15.2.1 Seguimiento y revisión de los servicios de los proveedores A.11.1.2 Controles de acceso físico A.9.4.5 Control de acceso a códigos fuente de programas A.18.2.1 Revisión independiente de la seguridad de la información

Amenaza	Descripción de la amenaza	Agente de amenaza	Estrategia	Controles Propuestos	Controles ISO 27001:2013
1035	Respaldos defectuosos	Empleado sin experiencia	Mitigar	Capacitación al personal, manuales de procedimientos, cláusulas de contratos, acuerdos de niveles de servicio, centro de cómputo alterno.	A.5.1.1 Políticas para la seguridad de la información A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información A.12.1.1 Procedimientos de operación documentados A.12.3.1 Respaldo de la información A.15.2.1 Seguimiento y revisión de los servicios de los proveedores A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores A.17.2.1 Disponibilidad de instalaciones de procesamiento de información
1038	Fallas estructurales del edificio	Empleado sin experiencia	Mitigar	Capacitación al personal, manuales de procedimientos, póliza de seguros, centro de cómputo alterno, respaldos externos, cláusulas de contratos, acuerdos de niveles de servicio.	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información A.12.1.1 Procedimientos de operación documentados A.5.1.1 Políticas para la seguridad de la información A.17.2.1 Disponibilidad de instalaciones de procesamiento de información A.12.3.1 Respaldo de la información A.15.2.1 Seguimiento y revisión de los servicios de los proveedores
1041	Virus en las redes o computadoras	Hacker	Mitigar	Antivirus corporativo, IDS/IPS, cláusulas de contratos, acuerdos de niveles de servicio.	A.12.2.1 Controles contra códigos maliciosos A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores A.15.2.1 Seguimiento y revisión de los servicios de los proveedores
1042	Virus en las redes o computadoras	Personal descontento	Mitigar	Antivirus corporativo, IDS / IPS, cláusulas de contratos y acuerdos de niveles de servicio.	A.5.1.1 Políticas para la seguridad de la información A.8.3.1 Gestión de medios removibles A.12.2.1 Controles contra códigos maliciosos A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores A.15.2.1 Seguimiento y revisión de los servicios de los proveedores A.8.3.1 Gestión de medios removibles

Amenaza	Descripción de la amenaza	Agente de amenaza	Estrategia	Controles Propuestos	Controles ISO 27001:2013
1048	UPS defectuoso o sin mantenimiento	Personal descontento	Mitigar	Pólizas de seguros, centro de cómputo alterno, respaldos externos, contrato de mantenimiento periódico, cláusulas de contratos, acuerdos de niveles de servicio.	A.5.1.1 Políticas para la seguridad de la información A.17.2.1 Disponibilidad de instalaciones de procesamiento de información A.12.3.1 Respaldo de la información A.11.2.4 Mantenimiento de equipos A.15.2.1 Seguimiento y revisión de los servicios de los proveedores

ANEXO E: Plan de acción para mitigación de riesgos

Controles ISO 27001:2013 a implementar							
Control	**Riesgo mitigado**	**Descripción**	**Responsables**	**Presupuesto estimado**	**Tiempo**	**Inicio**	**Fin**
A.5.1.1 Políticas para la seguridad de la información	Todos los riesgos	La universidad establecerá un conjunto de políticas para la seguridad de la información, aprobada por la alta dirección, y deberá ser publicada y socializada a la comunidad educativa, personal administrativo y a las partes externas pertinentes.	Director de Planificación Director de Tecnologías de la Información y Comunicación Consejo Universitario	-	3 meses	01-mar-17	31-may-17
A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información	Interrupción energía eléctrica Modificación no autorizada de información Respaldos defectuosos Fallas estructurales del edificio	Planes de educación y capacitación para concientizar sobre la seguridad de la información al personal interno y proveedores externos que sean necesarios, así como dar a conocer la existencia y cambios en las políticas de seguridad de la información vigentes. Capacitación masiva a la comunidad académica. Capacitación especializada al área de TIC y Planificación.	Director de Planificación Director de Comunicación Social Director General de Servicios Institucionales Director de Desarrollo de Talento Humano Director de Tecnologías de la Información y Comunicación	8,000.00	10 meses	01-may-17	31-mar-18

Controles ISO 27001:2013 a implementar							
Control	**Riesgo mitigado**	**Descripción**	**Responsables**	**Presupuesto estimado**	**Tiempo**	**Inicio**	**Fin**
A.8.3.1 Gestión de medios removibles	Código malicioso Virus en las redes o computadoras	Definir y aprobar procedimientos para la gestión y uso de medios extraíbles, tales como: memorias USB, discos duros externos, CD, DVD, etc.	Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales	-	2 semanas	01-may-17	12-may-17
A.9.1.1 Política de control de acceso	Código malicioso Fraude Modificación no autorizada de información	Establecer, documentar, revisar y aprobar una política de control de accesos a los activos de información de la institución.	Director de Planificación Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales Consejo Universitario	-	2 meses	01-abr-17	31-may-17
A.9.1.2 Acceso a redes y a servicios en red	Fraude Modificación no autorizada de información	Se debe permitir el acceso a la red institucional únicamente a los usuarios autorizados conforme a las políticas de control de acceso.	Director de Tecnologías de la Información y Comunicación Todas las áreas	-	2 meses	01-ago-17	30-sep-17
A.9.2.1 Registro y cancelación de usuarios	Código malicioso Fraude Modificación no autorizada de información	Definición y aprobación de un procedimiento para la administración de usuarios.	Director de Tecnologías de la Información y Comunicación Director General de Servicios	-	2 meses	01-ago-17	30-sep-17

Controles ISO 27001:2013 a implementar							
Control	**Riesgo mitigado**	**Descripción**	**Responsables**	**Presupuesto estimado**	**Tiempo**	**Inicio**	**Fin**
			Institucionales				
A.9.2.2 Suministro de acceso de usuarios	Código malicioso Fraude Modificación no autorizada de información	Definición y aprobación de un procedimiento para la administración de usuarios.	Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales	-	2 meses	01-ago-17	30-sep-17
A.9.2.3 Gestión de derechos de acceso privilegiado	Código malicioso Fraude Modificación no autorizada de información	Definición y aprobación de un procedimiento para la administración de usuarios.	Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales	-	2 meses	01-ago-17	30-sep-17
A.9.2.4 Gestión de información de autenticación secreta de usuarios	Modificación no autorizada de información Código malicioso Fraude	Definición y aprobación de un procedimiento para la administración de usuarios.	Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales	-	2 meses	01-ago-17	30-sep-17

Controles ISO 27001:2013 a implementar							
Control	**Riesgo mitigado**	**Descripción**	**Responsables**	**Presupuesto estimado**	**Tiempo**	**Inicio**	**Fin**
A.9.2.5 Revisión de los derechos de acceso de usuarios	Código malicioso Fraude Modificación no autorizada de información	Definir y aprobar un procedimiento para la revisión periódica de los derechos de acceso de usuarios por parte de los propietarios de los activos de información.	Director de Planificación Director General de Servicios Institucionales Director de Tecnología Propietarios de los activos de información	-	10 semanas	15-jun-17	31-ene-18
A.9.2.6 Retiro o ajuste de los derechos de acceso	Código malicioso Fraude Modificación no autorizada de información	Definir y aprobar un procedimiento para la revocación de derechos de acceso de los usuarios al terminar su empleo o vinculación con la institución.	Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales	-	2 semanas	01-ago-17	15-ago-17
A.9.3.1 Uso de información de autenticación secreta	Código malicioso Fraude Modificación no autorizada de información	Concientizar y exigir al personal cumplir con las políticas de resguardo de su información secreta, tales como: usuarios, claves, etc.	Director de Planificación Director de Comunicación Social Director General de Servicios Institucionales Director de Desarrollo de Talento Humano Director de Tecnologías de la Información y	-	10 meses	01-may-17	31-mar-18

Controles ISO 27001:2013 a implementar							
Control	**Riesgo mitigado**	**Descripción**	**Responsables**	**Presupuesto estimado**	**Tiempo**	**Inicio**	**Fin**
			Comunicación				
A.9.4.1 Restricción de acceso a la información	Código malicioso Fraude Modificación no autorizada de información	Definición y aprobación de un procedimiento para la administración de usuarios.	Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales	-	2 meses	01-ago-17	30-sep-17
A.9.4.2 Procedimiento de ingreso seguro	Código malicioso Fraude Modificación no autorizada de información	Se debe solicitar usuario y contraseña al ingresar a los sistemas y aplicaciones.	Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales	-	Implementado		
A.9.4.3 Sistema de gestión de contraseñas	Código malicioso Fraude Modificación no autorizada de información	Verificar que los sistemas y aplicaciones se encuentran configurados para asegurar la gestión de contraseñas, tales como: complejidad de contraseñas, periodicidad de cambio de contraseñas, intentos	Director de Tecnologías de la Información y Comunicación	-	1 mes	01-oct-17	31-oct-17

Controles ISO 27001:2013 a implementar							
Control	**Riesgo mitigado**	**Descripción**	**Responsables**	**Presupuesto estimado**	**Tiempo**	**Inicio**	**Fin**
		de accesos fallidos, histórico de contraseñas, entre otros, conforme a la política aprobada.					
A.9.4.5 Control de acceso a códigos fuente de programas	Fraude Modificación no autorizada de información	El acceso al código fuente de los programas debe ser restringido únicamente a usuarios autorizados.	Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales	-	2 semanas	01-nov-17	15-nov-17
A.10.1.1 Política sobre el uso de controles criptográficos	Código malicioso Fraude	Definir y aprobar una política para el uso de controles criptográficos, tales como: certificados digitales, cifrado de claves, etc.	Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales	1,000.00	2 meses	16-nov-17	16-ene-18
A.10.1.2 Control de llaves	Código malicioso Fraude	Desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas.	Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales	-	2 meses	16-nov-17	16-ene-18

Controles ISO 27001:2013 a implementar							
Control	**Riesgo mitigado**	**Descripción**	**Responsables**	**Presupuesto estimado**	**Tiempo**	**Inicio**	**Fin**
A.11.1.2 Controles de acceso físico	Fraude Robo Modificación no autorizada de información	Implementación de controles de acceso y protección física, tales como: acceso biométrico, puerta de acero, cámaras de seguridad al interior y exterior, botón de pánico conectado a una alarma, sensor de movimiento y alertas, pólizas de seguros, cláusulas de contrato y acuerdos de niveles de servicio con proveedores ISP. Para el caso de archivadores: cerraduras con llave.	Director General de Servicios Institucionales Director de Planificación	20,000.00	4 meses	30-nov-17	30-abr-18
A.11.2.4 Mantenimiento de equipos	UPS defectuoso o sin mantenimiento	Plan de mantenimiento de equipos de cómputo. Contrato con el proveedor para el mantenimiento del UPS.	Director de Tecnologías de la Información y Comunicación Jefe de Infraestructura	-	Implementado		
A.12.1.1 Procedimientos de operación documentados	Interrupción energía eléctrica Modificación no autorizada de información Respaldos defectuosos Fallas	Documentar los procedimientos del área de Tecnología, incluidos los procedimientos de gestión de la seguridad física y lógica.	Director de Planificación Director de Tecnologías de la Información y Comunicación Director General de Servicios	-	6 meses	01-jul-17	31-dic-17

Controles ISO 27001:2013 a implementar							
Control	**Riesgo mitigado**	**Descripción**	**Responsables**	**Presupuesto estimado**	**Tiempo**	**Inicio**	**Fin**
	estructurales del edificio		Institucionales				
A.12.1.2 Gestión de cambios	Código malicioso	Documentar los procedimientos del área de Tecnología, incluidos los procedimientos de gestión de la seguridad física y lógica.	Director de Planificación Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales	-			
A.12.2.1 Controles contra códigos maliciosos	Código malicioso Modificación no autorizada de información Virus en las redes o computadoras	Adquisición y configuración de antivirus corporativo para todos los equipos de la red institucional. Revisión y actualización de las reglas del firewall existente.	Director de Tecnologías de la Información y Comunicación	5,000.00	2 meses	01-may-17	30-jun-17

Controles ISO 27001:2013 a implementar							
Control	**Riesgo mitigado**	**Descripción**	**Responsables**	**Presupuesto estimado**	**Tiempo**	**Inicio**	**Fin**
A.12.3.1 Respaldo de la información	Sismo Atentado / terrorismo Sabotaje Fraude Robo Modificación no autorizada de información Respaldos defectuosos Fallas estructurales del edificio UPS defectuoso o sin mantenimiento	Implementar procedimientos de respaldos periódicos de información para los diferentes activos seleccionados, en función de los requerimientos de disponibilidad y continuidad del negocio.	Director de Planificación Director de Tecnologías de la Información y Comunicación Propietarios de activos de información Jefe de Infraestructura	-	1 mes	01-jun-17	30-jun-17
A.12.5.1 Instalación de software en sistemas operativos	Código malicioso	Configurar mediante reglas del Directorio Activo existente, restricciones para instalación de software no autorizado.	Director de Tecnologías de la Información y Comunicación Jefe de Infraestructura	-	1 semana	02-oct-17	13-oct-17
A.12.7 Controles de auditorías de sistemas de información	Código malicioso Fraude	Ejecución de auditorías de sistemas, al menos una vez al año.	Director de Planificación Consejo Universitario	4,000.00	2 meses	01-mar-18	30-abr-18

Controles ISO 27001:2013 a implementar							
Control	**Riesgo mitigado**	**Descripción**	**Responsables**	**Presupuesto estimado**	**Tiempo**	**Inicio**	**Fin**
A.14.2.1 Política de desarrollo	Código malicioso	Elaborar una política que incluya las directrices para el desarrollo de sistemas en la institución.	Director de Planificación Director de Tecnologías de la Información y Comunicación Jefe de Desarrollo Director General de Servicios Institucionales	-	2 meses	01-ago-17	30-sep-17
A.14.2.2 Procedimientos de control de cambios en sistemas	Código malicioso Modificación no autorizada de información	Implementar procedimientos formales de control de cambios como parte de la política de desarrollo de sistemas.	Director de Planificación Director de Tecnologías de la Información y Comunicación Jefe de Desarrollo Director General de Servicios Institucionales	-	2 meses	01-ago-17	30-sep-17
A.14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Código malicioso	Implementar procedimientos formales para la revisión de aplicaciones como parte de las políticas de desarrollo de sistemas, a fin de probar que no existan impactos adversos o que afecten a	Director de Planificación Director de Tecnologías de la Información y Comunicación Jefe de Desarrollo Director General	-	2 meses	01-ago-17	30-sep-17

Controles ISO 27001:2013 a implementar							
Control	**Riesgo mitigado**	**Descripción**	**Responsables**	**Presupuesto estimado**	**Tiempo**	**Inicio**	**Fin**
		la seguridad de la información.	de Servicios Institucionales				
A.14.2.4 Restricciones en los cambios a los paquetes de software	Código malicioso	Incluir en la política de desarrollo, restricciones en los cambios a los paquetes de software.	Director de Planificación Director de Tecnologías de la Información y Comunicación Jefe de Desarrollo Director General de Servicios Institucionales	-	2 meses	01-ago-17	30-sep-17
A.14.2.5 Principios de construcción de los sistema seguros	Código malicioso	Establecer, documentar, y mantener principios para la construcción de sistemas seguros y aplicarlos a cualquier actividad de implementación de sistemas.	Director de Planificación Director de Tecnologías de la Información y Comunicación Jefe de Desarrollo Director General de Servicios Institucionales	-	2 meses	01-ago-17	30-sep-17

Controles ISO 27001:2013 a implementar							
Control	**Riesgo mitigado**	**Descripción**	**Responsables**	**Presupuesto estimado**	**Tiempo**	**Inicio**	**Fin**
A.14.2.6 Ambiente de desarrollo seguro	Código malicioso	Mantener segregados los ambientes de pruebas y producción con los debidos controles de acceso.	Director de Planificación Director de Tecnologías de la Información y Comunicación Jefe de Desarrollo Director General de Servicios Institucionales	-	Implementado		
A.15.1.1 Política de seguridad de la información para las relaciones con proveedores	Atentado / terrorismo Sabotaje Código malicioso	Definir los requerimientos de seguridad de la información que se deben solicitar a los proveedores y que deben ser incluidos en las nuevas contrataciones o adéndums.	Director de Planificación Procurador Judicial Director de Tecnologías de la Información y Comunicación	-	1 mes	01-nov-17	30-nov-17

Controles ISO 27001:2013 a implementar							
Control	**Riesgo mitigado**	**Descripción**	**Responsables**	**Presupuesto estimado**	**Tiempo**	**Inicio**	**Fin**
A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores	Atentado / terrorismo Sabotaje Código malicioso Robo Modificación no autorizada de información Respaldos defectuosos Virus en las redes o computadoras	Definir los requerimientos de seguridad de la información que se deben solicitar a los proveedores y que deben ser incluidos en las nuevas contrataciones o adendums.	Director de Planificación Procurador Judicial Director de Tecnologías de la Información y Comunicación	-	1 mes	01-nov-17	30-nov-17
A.15.2.1 Seguimiento y revisión de los servicios de los proveedores	Atentado / terrorismo Sabotaje Código malicioso Robo Modificación no autorizada de información Respaldos defectuosos Fallas estructurales del edificio Virus en las redes o computadoras UPS defectuoso o sin mantenimiento	Verificar que se cumplan los acuerdos de niveles de servicio para los proveedores: ISP y la compañía que brinda el mantenimiento a los UPS.	Director de Tecnologías de la Información y Comunicación	-	2 meses	01-ago-2017 01-feb-2018	31-ago-2017 28-feb-2018

Controles ISO 27001:2013 a implementar							
Control	**Riesgo mitigado**	**Descripción**	**Responsables**	**Presupuesto estimado**	**Tiempo**	**Inicio**	**Fin**
A.17.1.1 Planificación de la continuidad de la seguridad de la información	Sismo / Atentado terrorismo Sabotaje	Elaborar el plan de continuidad que incluya los requerimientos de seguridad de la información.	Director de Planificación Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales Consejo Universitario	8,000.00	6 meses	01-feb-18	31-jul-18
A.17.1.2 Implementación de la continuidad de la seguridad de la información	Sismo / Atentado terrorismo Sabotaje	La universidad debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	Director de Planificación Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales Consejo Universitario	-	6 meses	01-feb-18	31-jul-18
A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Sismo / Atentado terrorismo Sabotaje	Definir procedimientos de verificación periódica de los controles de continuidad de la seguridad de la información establecidos e implementados, para asegurar que son válidos y eficaces en situaciones	Director de Planificación Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales	-	6 meses	01-feb-18	31-jul-18

Controles ISO 27001:2013 a implementar							
Control	**Riesgo mitigado**	**Descripción**	**Responsables**	**Presupuesto estimado**	**Tiempo**	**Inicio**	**Fin**
		adversas.	Consejo Universitario				
A.17.2.1 Disponibilidad de instalaciones de procesamiento de información	Sismo Atentado / terrorismo Sabotaje Interrupción energía eléctrica Variaciones de voltaje Robo Respaldos defectuosos Fallas estructurales del edificio UPS defectuoso o sin mantenimiento	Contratación de un housing para la implementación de un centro de datos alterno con ISP que mantenga un centro de datos al menos de categoría TIER III.	Director de Planificación Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales Consejo Universitario	10,000.00	2 meses	01-feb-18	31-mar-18
A.18.2.1 Revisión independiente de la seguridad de la información	Código malicioso Fraude Modificación no autorizada de información	Contratar un análisis de ethical hacking al menos una vez al año.	Director de Planificación Consejo Universitario	2,000.00	1 mes	01-abr-18	30-abr-18

ANEXO F: Análisis de la aplicación de controles

Código de amenaza	Amenaza	Agente de amenaza	R	Control ISO 27001:2013	Costo	P	I (USD)	R (USD)	¿Se acepta control? Costo<=R (USD)	P'	I'	R'	¿Es conveniente? R (USD) >R'	¿Se recomienda el control?
1013	Código malicioso	Hacker	8	A.10.1.1 Política sobre el uso de controles criptográficos A.12.2.1 Controles contra códigos maliciosos A.12.7 Controles de auditorías de sistemas de información A.18.2.1 Revisión independiente de la seguridad de la información	12,000	0.80	450,000	360,000	ACEPTABLE	0.32	8	2.56	CONVENIENTE	SI
1020	Robo	Delincuencia organizada	7	A.11.1.2 Controles de acceso físico A.17.2.1 Disponibilidad de instalaciones de procesamiento de información	30,400	0.71	450,000	319,500	ACEPTABLE	0.28	7	1.99	CONVENIENTE	SI

Código de amenaza	Amenaza	Agente de amenaza	R	Control ISO 27001:2013	Costo	P	I (USD)	R (USD)	¿Se acepta control? Costo<=R (USD)	P'	I'	R'	¿Es conveniente? R (USD) >R'	¿Se recomienda el control?
1029	Modificación no autorizada de información	Empleado sin experiencia	7	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información A.11.1.2 Controles de acceso físico A.12.2.1 Controles contra códigos maliciosos A.18.2.1 Revisión independiente de la seguridad de la información	35,400	0.67	450,000	301,500	ACEPTABLE	0.27	7	1.88	CONVENIENTE	SI
1028	Modificación no autorizada de información	Personal descontento	6	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información A.11.1.2 Controles de acceso físico A.12.2.1 Controles contra códigos maliciosos A.18.2.1 Revisión independiente	35,400	0.62	450,000	279,000	ACEPTABLE	0.25	6	1.49	CONVENIENTE	SI

Código de amenaza	Amenaza	Agente de amenaza	R	Control ISO 27001:2013	Costo	P	I (USD)	R (USD)	¿Se acepta control? Costo<=R (USD)	P'	I'	R'	¿Es conveniente? R (USD) >R'	¿Se recomienda el control?
				de la seguridad de la información										
1031	Modificación no autorizada de información	Ex–empleado	6	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información A.11.1.2 Controles de acceso físico A.12.2.1 Controles contra códigos maliciosos A.18.2.1 Revisión independiente de la seguridad de la información	35,400	0.62	450,000	279,000	ACEPTABLE	0.25	6	1.49	CONVENIENTE	SI

Código de amenaza	Amenaza	Agente de amenaza	R	Control ISO 27001:2013	Costo	P	I (USD)	R (USD)	¿Se acepta control? Costo<=R (USD)	P'	I'	R'	¿Es conveniente? R (USD) >R'	¿Se recomienda el control?
1041	Virus en las redes o computadoras	Hacker	6	A.12.2.1 Controles contra códigos maliciosos	5,000	0.80	90,000	72,000	ACEPTABLE	0.32	6	1.92	CONVENIENTE	SI
1012	Sabotaje	Personal descontento	5	A.12.3.1 Respaldo de la información A.17.1.1 Planificación de la continuidad de la seguridad de la información A.17.1.2 Implementación de la continuidad de la seguridad de la información A.17.2.1 Disponibilidad de instalaciones de procesamiento de información	18,400	0.62	450,000	279,000	ACEPTABLE	0.25	5	1.24	CONVENIENTE	SI
1042	Virus en las redes o computadoras	Personal descontento	5	A.12.2.1 Controles contra códigos maliciosos	5,000	0.60	90,000	54,000	ACEPTABLE	0.24	5	1.2	CONVENIENTE	SI

Código de amenaza	Amenaza	Agente de amenaza	R	Control ISO 27001:2013	Costo	P	I (USD)	R (USD)	¿Se acepta control? Costo<=R (USD)	P'	I'	R'	¿Es conveniente? R (USD) >R'	¿Se recomienda el control?
1011	Atentado / terrorismo	Grupo subversivo	5	A.12.3.1 Respaldo de la información A.17.1.1 Planificación de la continuidad de la seguridad de la información A.17.2.1 Disponibilidad de instalaciones de procesamiento de información	18,400	0.47	675,000	317,250	ACEPTABLE	0.19	5	0.94	CONVENIENTE	SI
1038	Fallas estructurales del edificio	Empleado sin experiencia	4	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información A.12.3.1 Respaldo de la información A.17.2.1 Disponibilidad de instalaciones de procesamiento de información	18,400	0.42	450,000	189,000	ACEPTABLE	0.17	4	0.67	CONVENIENTE	SI

Código de amenaza	Amenaza	Agente de amenaza	R	Control ISO 27001:2013	Costo	P	I (USD)	R (USD)	¿Se acepta control? Costo<=R (USD)	P'	I'	R'	¿Es conveniente? R (USD) >R'	¿Se recomienda el control?
1030	Modificación no autorizada de información	Proveedor / Contratista	4	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información A.11.1.2 Controles de acceso físico A.12.2.1 Controles contra códigos maliciosos A.18.2.1 Revisión independiente de la seguridad de la información	35,000	0.42	450,000	189,000	ACEPTABLE	0.17	4	0.67	CONVENIENTE	SI
1035	Respaldos defectuosos	Empleado sin experiencia	4	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información A.12.3.1 Respaldo de la información A.17.2.1 Disponibilidad de instalaciones de procesamiento de información	18,400	0.40	225,000	90,000	ACEPTABLE	0.16	4	0.64	CONVENIENTE	SI

Código de amenaza	Amenaza	Agente de amenaza	R	Control ISO 27001:2013	Costo	P	I (USD)	R (USD)	¿Se acepta control? Costo<=R (USD)	P'	I'	R'	¿Es conveniente? R (USD) >R'	¿Se recomienda el control?
1002	Sismo	Natural	4	A.12.3.1 Respaldo de la información A.17.1.1 Planificación de la continuidad de la seguridad de la información A.17.2.1 Disponibilidad de instalaciones de procesamiento de información	18,400	0.40	675,000	270,000	ACEPTABLE	0.16	4	0.64	CONVENIENTE	SI
1019	Robo	Personal descontento	4	A.11.1.2 Controles de acceso físico A.17.2.1 Disponibilidad de instalaciones de procesamiento de información	30,400	0.64	225,000	144,000	ACEPTABLE	0.26	4	1.02	CONVENIENTE	SI
1048	UPS defectuoso o sin mantenimiento	Personal descontento	4	A.12.3.1 Respaldo de la información A.17.2.1 Disponibilidad de instalaciones de procesamiento	10,400	0.60	90,000	54,000	ACEPTABLE	0.24	4	0.96	CONVENIENTE	SI

Código de amenaza	Amenaza	Agente de amenaza	R	Control ISO 27001:2013	Costo	P	I (USD)	R (USD)	¿Se acepta control? Costo<=R (USD)	P'	I'	R'	¿Es conveniente? R (USD) >R'	¿Se recomienda el control?
				de información										
1015	Fraude	Personal descontento	4	A.10.1.1 Política sobre el uso de controles criptográficos A.11.1.2 Controles de acceso físico A.12.3.1 Respaldo de la información A.12.7 Controles de auditorías de sistemas de información A.18.2.1 Revisión independiente de la seguridad de la información	27,400	0.63	225,000	141,750	ACEPTABLE	0.25	4	1.00	CONVENIENTE	SI

Código de amenaza	Amenaza	Agente de amenaza	R	Control ISO 27001:2013	Costo	P	I (USD)	R (USD)	¿Se acepta control? Costo<=R (USD)	P'	I'	R'	¿Es conveniente? R (USD) >R'	¿Se recomienda el control?
1016	Interrupción energía eléctrica	Material (falla)	4	A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información A.17.2.1 Disponibilidad de instalaciones de procesamiento de información	18,000	0.45	450,000	202,500	ACEPTABLE	0.18	4	0.72	CONVENIENTE	SI
1017	Variaciones de voltaje	Material (falla)	4	A.17.2.1 Disponibilidad de instalaciones de procesamiento de información	10,000	0.45	450,000	202,500	ACEPTABLE	0.18	4	0.72	CONVENIENTE	SI
1037	Negación de servicio	Empleado sin experiencia	4	A.11.1.2 Controles de acceso físico A.12.2.1 Controles contra códigos maliciosos A.17.2.1 Disponibilidad de instalaciones de procesamiento de información	35,000	0.45	90,000	40,500	ACEPTABLE	0.18	4	0.72	CONVENIENTE	SI

Código de amenaza	Amenaza	Agente de amenaza	R	Control ISO 27001:2013	Costo	P	I (USD)	R (USD)	¿Se acepta control? Costo<=R (USD)	P'	I'	R'	¿Es conveniente? R (USD) >R'	¿Se recomienda el control?
1043	Virus en las redes o computadoras	Empleado sin experiencia	4	A.12.2.1 Controles contra códigos maliciosos	5,000	0.45	90,000	40,500	ACEPTABLE	0.18	4	0.72	CONVENIENTE	SI

ANEXO G: Mecanismos de monitoreo para el cumplimiento de controles

Control	Descripción del control	Responsables de implementación del control	Mecanismo de monitoreo	Descripción mecanismo de monitoreo	Periodicidad	Responsable monitoreo
A.5.1.1 Políticas para la seguridad de la información	La institución definirá un conjunto de políticas para la seguridad de la información, aprobada por la dirección, publicada y comunicada a los colaboradores y a las partes externas pertinentes.	Director de Planificación Director de Tecnologías de la Información y Comunicación Consejo Universitario	Revisión y actualización periódica de políticas de seguridad de la información.	Las políticas de seguridad de la información deben ser revisadas para verificar su conveniencia, adecuación y eficacia.	Al menos 1 vez al año	Director de Planificación Director de Tecnologías de Información y Comunicación Consejo Universitario
A.7.2.2 Toma de conciencia, educación y formación en la seguridad de la información	Planes de educación y capacitación para concientizar sobre la seguridad de la información al personal interno y proveedores externos que sean necesarios, así como dar a conocer la existencia y cambios en las políticas de seguridad de la información vigentes. Capacitación masiva a la comunidad académica. Capacitación	Director de Planificación Director de Comunicación Social Director General de Servicios Institucionales Director de Desarrollo de Talento Humano Director de Tecnologías de la Información y Comunicación	Revisión de certificados de capacitación y registro de asistencia de participantes en las capacitaciones. Seguimiento al presupuesto de capacitación. Evaluaciones a los participantes.	Se debe mantener información documentada de las capacitaciones recibidas por la comunidad académica, misma que debe estar a disposición de la Dirección de Desarrollo de Talento Humano y Vicerrectorado Académico. Contar con la aprobación formal del presupuesto destinado a la capacitación así como de su asignación presupuestaria.	Trimestralmente	Director de Desarrollo de Talento Humano Vicerrector Académico

Control	Descripción del control	Responsables de implementación del control	Mecanismo de monitoreo	Descripción mecanismo de monitoreo	Periodicidad	Responsable monitoreo
	especializada al área de TIC y Planificación.					
A.8.3.1 Gestión de medios removibles	Definir y aprobar procedimientos para la gestión y uso de medios extraíbles, tales como: memorias USB, discos duros externos, CD, DVD, etc.	Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales	Revisión independiente del cumplimiento de la política de gestión de medios removibles.	Revisión de una muestra de computadores a fin de verificar que se estén cumpliendo las políticas de gestión de medios removibles.	Cuatrimestralmente	Auditoría Interna
A.9.1.1 Política de control de acceso	Establecer, documentar, revisar y aprobar una política de control de accesos a los activos de información de la institución.	Director de Planificación Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales Consejo Universitario	Revisión y actualización periódica de política de control de acceso.	La política de control de accesos debe ser revisada para verificar su conveniencia, adecuación y eficacia.	Al menos 1 vez al año	Director de Planificación Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales Consejo Universitario

Control	Descripción del control	Responsables de implementación del control	Mecanismo de monitoreo	Descripción mecanismo de monitoreo	Periodicidad	Responsable monitoreo
A.9.1.2 Acceso a redes y a servicios en red	Se debe permitir el acceso a la red institucional únicamente a los usuarios autorizados conforme a las políticas de control de acceso.	Director de Tecnologías de la Información y Comunicación Todas las áreas	Revisión independiente del cumplimiento del procedimiento de accesos a la red institucional.	Prueba de cumplimiento del procedimiento de accesos a la red institucional.	Semestralmente	Propietario de activos de información
A.9.2.1 Registro y cancelación de usuarios	Definición y aprobación de un procedimiento para la administración de usuarios.	Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales	Revisión independiente del cumplimiento del procedimiento de administración de usuarios.	Prueba de cumplimiento del procedimiento de administración de usuarios.	Semestralmente	Propietario de activos de información
A.9.2.2 Suministro de acceso de usuarios	Definición y aprobación de un procedimiento para la administración de usuarios.	Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales	Revisión independiente del cumplimiento del procedimiento de administración de usuarios.	Prueba de cumplimiento del procedimiento de administración de usuarios.	Semestralmente	Propietario de activos de información
A.9.2.3 Gestión de derechos de acceso privilegiado	Definición y aprobación de un procedimiento para la administración de usuarios.	Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales	Revisión independiente del cumplimiento del procedimiento de administración de usuarios.	Prueba de cumplimiento del procedimiento de administración de usuarios.	Semestralmente	Propietario de activos de información

Control	Descripción del control	Responsables de implementación del control	Mecanismo de monitoreo	Descripción mecanismo de monitoreo	Periodicidad	Responsable monitoreo
A.9.2.4 Gestión de información de autenticación secreta de usuarios	Definición y aprobación de un procedimiento para la administración de usuarios.	Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales	Revisión independiente del cumplimiento del procedimiento de administración de usuarios.	Prueba de cumplimiento del procedimiento de administración de usuarios.	Semestralmente	Propietario de activos de información
A.9.2.5 Revisión de los derechos de acceso de usuarios	Definir y aprobar un procedimiento para la revisión periódica de los derechos de acceso de usuarios por parte de los propietarios de los activos de información.	Director de Planificación Director General de Servicios Institucionales Director de Tecnología Propietarios de los activos de información	Revisión independiente del cumplimiento del procedimiento de administración de usuarios.	Prueba de cumplimiento del procedimiento de administración de usuarios.	Semestralmente	Propietario de activos de información
A.9.2.6 Retiro o ajuste de los derechos de acceso	Definir y aprobar un procedimiento para la revocación de derechos de acceso de los usuarios al terminar su empleo o vinculación con la institución.	Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales	Revisión independiente del cumplimiento del procedimiento de administración de usuarios.	Prueba de cumplimiento del procedimiento de administración de usuarios.	Semestralmente	Propietario de activos de información

Control	Descripción del control	Responsables de implementación del control	Mecanismo de monitoreo	Descripción mecanismo de monitoreo	Periodicidad	Responsable monitoreo
A.9.3.1 Uso de información de autenticación secreta	Concientizar y exigir al personal cumplir con las políticas de resguardo de su información secreta, tales como: usuarios, claves, etc.	Director de Planificación Director de Comunicación Social Director General de Servicios Institucionales Director de Desarrollo de Talento Humano Director de Tecnologías de la Información y Comunicación	Verificar la ejecución de capacitaciones relacionadas al resguardo de información secreta o confidencial. Revisiones de escritorio y pantalla limpia.	Verificar que se hayan realizado capacitaciones relacionadas al resguardo de información secreta o confidencial, mediante la revisión de certificados, registro de asistencia, convocatorias, mensajes a correos electrónicos con consejos de seguridad, etc. Realizar revisiones de escritorio y pantalla limpia.	Semestralmente	Auditoría Interna
A.9.4.1 Restricción de acceso a la información	Definición y aprobación de un procedimiento para la administración de usuarios.	Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales	Revisión del cumplimiento del procedimiento de administración de usuarios.	Prueba de cumplimiento del procedimiento de administración de usuarios.	Semestralmente	Propietario de activos de información
A.9.4.2 Procedimiento de ingreso seguro	Se debe solicitar usuario y contraseña al ingresar a los sistemas y aplicaciones.	Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales	Verificar que exista un procedimiento de ingreso seguro a los activos de información críticos.	Prueba de cumplimiento del procedimiento de ingreso seguro a los activos de información críticos.	Anualmente	Auditoría Interna

Control	Descripción del control	Responsables de implementación del control	Mecanismo de monitoreo	Descripción mecanismo de monitoreo	Periodicidad	Responsable monitoreo
A.9.4.3 Sistema de gestión de contraseñas	Verificar que los sistemas y aplicaciones se encuentran configurados para asegurar la gestión de contraseñas, tales como: complejidad de contraseñas, periodicidad de cambio de contraseñas, intentos de accesos fallidos, histórico de contraseñas, entre otros, conforme a la política aprobada.	Director de Tecnologías de la Información y Comunicación	Verificar que exista gestión de contraseñas utilizadas para el ingreso a los activos críticos identificados.	Verificar que los sistemas y aplicaciones se encuentran configurados para asegurar la gestión de contraseñas, tales como: complejidad de contraseñas, periodicidad de cambio de contraseñas, intentos de accesos fallidos, histórico de contraseñas, entre otros, conforme a la política aprobada.	Anualmente	Auditoría Interna
A.9.4.5 Control de acceso a códigos fuente de programas	El acceso al código fuente de los programas debe ser restringido únicamente a usuarios autorizados.	Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales	Verificar la existencia de segregación de funciones en el área de Tecnologías de Información y Comunicación.	Verificar que no exista concentración de funciones incompatibles en el área de Tecnologías de la Información y Comunicación.	Anualmente	Auditoría Interna Director de Desarrollo del Talento Humano
A.10.1.1 Política sobre el uso de controles criptográficos	Definir y aprobar una política para el uso de controles criptográficos, tales como: certificados digitales, cifrado de claves, etc.	Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales	Verificar la vigencia de los certificados digitales y la complejidad del algoritmo de cifrado, conforme a las políticas aprobadas. Revisar la configuración del servidor web.	Verificar la vigencia de los certificados digitales y la complejidad del algoritmo de cifrado. Revisar la configuración del servidor web a fin de determinar su razonabilidad.	Anualmente	Director de Tecnologías de la Información y Comunicación

Control	Descripción del control	Responsables de implementación del control	Mecanismo de monitoreo	Descripción mecanismo de monitoreo	Periodicidad	Responsable monitoreo
A.10.1.2 Control de llaves	Desarrollar e implementar una política sobre el uso, protección y tiempo de vida de las llaves criptográficas.	Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales	Verificar la aplicación de la política sobre el uso, protección y tiempo de vida de las llaves criptográficas.	Verificar la aplicación de la política sobre el uso, protección y tiempo de vida de las llaves criptográficas.	Anualmente	Auditoría Interna
A.11.1.2 Controles de acceso físico	Implementación de controles de acceso y protección física, tales como: acceso biométrico, puerta de acero, cámaras de seguridad al interior y exterior, botón de pánico conectado a una alarma, sensor de movimiento y alertas, pólizas de seguros, cláusulas de contrato y acuerdos de niveles de servicio con proveedores ISP. Para el caso de archivadores: cerraduras con llave.	Director General de Servicios Institucionales Director de Planificación	Verificar que existan controles de acceso y protección física al centro de cómputo principal y alterno, y a los archivos físicos, así como la vigencia de las pólizas de seguros.	Verificar que existan controles de acceso y protección física al centro de cómputo principal y alterno, y a los archivos físicos, así como la vigencia de las pólizas de seguros.	Anualmente	Auditoría Interna

Control	Descripción del control	Responsables de implementación del control	Mecanismo de monitoreo	Descripción mecanismo de monitoreo	Periodicidad	Responsable monitoreo
A.11.2.4 Mantenimiento de equipos	Plan de mantenimiento de equipos de cómputo. Contrato con el proveedor para el mantenimiento del UPS.	Director de Tecnologías de la Información y Comunicación Jefe de Infraestructura	Verificar la existencia de un plan de mantenimiento de equipos de cómputo y documentación que sustente su cumplimiento. Verificar la vigencia del contrato de mantenimiento de UPS y documentación que sustente su cumplimiento.	Verificar la existencia de un plan de mantenimiento de equipos de cómputo y documentación que sustente su cumplimiento. Verificar la vigencia del contrato de mantenimiento de UPS y documentación que sustente su cumplimiento.	Trimestralmente	Auditoría Interna
A.12.1.1 Procedimientos de operación documentados	Documentar los procedimientos del área de Tecnología, incluidos los procedimientos de gestión de la seguridad física y lógica.	Director de Planificación Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales	Verificar la existencia de procedimientos de operación documentados.	Verificar que los procedimientos del área de Tecnología, incluidos los procedimientos de gestión de seguridad física y lógica estén documentados y actualizados acorde a las necesidades de la institución.	Anualmente	Director de Planificación
A.12.1.2 Gestión de cambios	Documentar los procedimientos del área de Tecnología, incluidos los procedimientos de gestión de la seguridad física y lógica.	Director de Planificación Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales	Verificar la existencia de procedimientos de operación documentados.	Verificar que los procedimientos del área de Tecnología, incluidos los procedimientos de gestión de seguridad física y lógica estén documentados y actualizados acorde a las necesidades de la institución.	Anualmente	Director de Planificación

Control	Descripción del control	Responsables de implementación del control	Mecanismo de monitoreo	Descripción mecanismo de monitoreo	Periodicidad	Responsable monitoreo
A.12.2.1 Controles contra códigos maliciosos	Adquisición y configuración de antivirus corporativo para todos los equipos de la red institucional. Revisión y actualización de las reglas del firewall existente.	Director de Tecnologías de la Información y Comunicación	Verificar que existan procedimientos de actualización periódicos del antivirus y que se estén aplicando. Revisar el procedimiento para actualización de las reglas del firewall existente.	Verificar que existan procedimientos de actualización periódicos del antivirus y que se estén aplicando. Revisar el procedimiento para actualización de las reglas del firewall existente.	Semestralmente	Auditoría Interna
A.12.3.1 Respaldo de la información	Implementar procedimientos de respaldos periódicos de información para los diferentes activos seleccionados, en función de los requerimientos de disponibilidad y continuidad del negocio.	Director de Planificación Director de Tecnologías de la Información y Comunicación Propietarios de activos de información Jefe de Infraestructura	Verificar que se estén ejecutando procedimientos de respaldos de información conforme a la periodicidad definida acorde a las necesidades de continuidad del negocio.	Verificar que se estén ejecutando procedimientos de respaldos de información conforme a la periodicidad definida, que incluya las pruebas de restauración de los mismos. Además, se debe constatar que se está respaldando la información de los activos críticos, acorde a las necesidades de continuidad del negocio.	Trimestralmente	Director de Tecnologías de la Información y Comunicación Auditoría Interna
A.12.5.1 Instalación de software en sistemas operativos	Configurar mediante reglas del Directorio Activo existente, restricciones para instalación de software no	Director de Tecnologías de la Información y Comunicación Jefe de Infraestructura	Verificar que las reglas del Directorio Activo relacionadas a la restricción para instalación de software no	Mediante una muestra, verificar que exista restricción para instalación de software no autorizado en equipos	Cuatrimestralmente	Director de Tecnologías de la Información y Comunicación.

Control	Descripción del control	Responsables de implementación del control	Mecanismo de monitoreo	Descripción mecanismo de monitoreo	Periodicidad	Responsable monitoreo
	autorizado.		autorizado, se encuentren vigentes.	de usuario final y emitir informe técnico respectivo.		
A.12.7 Controles de auditorías de sistemas de información	Ejecución de auditorías de sistemas, al menos una vez al año.	Director de Planificación Consejo Universitario	Ejecución de auditorías externas e internas informáticas.	Auditorías informáticas a los controles generales de Tecnología de Información y a la plataforma tecnológica de gestión académica.	Anualmente	Auditoría Interna Auditoría Informática externa
A.14.2.1 Política de desarrollo	Elaborar una política que incluya las directrices para el desarrollo de sistemas en la institución.	Director de Planificación Director de Tecnologías de la Información y Comunicación Jefe de Desarrollo Director General de Servicios Institucionales	Verificar la existencia de la política que incluya las directrices para el desarrollo de sistemas.	Verificar la existencia de la política que incluya las directrices para el desarrollo de sistemas y que la misma se encuentre aprobada.	Anualmente	Director de Planificación
A.14.2.2 Procedimientos de control de cambios en sistemas	Implementar procedimientos formales de control de cambios como parte de la política de desarrollo de sistemas.	Director de Planificación Director de Tecnologías de la Información y Comunicación Jefe de Desarrollo Director General de Servicios	Ejecución de auditorías externas e internas informáticas.	Auditorías informáticas a los controles generales de Tecnología de Información y a la plataforma tecnológica de gestión académica.	Anualmente	Auditoría Interna Auditoría Informática externa

Control	Descripción del control	Responsables de implementación del control	Mecanismo de monitoreo	Descripción mecanismo de monitoreo	Periodicidad	Responsable monitoreo
		Institucionales				
A.14.2.3 Revisión técnica de las aplicaciones después de cambios en la plataforma de operación	Implementar procedimientos formales para la revisión de aplicaciones como parte de las políticas de desarrollo de sistemas, a fin de probar que no existan impactos adversos o que afecten a la seguridad de la información.	Director de Planificación Director de Tecnologías de la Información y Comunicación Jefe de Desarrollo Director General de Servicios Institucionales	Verificar la existencia de informes de control de calidad de sistemas previo al paso a producción.	Verificar la existencia de informes de control de calidad de sistemas previo al paso a producción.	Trimestralmente	Director de Tecnologías de la Información y Comunicación Director de Planificación
A.14.2.4 Restricciones en los cambios a los paquetes de software	Incluir en la política de desarrollo, restricciones en los cambios a los paquetes de software.	Director de Planificación Director de Tecnologías de la Información y Comunicación Jefe de Desarrollo Director General de Servicios Institucionales	Verificar que exista segregación de funciones y acceso a los paquetes de software y autorizaciones formales de cambio, de ser necesario.	Verificar que exista segregación de funciones y acceso a los paquetes de software y autorizaciones formales de cambio, de ser necesario.	Semestralmente	Director de Planificación Auditoría Interna

Control	Descripción del control	Responsables de implementación del control	Mecanismo de monitoreo	Descripción mecanismo de monitoreo	Periodicidad	Responsable monitoreo
A.14.2.5 Principios de construcción de los sistema seguros	Establecer, documentar, y mantener principios para la construcción de sistemas seguros y aplicarlos a cualquier actividad de implementación de sistemas.	Director de Planificación Director de Tecnologías de la Información y Comunicación Jefe de Desarrollo Director General de Servicios Institucionales	Verificar la existencia de informes técnicos del nivel de seguridad de los sistemas previo al paso a producción.	Verificar la existencia de informes técnicos del nivel de seguridad de los sistemas previo al paso a producción.	Semestralmente	Director de Tecnologías de la Información y Comunicación
A.14.2.6 Ambiente de desarrollo seguro	Mantener segregados los ambientes de pruebas y producción con los debidos controles de acceso.	Director de Planificación Director de Tecnologías de la Información y Comunicación Jefe de Desarrollo Director General de Servicios Institucionales	Verificar que existan ambientes y redes separados para desarrollo y producción.	Verificar que existan ambientes y redes separados para desarrollo y producción.	Anualmente	Auditor Informático externa Auditor Interno
A.15.1.1 Política de seguridad de la información para las relaciones con proveedores	Definir los requerimientos de seguridad de la información que se deben solicitar a los proveedores y que deben ser incluidos en las nuevas contrataciones o adéndums.	Director de Planificación Procurador Judicial Director de Tecnologías de la Información y Comunicación	Revisión de contratos y acuerdos de niveles de servicio con los proveedores de TI.	Revisar que en los contratos con proveedores tecnológicos, existan cláusulas y acuerdos de niveles de servicio relacionados a la seguridad de la información.	Anualmente	Procurador Judicial Director de Tecnologías de la Información y Comunicación

Control	Descripción del control	Responsables de implementación del control	Mecanismo de monitoreo	Descripción mecanismo de monitoreo	Periodicidad	Responsable monitoreo
A.15.1.2 Tratamiento de la seguridad dentro de los acuerdos con proveedores	Definir los requerimientos de seguridad de la información que se deben solicitar a los proveedores y que deben ser incluidos en las nuevas contrataciones o adéndums.	Director de Planificación Procurador Judicial Director de Tecnologías de la Información y Comunicación	Revisión de contratos y acuerdos de niveles de servicio con los proveedores de TI previo a su suscripción.	Revisar que en los contratos con proveedores tecnológicos que se van a suscribir, existan cláusulas y acuerdos de niveles de servicio relacionados a la seguridad de la información.	Todo el año	Procurador Judicial Director de Tecnologías de la Información y Comunicación
A.15.2.1 Seguimiento y revisión de los servicios de los proveedores	Verificar que se cumplan los acuerdos de niveles de servicio para los proveedores: ISP y la compañía que brinda el mantenimiento a los UPS.	Director de Tecnologías de la Información y Comunicación	Informes de monitoreo de los servicios brindados por los proveedores tecnológicos: ISP y la compañía que brinda el mantenimiento a los UPS.	Informes de monitoreo de los servicios brindados por los proveedores tecnológicos: ISP y la compañía que brinda el mantenimiento a los UPS.	Trimestralmente	Director de Tecnologías de la Información y Comunicación

Control	Descripción del control	Responsables de implementación del control	Mecanismo de monitoreo	Descripción mecanismo de monitoreo	Periodicidad	Responsable monitoreo
A.17.1.1 Planificación de la continuidad de la seguridad de la información	Elaborar el plan de continuidad que incluya los requerimientos de seguridad de la información.	Director de Planificación Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales Consejo Universitario	Revisión y actualización de los requerimientos de seguridad de la información mientras se mantengan las contingencias que activen un plan de continuidad. Presupuesto para continuidad de la seguridad de la información.	Revisión y actualización de los requerimientos de seguridad de la información mientras se mantengan las contingencias que activen un plan de continuidad. Verificar la existencia de un presupuesto aprobado para la continuidad de la seguridad de la información y documentación que sustente su cumplimiento.	Anualmente	Director de Tecnologías de la Información y Comunicación Director de Planificación Consejo Universitario
A.17.1.2 Implementación de la continuidad de la seguridad de la información	La universidad debe establecer, documentar, implementar y mantener procesos, procedimientos y controles para asegurar el nivel de continuidad requerido para la seguridad de la información durante una situación adversa.	Director de Planificación Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales Consejo Universitario	Revisión y actualización de los requerimientos de seguridad de la información mientras se mantengan las contingencias que activen un plan de continuidad. Presupuesto para continuidad de la seguridad de la información.	Revisión y actualización de los requerimientos de seguridad de la información mientras se mantengan las contingencias que activen un plan de continuidad. Verificar la existencia de un presupuesto aprobado para la continuidad de la seguridad de la información y documentación que sustente su	Anualmente	Director de Tecnologías de la Información y Comunicación Director de Planificación

Control	Descripción del control	Responsables de implementación del control	Mecanismo de monitoreo	Descripción mecanismo de monitoreo	Periodicidad	Responsable monitoreo
				cumplimiento.		
A.17.1.3 Verificación, revisión y evaluación de la continuidad de la seguridad de la información	Definir procedimientos de verificación periódica de los controles de continuidad de la seguridad de la información establecidos e implementados, para asegurar que son válidos y eficaces en situaciones adversas.	Director de Planificación Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales Consejo Universitario	Revisión y actualización de los requerimientos de seguridad de la información mientras se mantengan las contingencias que activen un plan de continuidad. Presupuesto para continuidad de la seguridad de la información. Revisar las pruebas realizadas.	Revisión y actualización de los requerimientos de seguridad de la información mientras se mantengan las contingencias que activen un plan de continuidad. Verificar la existencia de un presupuesto aprobado para la continuidad de la seguridad de la información y documentación que sustente su cumplimiento. Verificar que exista documentación relacionada a las pruebas realizadas.	Anualmente	Director de Tecnologías de la Información y Comunicación Director de Planificación

Control	Descripción del control	Responsables de implementación del control	Mecanismo de monitoreo	Descripción mecanismo de monitoreo	Periodicidad	Responsable monitoreo
A.17.2.1 Disponibilidad de instalaciones de procesamiento de información	Contratación de un housing para la implementación de un centro de datos alterno con ISP que mantenga un centro de datos al menos de categoría TIER III.	Director de Planificación Director de Tecnologías de la Información y Comunicación Director General de Servicios Institucionales Consejo Universitario	Contrato con el proveedor, certificación TIER III ó IV, presupuesto aprobado para la contratación del housing en el lugar externo.	Verificar que exista un contrato vigente con un proveedor de housing con categoría TIER III ó superior así como el presupuesto para este servicio. Visita al centro de cómputo alterno.	Anualmente	Director de Tecnologías de la Información y Comunicación Director de Planificación Consejo Universitario Procurador Judicial
A.18.2.1 Revisión independiente de la seguridad de la información	Contratar un análisis de ethical hacking al menos una vez al año.	Director de Planificación Consejo Universitario	Verificar la existencia de contrato para análisis de ethical hacking, informe, plan de mitigación de riesgos detectados por el ethical hacking, evidencias de cumplimiento del plan de mitigación.	Verificar la existencia de contrato para análisis de ethical hacking, informe, plan de mitigación de riesgos detectados por el ethical hacking, evidencias de cumplimiento del plan de mitigación.	Anualmente	Director de Tecnologías de la Información y Comunicación Director de Planificación Auditoría Interna Consejo Universitario