RESUMEN – TRABAJO DE GRADO

AUTORES	**Yenis Piedad Osorio Rivero** **Yesica María Pérez Pérez,**
FACULTAD	**Ingenierías**
PLAN DE ESTUDIOS	**Especialización en Auditoria de Sistemas.**
DIRECTOR	**Andrés Mauricio Puentes Velásquez**
TÍTULO DE LA TESIS	**Diseño de una Política de Gestión de Riesgos de la Información para La Dependencia de Admisiones Registro y Control de Universidad Francisco de Paula Santander Ocaña.**

RESUMEN

(70 palabras aproximadamente)

LA PRESENTE INVESTIGACIÓN PROPONE UNA POLÍTICA DE GESTIÓN DE RIESGOS DE LA INFORMACIÓN PARA LA OFICINA DE ADMISIONES REGISTRO Y CONTROL DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA; SE SUSTENTA EN EL MARCO DE TRABAJO DE ISO/IEC 31000/ 2009 Y EN LA METODOLOGÍA DE ANÁLISIS Y GESTIÓN DE RIESGOS DE LOS SISTEMAS DE INFORMACIÓN MAGERIT.

TENIENDO EN CUENTA, QUE LA PRESENTE PROPUESTA ESTÁ ENFOCADA EN LA GESTIÓN DE RIESGOS DE LA INFORMACIÓN, TAMBIÉN SE INVOLUCRAN CONCEPTOS RELACIONADOS CON SEGURIDAD DE LA INFORMACIÓN QUE CONSISTE EN LA PRESERVACIÓN DE LA CONFIDENCIALIDAD, LA INTEGRIDAD Y LA DISPONIBILIDAD DE LA INFORMACIÓN.

CARACTERÍSTICAS

PÁGINAS:	PLANOS:	ILUSTRACIONES:	CD-ROM:
116	0	0	1

DISEÑO DE UNA POLÍTICA DE GESTIÓN DE RIESGOS DE LA INFORMACIÓN PARA LA DEPENDENCIA DE ADMISIONES REGISTRO Y CONTROL DE UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA.

YENIS PIEDAD OSORIO RIVERO
YESICA MARIA PÉREZ PÉREZ

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
ESPECIALIZACION EN AUDITORIA DE SISTEMAS
FACULTAD DE INGENIERIAS
OCAÑA
2014

DISEÑO DE UNA POLÍTICA DE GESTIÓN DE RIESGOS DE LA INFORMACIÓN PARA LA DEPENDENCIA DE ADMISIONES REGISTRO Y CONTROL DE UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA.

YESICA MARIA PÉREZ PÉREZ
YENIS PIEDAD OSORIO RIVERO

Proyecto para optar el título de Especialista en Auditoria de Sistemas

Director
ANDRES MAURICIO PUENTES VELASQUEZ
IS. ESP. MSC(C) Ingeniería de Sistemas

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
ESPECIALIZACION EN AUDITORIA DE SISTEMAS
FACULTAD DE INGENIERIAS
OCAÑA
2014

ADVERTENCIA

DEDICATORIA

A Dios, por permitirme llegar a este momento tan especial en mi vida, por los triunfos y los momentos difíciles que me han enseñado a valorarlo cada día más.
A mis hijos que son la luz de mi vida, los que me animan salir avante, el origen de mis desvelos, de mis preocupaciones y de mis ganas de ser cada día mejor persona.
A mi madre en el cielo porque hoy su sueño se ha cumplido. A mi esposo por su comprensión y apoyo incondicional en mis estudios.

Yenis Piedad Osorio Rivero.

Primero y antes que nada, dar gracias a Dios, por estar conmigo en cada paso que doy, por fortalecer mi corazón e iluminar mi mente y por haber puesto en mi camino a aquellas personas que han sido mi soporte y compañía durante todo el periodo de estudio.
Agradecer hoy y siempre a mis padres y hermanos por el esfuerzo realizado y apoyo en mis estudios, por las sabias palabras llenas de amor que me dan la fortaleza necesaria para seguir adelante.
A mi esposo, por su colaboración, paciencia, entrega y amor al transmitirme cada una de sus enseñanzas.

Yesica María Pérez Pérez

AGRADECIMIENTOS

Queremos en estas líneas expresar nuestros sinceros agradecimientos a aquellas personas que colaboraron para que este proyecto fuera una realidad; a la MSC. Torcoroma Velásquez Pérez por facilitarnos la dependencia Admisiones Registro y Control para el desarrollo de las actividades del presente trabajo de investigación.

Al director del proyecto MSC. Andrés Mauricio Puentes Velásquez por su motivación, seguimiento y enseñanzas en todo el proceso de la especialización.

También nos gustaría agradecer a los profesores por su aporte a nuestra formación profesional.

TABLA DE CONTENIDO

ILUSTRACIONES

TABLAS

GLOSARIO

ACEPTACIÓN DEL RIESGO: decisión de asumir un riesgo.

ACTIVO: es cualquier cosa que representa o que tiene un valor para la organización.

AMENAZA: causa potencial de un incidente no deseado, que puede ocasionar daño a un sistema u organización.

ANÁLISIS DE RIESGO: uso sistemático de la información para identificar las fuentes y estimar el riesgo, con el fin de prever o corregir las vulnerabilidades que se presentan.

ARQUITECTURA DE TI: Marco integrado para evolucionar o dar mantenimiento a TI existente y adquirir nueva TI para alcanzar las metas estratégicas y de negocio de la empresa.

CONFIDENCIALIDAD: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

CONTROL: medios para gestionar el riesgo, incluyendo políticas, procedimientos, directrices, prácticas o estructuras de la organización que pueden ser de naturaleza administrativa, técnica, de gestión o legal.

DIRECTRIZ: descripción que aclara lo que se debería hacer y cómo hacerlo, para alcanzar los objetivos establecidos en las políticas.

DISPONIBILIDAD: propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

EVALUACIÓN DEL RIESGO: Proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del mismo.

GESTIÓN DEL RIESGO: actividades coordinadas para dirigir y controlar una organización en relación con el riesgo.

INTEGRIDAD: Propiedad de salvaguardar la exactitud y estado complete de los activos.
MODELO: representación de un objeto, sistema o idea, de forma diferente al de la entidad misma.

MODELO DE GESTIÓN: esquema o marco de referencia para la administración de una entidad.

POLÍTICA: es toda intención y directriz expresada formalmente por la Dirección.

PROCEDIMIENTO: método o sistema estructurado para ejecutar algunas cosas.

REGISTRO: asiento o anotación que queda de lo que se registra.

RIESGO: probabilidad de que una amenaza cause un impacto.

RIESGO RESIDUAL: nivel restante de riesgo después del tratamiento del riesgo.

SEGURIDAD DE LA INFORMACIÓN: preservación de la confidencialidad, la integridad y la disponibilidad de la información.

TI: tecnologías de la Información.

TRATAMIENTO DEL RIESGO: proceso de selección e implementación de medidas para modificar el riesgo.

VALORACIÓN DEL RIESGO: proceso global de análisis y evaluación del riesgo.

VULNERABILIDAD: debilidad de un activo o grupo de activos que pueden ser aprovechadas por una o varias amenazas.

INTRODUCCIÓN

La administración del riesgo de la información para las entidades públicas y privadas en todos sus órdenes cobra cada día mayor importancia, dado el dinamismo y los constantes cambios que exige este mundo globalizado.

Estos cambios hacen que cada día las entidades deban enfrentarse a factores internos y externos que pueden crear incertidumbre sobre el logro de sus objetivos, ya que esta incertidumbre trae como consecuencia inevitablemente riesgos que ponen en peligro la estabilidad de las instituciones.

El Estado colombiano, en busca de fortalecer sus instituciones estableció normas y adoptó una serie de elementos técnicos requeridos para la administración del riesgo. Es así como la Universidad Francisco de Paula Santander Ocaña, dando cumplimiento a estos requerimientos y en busca de la mejora continua ha adoptado una serie de actividades y procesos administrativos como es el Modelo Estándar de Control Interno (MECI), el Sistema Integrado de Gestión, que ha permitido integrar herramientas modernas y efectivas para la gestión organizacional y su desarrollo sostenible dentro de los parámetros de la eficiencia, eficacia y efectividad de las estrategias implementadas, obteniendo como resultado la renovación del certificado en las normas de calidad ISO 9001, NTC GP 1000.

En este orden de ideas y consciente de las necesidades actuales que presenta la oficina Admisiones Registro y Control de la Universidad Francisco de Paula Santander con respecto a la seguridad de la información, se plantea el diseño de una Política de Gestión del Riesgo de la Información, como herramienta que le permita al líder de proceso analizar elementos de forma metódica para llegar a conclusiones con fundamento y proceder a la fase de tratamiento.
El modelo de Magerit informalmente expresa que la gestión de la seguridad de un sistema de información es la gestión de sus riesgos y que el análisis permite racionalizar dicha gestión.

1 TITULO

Diseño de una política de Gestión de riesgos de la información para la dependencia de admisiones, registro y control de la Universidad Francisco de Paula Santander Ocaña.

1.1 PLANTEAMIENTO DEL PROBLEMA

La Oficina de Admisiones, Registro y Control de la Universidad Francisco de Paula Santander Ocaña, es la dependencia de la Subdirección Académica que se encarga de registrar, actualizar y custodiar los registros académicos de los estudiantes como son los procesos de inscripción, admisión y matrícula.

En la oficina de admisiones registro y control, se han venido presentando inconsistencias, retardo, exposición a la pérdida y manipulación de la información; problemática que puede generar sanciones legales y perjudicar la imagen de la institución de educación superior.

La información gestionada por la oficina de admisiones registro y control tiene un alto nivel de sensibilidad en cada uno de sus procesos, está expuesta permanentemente a riesgos que comprometen su disponibilidad, integridad y confidencialidad. Con el fin de apoyar la seguridad de dicha información se propone diseñar una política de Gestión de riesgos.

1.2 FORMULACION DEL PROBLEMA

Este trabajo se fundamenta en ¿Cómo una política de gestión de riesgos permitirá al proceso de admisiones, registro y control de la UFPSO la identificación, valoración y tratamiento de los riesgos de su entorno de una forma efectiva y eficiente?

1.3 OBJETIVOS

1.3.1 General.

Diseñar una política para la gestión de riesgos de la información en la oficina de Admisiones Registro y Control de la Universidad Francisco de Paula Santander Ocaña.

1.3.2 Objetivos específicos

- ✓ Realizar un reconocimiento de la dependencia de Admisiones Registro y Control, para identificar y valorar los riesgos.

- ✓ Identificar la norma para el diseño de una política de administración de riesgos para reducir los posibles daños e impactos.

- ✓ Documentar el análisis a través de una política de gestión de riesgos de la oficina de admisiones registro y control.

1.4 JUSTIFICACIÓN

Según Alter Wriston (Ex presidente de Citicorp) "todo en la vida es la administración del riesgo, no su eliminación".
Al hablar de "riesgos" se piensa en la posibilidad de que ocurran eventos no deseados. Por una parte los riesgos ocurren por sucesos a los cuales no se les asocia ninguna probabilidad. Asignar una probabilidad a todos los eventos que puedan alterar las utilidades de las empresas, es lo que se denomina "Análisis de Riesgo"

Actualmente en la oficina de Admisiones, Registro y Control no existe una política para la administración de riesgos que ayude en los objetivos misionales de la institución ya que es uno de los puntos primordiales en el Gobierno de TI.

La política de administración de riesgos propuesta para la oficina de admisiones registro y control es importante porque servirá como apoyo para reconocer y neutralizar las amenazas, debilidades y riesgos que puedan causar cambios o pérdida de su información.
La implementación de la política de administración de riesgos dará las pautas para analizar, evaluar, controlar y tratar los riesgos que se presenten, convirtiéndose en una oportunidad para su desarrollo y el establecimiento de una cultura organizacional.

1.5 HIPÓTESIS

La creación de una política de gestión de riesgos de la información para la oficina de admisiones registro y control de La Universidad Francisco de Paula Santander Ocaña, contribuirá al fortalecimiento de los procesos que apoyan el cumplimiento de su misión, visión y objetivos institucionales, identificando los niveles de incertidumbre a los que se encuentra expuesta.

1.6 DELIMITACIONES

1.6.1 GEOGRÁFICAS.

Este proyecto se desarrollará en la oficina de admisiones registro y control de la universidad Francisco de Paula Santander Ocaña.

1.6.2 Temporales.

El proyecto de investigación se llevara a cabo en un lapso de 2 meses desarrollando cada objetivo propuesto, a partir de la aprobación del Anteproyecto.

1.6.3 Conceptuales.

Los conceptos que abarcarán esta investigación se fundamenta en gobernabilidad de TI y seguridad de la información, específicamente relacionados con la administración de riesgos y buenas prácticas.

NTC ISO/IEC 27001 Tecnología de la Información. Sistema de Gestión de Seguridad de la Información (SGSI). 2005.

NTC ISO/IEC 27002 Código de las Buenas Prácticas para la Gestión de la Seguridad de la Información. 2005.

NTC 5254. Gestión del Riesgo. 2004.

NTC ISO/IEC 27005. Tecnología de la Información. Técnicas de Seguridad. Gestión del Riesgo en la Seguridad de la Información. 27005.

NTC ISO 31000. Gestión del Riesgo. Principios y Directrices. 2011

1.6.4 Operativa.

El desarrollo del proyecto desde el punto de vista operativo se soporta en los procesos principales de la oficina de admisiones registro y control.

Preinscripción, inscripción, admisión, registro, control y reportes.

2 MARCO REFERENCIAL

2.1 MARCO HISTORICO

La información actualmente es considerada un activo que representa gran valor para cualquier organización. Por tal motivo, se hace necesario protegerla y darle un manejo adecuado a la misma con el fin de evitar impactos significativos que pueden ser causados por agentes externos o interno que permanentemente se encuentran a esperas para aprovechar las vulnerabilidades o puntos débiles que presentan los sistemas de información en las organizaciones. Cabe aclarar, que los sistemas de información están compuestos por activos que cumplen funciones dentro de los mismos. Estos activos son las personas, el hardware, el software, los procesos, la infraestructura y la misma información, entre otros.
Para este proyecto se consideran activos de información los mencionados anteriormente.
Dichos activos están sujetos a ser atacados por amenazas que de no controlarse pueden causar impactos en la información y en efecto a la organización reflejándose en pérdidas económicas y de imagen. Así de esta manera, la alta dirección de cualquier organización debe ser consciente de que su información siempre se encontrará en riesgo y que debe tomar las medidas necesarias para enfrentarse a este tipo de adversidades.[1]

Hablar de seguridad de la información involucra muchos conceptos en especial el delo que significa el riesgo de TI y la manera de administrarlo o gestionarlo en la organización. Existen muchos estudios donde se aplican los conceptos de gestión de riesgos de tecnologías de la información en las organizaciones. Se habla de procesos, metodologías, planes tratamiento, mapas de riesgo, herramientas tecnológicas para riesgos. Pero, aún es muy ambiguo el concepto de modelo de gestión para manejar los riesgos de TI. Siendo esta una temática que trae consigo ser la razón fundamental o el motor que hace parte de un gran Sistema de Gestión de Seguridad de la Información, o comúnmente llamado SGSI. Un SGSI debe gestionar el riesgo a través de la definición e implementación de elementos y prácticas que garanticen proteger la información.

2.1.1 Antecedentes

Universidad Francisco de Paula Santander Ocaña Desarrollo una guía para la gestión del riesgo, utilizando como referencia;

- Modelo Estándar de Control Interno, MECI 1000:2005 (componente de Administración de Riesgos)

[1] DINAEL ACOSTA PORTILLO, I. L. (2013). *DISEÑO DE UN MODELO DE GESTIÓN DEL RIESGO DE TECNOLOGÍAS DE INFORMACIÓN PARA LA UNIDAD DE CONTABILIDAD DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER* . OCAÑA: Tesis de grado para la Esp Auditoria de Sistemas.

- Norma Técnica de Calidad GP 1000:2009.
- Norma Técnica Colombiana de Gestión del Riesgo, NTC 5254
- Norma Técnica Colombiana de Gestión del Riesgo, Principios y Directrices NTC-ISO 31000

Unidad de contabilidad de la Universidad Francisco de Paula Santander Ocaña, Para esta oficina se diseñó un modelo de gestión del riesgo de las tecnologías de la información.

En la alcaldía de Ocaña. El Plan Municipal de Gestión del Riesgo está enfocado a desastres naturales.

Banco Agrario de Colombia

Los Sistemas de Administración de Riesgos implementados en el Banco Agrario de Colombia son:

- Sistema de Administración de Riesgo de Crédito – SARC
- Sistema de Administración de Riesgo de Mercado – SARM.
- Sistema de Administración de Riesgo de Liquidez – SARL
- Sistema de Administración de Riesgo Operativo – SARO
- Sistema de Administración del Sistema de Gestión y Seguridad de la Información – SGSI
- Sistema de Administración de Lavados de Activos y Financiación del Terrorismo – SARLAFT

En cuanto a Gobierno Corporativo, la Junta Directiva es informada periódicamente del estado de los principales indicadores que muestran la exposición a cada uno de los riesgos y la gestión que sobre cada uno de ellos se realiza y a su vez, aprueba las políticas en materia de administración de riesgos.

Además, el Banco cuenta con un Comité de Riesgos en el cual se informa mensualmente a las directivas del Banco sobre la materialización y los niveles de exposición de los riesgos administrados.

Policía Nacional de Colombia

Acorde con los principios constitucionales y las políticas de modernización del Estado, la metodología para la administración del riesgo ayuda al conocimiento y mejoramiento de la entidad, contribuye a elevar la productividad y a garantizar la eficiencia y la eficacia en los procesos organizacionales, permitiendo definir estrategias de mejoramiento continuo, brindándole un manejo sistémico a la entidad." (Cartilla Guía de Administración del Riesgo - DAFP 2001).

2.2 MARCO CONCEPTUAL

La administración del riesgo ayuda al conocimiento y mejoramiento de la entidad, contribuye a elevar la productividad y a garantizar la eficiencia y la eficacia en los procesos organizacionales, permitiendo definir estrategias de mejoramiento continuo, brindándole un manejo sistémico a la entidad.
Teniendo en cuenta, que la presente propuesta está enfocada en la administración de riesgos de la información, también se involucran conceptos relacionados con Seguridad de la Información que consiste en la preservación de la confidencialidad, la integridad y la disponibilidad de la información.

Integridad: Se considera a la propiedad de salvaguardar la exactitud y estado completo de los activos.

Confidencialidad: Se refiere a la propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados.

Disponibilidad: Es la propiedad de que la información sea accesible y utilizable por solicitud de una entidad autorizada.

Evento. Presencia o cambio de un conjunto particular de circunstancias.

Consecuencia. Resultado de un evento.

Probabilidad. Oportunidad de que algo suceda.

Amenaza: La fuente de daño potencial o una situación que potencialmente cause Pérdidas.

Causas: Son los medios, las circunstancias y agentes generadores de riesgo.

Riesgo: Probabilidad de que suceda algún evento que tendrá un impacto sobre los objetivos institucionales o del proceso. Se expresa en términos de probabilidad y consecuencias.

Administración del riesgo: Es la capacidad que tiene la Entidad para emprender acciones necesarias que le permitan el manejo de los eventos que puedan afectar negativamente el logro de los objetivos institucionales, protegerla de los efectos ocasionados por su ocurrencia.

Gestión del riesgo. Actividades coordinadas para dirigir y controlar una organización con respecto al riesgo.

Análisis del riesgo: El uso sistemático de información disponible para determinar con qué frecuencia un determinado evento puede ocurrir y la magnitud de sus consecuencias.

Control. Medida que modifica el riesgo.

- Preventivos**:** aquellos que actúan para eliminar las causas del riesgo para prevenir su ocurrencia o materialización.
- Correctivos: Aquellos que permiten el restablecimiento de actividad, después de ser detectado un evento no deseable; también la modificación de las acciones que propiciaron su ocurrencia

Mejora continua. Acción permanente realizada, con el fin de aumentar la capacidad para cumplir los requisitos y optimizar el desempeño.

2.3 MARCO CONTEXTUAL

2.3.1 La organización

La Universidad Francisco de Paula Santander Ocaña, nace institucionalmente el 18 de julio de 1974, a través del acuerdo 003, como una opción de Educación Superior, para los estudiantes de la provincia de Ocaña y su zona de influencia.

El 5 de marzo de 1975 se dio inicio a las labores académicas en el Antiguo Convento anexo al Templo de San Francisco, con un programa académico de corte tecnológico denominado "Tecnología en Matemáticas y Física". Posteriormente la Universidad empieza a ofertar la Tecnología en Producción Agropecuaria, Zootecnia, Tecnología en Administración

Comercial y Financiera. En su constante preocupación el cuerpo docente y el personal Administrativo, logran más tarde su profesionalización con el programa de Administración de Empresas; así mismo empiezan las Ingenierías de Sistemas, Civil y Mecánica, igualmente se oferta un segundo ciclo de Profesionalización de Tecnología en Producción Agropecuaria, dirigido hacia la Ingeniería Ambiental.[2]

2.3.2 Dependencia de la Organización

La Oficina de admisiones, registro y control adscrita a la subdirección académica encargada de mantener actualizados y custodiar los registros académicos de los estudiantes y apoyar los procesos de inscripción, admisión y matrícula.

Misión: Prestar un buen servicio a los estudiantes y demás estamentos en cada uno de los requerimientos que se hagan ya que esta dependencia es un pilar fundamental por los documentos que allí reposan y hacer cumplir las normas del reglamento estudiantil en materia de desempeño.

Visión: La oficina de admisiones registro y control será la dependencia en donde los estudiantes encontrarán sistematizada toda la información académica y con sólo consultar a la página de la universidad y demás información que se requiera en la oficina.

Según Acuerdo N° 084 de septiembre 11 de 1995, el consejo superior universitario, con base en las atribuciones legales y estatutarias que le confieren la ley 30 de 1992 y el Acuerdo N° 029 del 12 de Abril de 1994, aprueba la estructura orgánica de la universidad Francisco de Paula Santander Ocaña.[3]

2.4 MARCO TEORICO

La Gobernabilidad de TI busca alinear la TI con la misión, visión y objetivos del negocio. Para su aplicación se usan metodologías, estándares o buenas prácticas. En el caso de este proyecto aplica al área de arquitectura de TI como parte del desarrollo de una política para la administración del riesgo de TI en la oficina de admisiones, registro y control.

---

[2] Perez, T. V. (2012). *Modulo de Inducción.* Ocaña: www.ufpso.edu.co.

[3] UFPSO. (2014). *Admisiones, Registro y Control.* Ocaña: www.ufpso.edu.co.

Las siguientes son teorías que dan soporte a la política de administración de riesgos para la oficina de admisiones, registro y control de la Universidad Francisco de Paula Santander Ocaña.

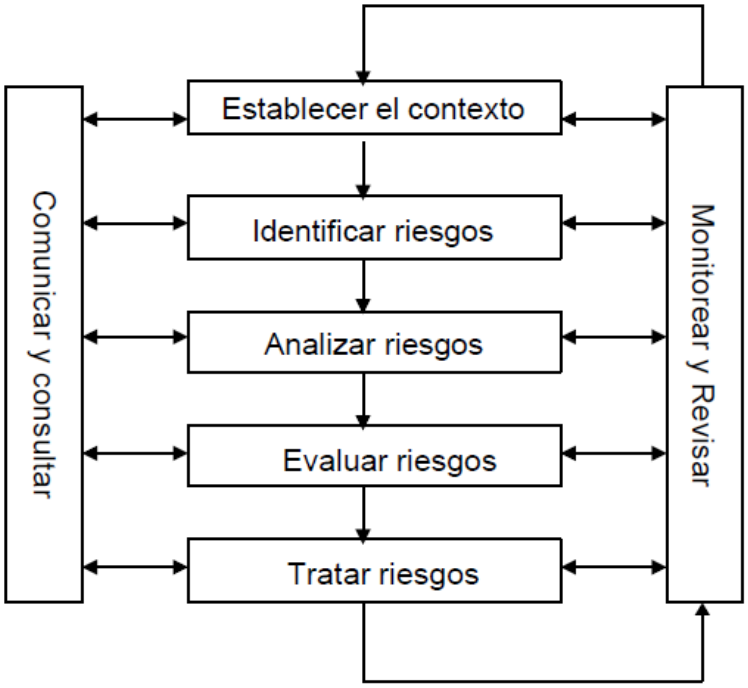
2.4.1 AS/NZS 4360:1999

En el Estándar Australiano AS/NZS 4360:1999, La administración de riesgos es reconocida como una parte integral de las buenas prácticas gerenciales. Es un proceso iterativo que consta de pasos, los cuales, cuando son ejecutados en secuencia, posibilitan una mejora continua en el proceso de toma de decisiones.
Administración de riesgos es el término aplicado a un método lógico y sistemático de establecer el contexto, identificar, analizar, evaluar, tratar, monitorear y comunicar los riesgos asociados con una actividad, función o proceso de una forma que permita a las organizaciones minimizar pérdidas y maximizar oportunidades. Administración de riesgos es tanto identificar oportunidades como evitar o mitigar pérdidas.

2.4.2 NTC 5254

Norma técnica Colombiana para le gestión de riesgos adoptada de la norma AS/NZ 4360:2004 es una guía genérica que sirve como fuente de verificación de definiciones y procesos de documentación.

Ilustración 1: Vista General de la Administración de Riesgos



Fuente: Estándar Australiano Administración de Riesgos AS/NZS 4360:1999, Pág. 9

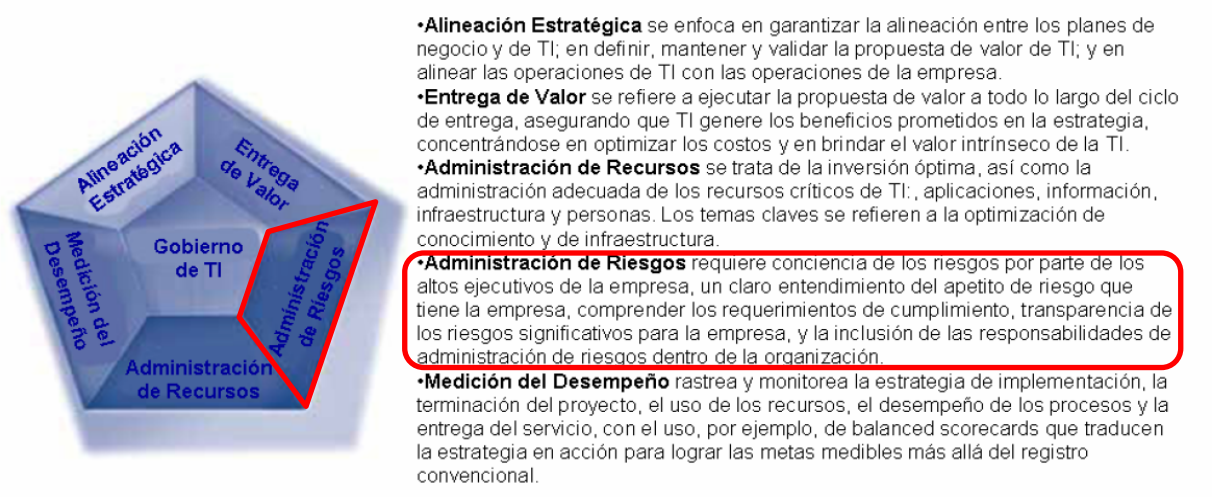
2.4.3 Cobit 4.1

La misión de Cobit es investigar, desarrollar, hacer público y promover un marco de control de gobierno de TI autorizado, actualizado, aceptado internacionalmente para la adopción por parte de las empresas y el uso diario por parte de gerentes de negocio, profesionales de TI y profesionales de aseguramiento.[4]

En el documento de Cobit 4.1 se habla de que Las empresas exitosas entienden los riesgos y aprovechan los beneficios de TI. La cuarta área del marco de Cobit es el enfoque de la administración de riesgos; pertinente para el diseño de la política de administración de riesgos.

[4] Institute, I. G. (2007). *MARCO DE TRABAJO DE COBIT.* www.itgi.org.

Ilustración 2: Áreas de enfoque del Gobierno de TI



Fuente: Cobit 4.1 Pág. 8

Cobit da soporte al gobierno de TI al brindar un marco de trabajo que garantiza que:

- TI está alineada con el negocio
- TI habilita al negocio y maximiza los beneficios
- Los recursos de TI se usan de manera responsable
- Los riesgos de TI se administran apropiadamente

2.4.4 NTC ISO/IEC 27

Esta norma técnica colombiana especifica los requerimientos para implementación de controles de seguridad acordes con el planteamiento del sistema de gestión de seguridad de la información (SGSI).

2.4.5 NTC/IEC 27002

Con este estándar se establecen pautas y principios generales para la implementación, mantenimiento y mejora de la gestión de seguridad. Cuenta con un amplio listado de objetivos de control y controles para el SGSI.

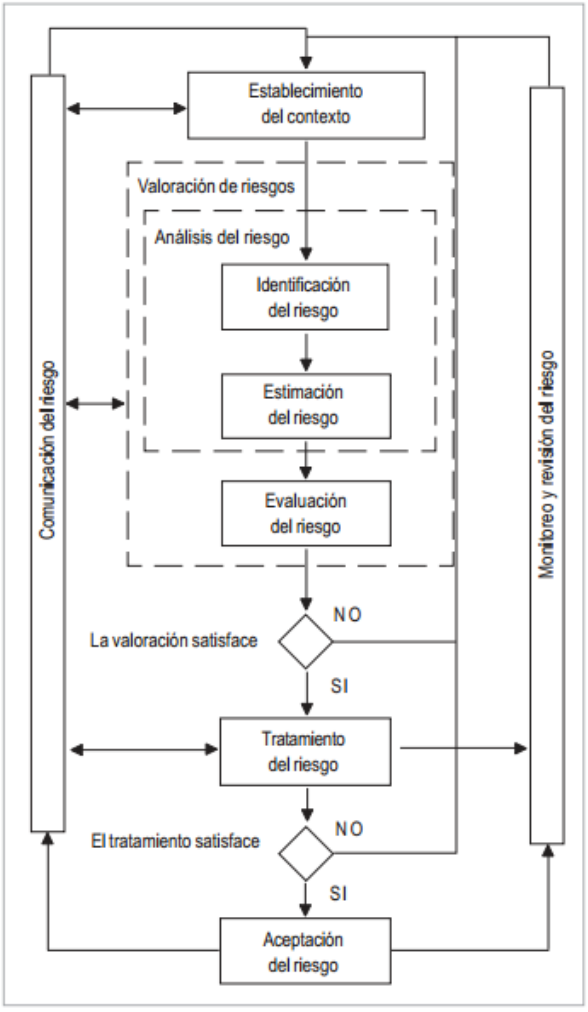
2.4.6 NIST SP 800-30

Guía desarrollada por el instituto nacional de estándares y Tecnología para la gestión de riesgos de sistemas de tecnología de la información de Estados Unidos. La guía provee apoyo en los procesos de valoración y mitigación dentro de la gestión de riesgos.

2.4.7 ISO/IEC 27005

Guía para la gestión del riesgo en relación a la seguridad de la información.

Ilustración 3: Guía para la Gestión de Riesgos ISO/IEC 27005



2.4.8 ISO 27000

Contiene términos y definiciones que se emplean en toda la serie 27000, La aplicación de cualquier estándar necesita de un vocabulario claramente definido, que evite distintas interpretaciones de conceptos técnicos y de gestión.

2.4.9 ISO 27001

Es la norma principal de requisitos del sistema de Gestión de seguridad de la información. Tiene su origen en la BS 7799-2:2002 y es la norma a la cual se certifican por auditores externos los SGSI de las organizaciones.

2.4.10 ISO 27002

Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. No es certificable, será la sustituta de ISO17799:2005 que la que actualmente está en vigor.
La ISO17799:2005 contienes 39 objetivos de control y 133 controles, agrupados en 11 dominios.

2.4.11 ISO 27003

Guía de implementación de SGSI e información acerca del uso del modelo de PDCA - PHVA (Planificar, Ejecutar, Verificar y Actuar) y de los requerimientos de sus fases.

2.4.12 ISO 27004

Esta norma Internacional proporciona orientación sobre la elaboración y utilización de medidas y la medición para evaluar la eficacia de un sistema de gestión de la información aplicadas de seguridad (SGSI) y controles o grupos de controles, tal como se especifica en la norma ISO/IEC 27001.
Esto incluye la política, gestión de información de riesgo de seguridad, objetivos de control, controles, procesos y procedimientos, y apoyar el proceso de su revisión, ayudar a determinar si alguno de los procesos de SGSI o controles necesitan ser cambiados o mejorados.

Hay que tener en cuenta que ninguna de las mediciones de los controles puede garantizar la seguridad total.

2.5 MARCO LEGAL

En Colombia desde la expedición de la Ley 87 de 1993, se gesta el concepto de riesgos, al establecer como uno de los objetivos del control interno en el artículo 2 literal a) "proteger los recursos de la organización, buscando su adecuada administración ante posibles riesgos que los afectan". También el literal f) expresa: "definir y aplicar medidas para prevenir los riesgos, detectar y corregir las desviaciones que se presenten en la organización y que puedan afectar el logro de los objetivos".

La creación de una política de administración de riesgos informáticos en la oficina de admisiones registro y control tiene como base legal las siguientes normas y reglamentos.

El análisis de riesgos puede venir requerido por precepto legal. Tal es el caso de Real Decreto 3/2010, de 8 de enero, por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica. En el Capítulo II, Principios Básicos, se dice:

Artículo 6. Gestión de la seguridad basada en los riesgos.

1. El análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado.
2. La gestión de riesgos permitirá el mantenimiento de un entorno controlado, minimizando los riesgos hasta niveles aceptables. La reducción de estos niveles se realizará mediante el despliegue de medidas de seguridad, que establecerá un equilibrio entre la naturaleza de los datos y los tratamientos, los riesgos a los que estén expuestos y las medidas de seguridad.

El mismo Real Decreto 3/2010, en el Capítulo III, Requisitos Mínimos, se dice:

Artículo 13. Análisis y gestión de los riesgos.

1. Cada organización que desarrolle e implante sistemas para el tratamiento de la información y las comunicaciones realizará su propia gestión de riesgos.
2. Esta gestión se realizará por medio del análisis y tratamiento de los riesgos a los que está expuesto el sistema. Sin perjuicio de lo dispuesto en el Anexo II, se empleará alguna meto-dología reconocida internacionalmente.
3. Las medidas adoptadas para mitigar o suprimir los riesgos deberán estar justificadas y, en todo caso, existirá una proporcionalidad entre ellas y los riesgos.

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, que en su Artículo 1, Objeto de la Ley, dice así:

Las Administraciones Públicas utilizarán las tecnologías de la información de acuerdo con lo dispuesto en la presente Ley, asegurando la disponibilidad, el acceso, la integridad, la autenticidad, la confidencialidad y la conservación de los datos, informaciones y servicios que gestionen en el ejercicio de sus competencias.

La Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal, en su artículo 9 (Seguridad de los datos) dice así:

El responsable del fichero, y, en su caso, el encargado del tratamiento, deberán adoptar las medidas de índole técnica y organizativas necesarias que garanticen la seguridad de los datos de carácter personal y eviten su alteración, pérdida, tratamiento o acceso no autorizado, habida cuenta del estado de la tecnología, la naturaleza de los datos almacenados y *los riesgos a que están expuestos,* ya provengan de la acción humana o del medio físico o natural.

2.5.1 Ley 1273 del 5 de enero de 2009. Delitos informáticos

Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

2.5.2 Ley estatutaria 1266 del 31 de diciembre de 2008

Por la cual se dictan las disposiciones generales del Hábeas Data y se regula el manejo de la información contenida en bases de datos personales, en especial la financiera, crediticia, comercial, de servicios y la proveniente de terceros países y se dictan otras disposiciones.

2.5.3 Ley 1341 del 30 de julio de 2009

Por la cual se definen los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC-, se crea la Agencia Nacional del Espectro y se dictan otras disposiciones.

2.5.4 Ley estatutaria 1581 de 2012

Entró en vigencia la Ley 1581 del 17 de octubre 2012 de **PROTECCIÓN DE DATOS PERSONALES**, sancionada siguiendo los lineamientos establecidos por el Congreso de la República y la Sentencia C-748 de 2011 de la Corte Constitucional.

Como resultado de la sanción de la anunciada ley toda entidad pública o privada, cuenta con un plazo de seis meses para crear sus propias políticas internas de manejo de datos personales, establecer procedimientos adecuados para la atención de peticiones, quejas y reclamos, así como ajustar todos los procesos, contratos y autorizaciones a las disposiciones de la nueva norma.

2.5.5 Ley 603 de 2000

Esta ley se refiere a la protección de los derechos de autor en Colombia. Recuerde: el software es un activo, además está protegido por el Derecho de Autor y la Ley 603 de 2000 obliga a las empresas a declarar si los problemas de software son o no legales.

2.5.6 El derecho de autor[5].

Constitución Política de 1991. En su artículo 61, que expresa: "El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley".

Decisión 351 de 1993, o Régimen Común Andino sobre Derecho de Autor y Derechos Conexos, es de aplicación directa y preferente a las leyes internas de cada país miembro del Grupo Andino.

Ley 23 de 1982, contiene las disposiciones generales y especiales que regulan la protección del derecho de autor en Colombia.

Ley 44 de 1993 (febrero 15), modifica y adiciona la Ley 23 de 1982 y se modifica la Ley 29 de 1944.

Decreto 1360 de 1989 (junio 23). "Por el cual se reglamenta la inscripción de soporte lógico (software) en el Registro Nacional del Derecho de Autor".

Decreto 460 de 1995, por la cual se reglamenta el Registro Nacional de Derecho de Autor.

[5] MINISTERIO DEL INTERIOR Y DE JUSTICIA DE COLOMBIA. Dirección Nacional del Derecho de Autor. Unidad Administrativa Especial. [en línea].
http://www.propiedadintelectualcolombia.com/Site/LinkClick.aspx?fileticket=yDsveWsCdGE%3D&tabid=

Decreto 1474 de 2002 (julio 15). "Por el cual se promulga el "Tratado de la OMPI, Organización Mundial de la Propiedad Intelectual, sobre Derechos de Autor (WCT)", adoptado en Ginebra, el veinte (20) de diciembre de mil novecientos noventa y seis (1996)".

2.5.7 Ley 734 de 2002, Numeral 21 y 22 del Art. 34.

Son deberes de los servidores Públicos "vigilar y salvaguardar los bienes y valores que le han sido encomendados y cuidar que sean utilizados debida y racionalmente", y "responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización"[6].

2.5.8 Acuerdo N° 084

Septiembre 11 de 1995 Estructura de organismo de dirección y gobierno Art. 38 de la oficina de admisiones, registro y control.

2.5.9 Acuerdo N° 065 Agosto 26 de 1996 Estatuto Estudiantil

2.5.10 Norma Técnica Colombiana NTC-ISO/IEC 27000

Evaluación y tratamiento del riesgo Evaluación de los riesgos de seguridad

[6] SUPERINTENDENCIAS DE SOCIEDADES. Manual Manejo y Control Administrativo de los Bienes de Propiedad. Bogotá D.C., Colombia, 2009. 29h. [en línea]. http://www.supersociedades.gov.co/web/Ntrabajo/SISTEMA_INTEGRADO/Documentos%20Infraestructura/DOCUMENTOS/GINF-M-001%20MANUAL%20ADMINISTRATIVO.pdf

3 DISEÑO METODOLOGICO

3.1 TIPO DE INVESTIGACIÓN

El proyecto estará fundamentado en una investigación descriptiva.

3.2 POBLACIÓN

La población está conformada por el personal de la oficina de admisiones registro y control de la universidad Francisco de Paula Santander Ocaña.

3.3 MUESTRA

Debido que el personal de la oficina de admisiones registró y control de la Universidad Francisco de Paula Santander no supera un total de 10 personas se trabajara con toda la población involucrada en los procesos de la oficina.

3.4 TECNICAS DE RECOLECCION DE LA INFORMACION

3.4.1 FUENTES PRIMARIAS

Entrevista al jefe de la oficina de admisiones registro y control de la Universidad Francisco de Paula Santander Ocaña.

Entrevista al personal operativo de la oficina de admisiones registro y control de la Universidad Francisco de Paula Santander Ocaña.

Visita de observación y aplicación de instrumentos de recolección de la información en la oficina de admisiones registro y control de la Universidad Francisco de Paula Santander Ocaña.

Documentación de los procesos establecidos en la oficina de admisiones registro y control de la Universidad Francisco de Paula Santander Ocaña.

3.4.2 Fuentes segundarias

Apoyo en leyes, estándares y normas relacionadas con la seguridad de la información, auditoria basada en riesgos y administración de riesgos.

Artículos científicos relacionados con la seguridad de la información, auditoria basada en riesgos y administración de riesgos.

4 PRESENTACIÓN DE RESULTADOS

Para el logro de los objetivos propuestos se implementaron una serie de actividades que permiten identificar resultados evidenciado los riegos que enfrenta la oficina de admisiones registro y control.

Descripción Objetivo Especifico	**Actividad**	**Indicador**
Realizar un reconocimiento diagnóstico de la dependencia de Admisiones Registro y Control, para identificar y valorar los riesgos.	• Observar Explorar las instalaciones de la dependencia. • Identificar y analizar los factores de riesgo de la información, a través de aplicación de instrumentos de recopilación de información.	Listas de verificación Entrevistas Encuestas Listas de chequeo
Identificar la norma adecuada para el diseño de una política de administración de riesgos con el fin de minimizar posibles daños e impactos.	• Estudio y análisis de los procesos que contemplan las diferentes normas enfocadas al estudio de administración de riesgos de la información. • Clasificación y análisis de las etapas de la administración de riesgos de la información	Análisis de resultados obtenidos en el objetivo anterior. Cuadro comparativo de las normas más reconocidas en la administración de riesgos.
• Determinar elementos, procesos y características de la norma en la integración del plan de gestión de riesgos de la oficina de	• Comparación de procesos establecidos en la dependencia con los procesos de la norma. • Integración de Principios y	Valoración de Elementos. Análisis de la valoración a través de tablas y

admisiones registro y control.	Procesos de la dependencia y los descritos en la norma. • Consolidación de los esquemas encontrados con los hallazgos observados en la dependencia.	esquemas. Descripción de resultados. Documento: "Diseño de una Política de gestión de riesgo de la información para la oficina de Admisiones Registro y Control de la Universidad Francisco de Paula Santander Ocaña" Conclusiones Recomendaciones

4.1 RECONOCIMIENTO DE LA OFICINA DE ADMISIONES REGISTRO Y CONTROL DE UFPSO

En la etapa de reconocimiento realizado a la oficina de admisiones registro y control, se aplicaron instrumentos de recolección de información, los cuales arrojaron datos valiosos, que brindan soporte fundamental para el desarrollo del objetivo de la presente propuesta.

La información gestionada por la oficina de admisiones registro y control tiene un alto nivel de sensibilidad en cada uno de sus procesos, está expuesta permanentemente a riesgos que comprometen su disponibilidad, integridad y confidencialidad. Con el fin de apoyar la seguridad de dicha información se propone diseñar una política de Gestión de riesgos.

La información recolectada nos evidenció que la oficina de admisiones registro y control cuenta con una misión y visión; pero como resultado de al trabajo de investigación **Guia para la implementación de gobierno corporativo de TI** [7] se encuentra en estudio acoger el direccionamiento estratégico planteado.

[7] **Guia para la implementación de gobierno corporativo de TI** [Libro] / aut. Perez Yesica Maria Perez. - Ocaña : [s.n.], 2014.

4.1.1 Misión y Visión de la oficina de admisiones, registro y control.

Misión

Prestar un buen servicio a los estudiantes y demás estamentos en cada uno de los requerimientos que se hagan ya que ésta dependencia es un pilar fundamental por los documentos que allí reposan y hacer cumplir las normas del Reglamento Estudiantil en materia de desempeño académico.

Visión

La oficina de Admisiones Registro y Control será la dependencia en donde los estudiantes encontrarán sistematizado toda la información académica con sólo consultar a la página de la Universidad y demás información que se requiera de ésta oficina.

4.1.2 Misión y Visión en proceso de aprobación

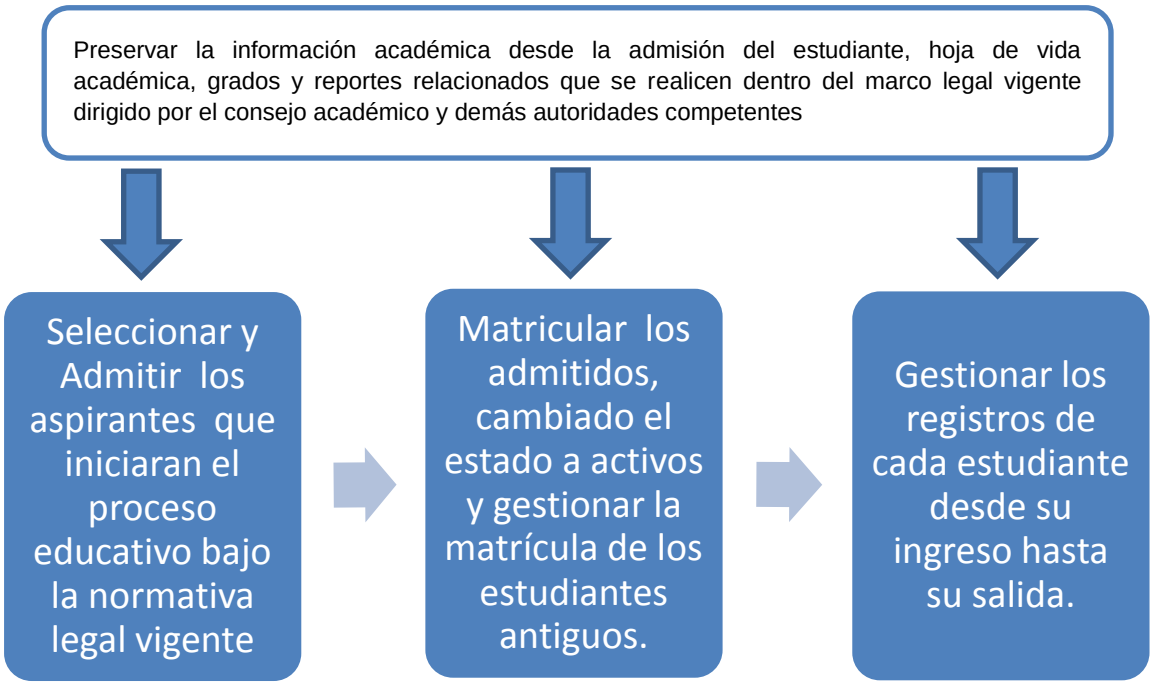
Ilustración 4: Misión y visión de la oficina de admisiones, registro y control[8]

Fuentes: *Guia para la implementación de gobierno corporativo de TI.* Ocaña. Perez, Y. M. (2014).

[8] Perez, Y. M. (2014). *Guia para la implementación de gobierno corporativo de TI.* Ocaña.

4.1.3 Objetivo General y específico de la oficina de Admisiones, Registro y control

Ilustración 5: Objetivo General y objetivos específicos de la Oficina de Admisiones Registro y Control



Fuente: Guía para la implementación de gobierno corporativo de TI. Ocaña.(Perez,Y.M)

4.1.4 Principios y Valores de la oficina de Admisiones Registro y Control.

Entre los principios corporativos que se aplican en ésta dependencia que ésta constantemente en comunicación y contacto con el público (estudiantes, profesores, personal administrativo y visitantes) es el de mantener diariamente lo siguiente principios:

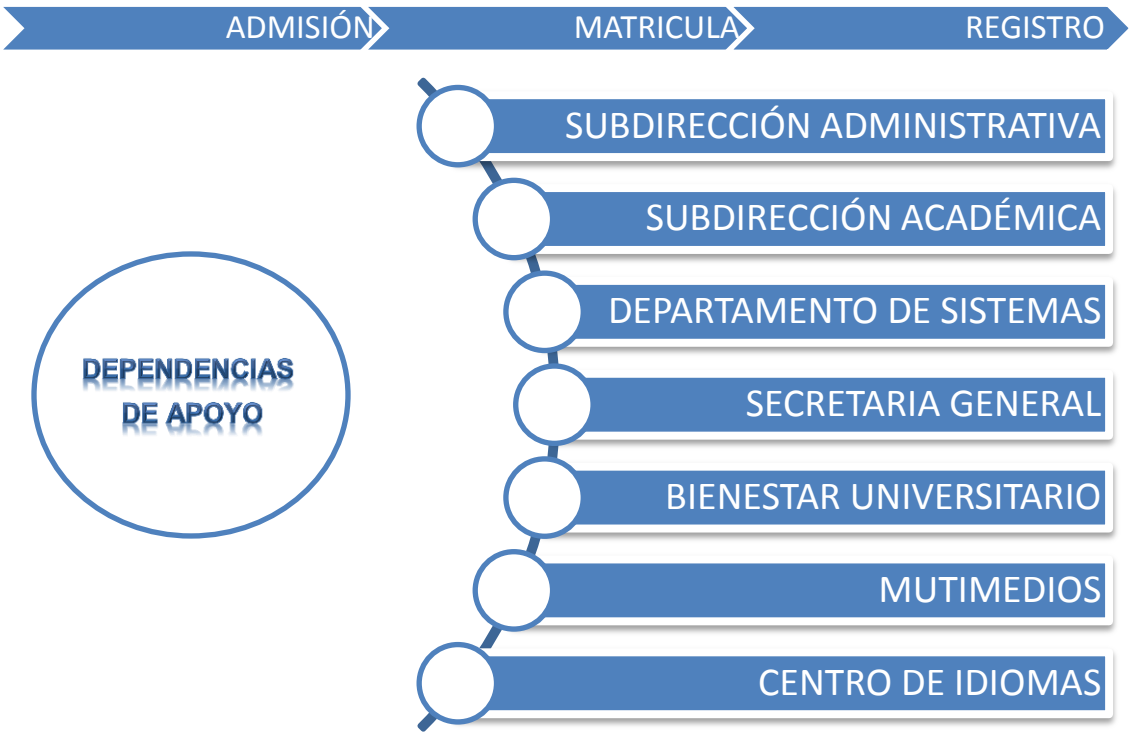
- EL RESPETO
- LA RESPONSABILIDAD
- HONRADEZ.

Lo anterior se consigue Manteniendo las buenas relaciones personales, con los diferentes estamentos de la Universidad, para conseguir un buen ambiente de trabajo.

4.1.5 Cadena de Valor de la Oficina de Admisiones Registro y Control:

La oficina de admisiones registro y control tiene 3 procesos fundamentales que son la admisión, matrícula y registro, para llevar a cabo un buen resultado en sus procesos la oficina tiene 7 dependencias de apoyo donde suministran información, apoyo en los procesos y parámetros, de esta forma consolidando un resultado que apoya el logro de sus objetivos.

Ilustración 6: Cadena de Valor de la oficina de Admisiones Registro y Control[9]



Fuente: Guía para la implementación de gobierno corporativo de TI. Ocaña.(Perez,Y.M)

4.1.6 Procesos de la Oficina de Admisiones Registro y control

La oficina de admisiones tiene documentados sus procesos de una forma lineal para mayor entendimiento de los procesos se toman los 3 procesos principales y de ellos se derivan los subprocesos, de esta forma facilitando la delegación de funciones.

[9] Perez, Y. M. (2014). *Guia para la implementación de gobierno corporativo de TI.* Ocaña

Ilustración 7: Procesos de la oficina de admisiones registro y control

Fuente: Adaptación por Autores del proyecto

4.1.7 Modelo de Actores:

La oficina de admisiones registro y control no tenía documentado un modelo de actores por lo cual se definió el siguiente:

Ilustración 8: Modelo de actores

Subproceso Planeación			
Actores	**Ejecuta**	**Supervisa**	**Apoya**
Jefe de Admisiones Registro y Control	x		
Subdirección académica		x	
Planeación Académica		x	
División de sistemas			x
Subproceso Inscripción			
Actores	**Ejecuta**	**Supervisa**	**Apoya**
Ingeniero de apoyo SIA	x		
Secretarias	x		
Auxiliares	x		
Jefe de Admisiones Registro y Control		x	
Subdirección Administrativa(Tesorería)			x
Subproceso Selección			
Actores	**Ejecuta**	**Supervisa**	**Apoya**
Comité de Admisiones	x		
Jefe de Admisiones Registro y Control		x	

Tabla 5: (Continuación)

Ingeniero de apoyo SIA			x
Subproceso Matricula Académica			
Actores	**Ejecuta**	**Supervisa**	**Apoya**
Ingeniero de apoyo SIA	x		
Jefe de Admisiones Registro y Control		x	
Planes de Estudios			x
Jefes de Departamento			x
División de Sistemas			x
Subproceso Matricula Académica			
Actores	**Ejecuta**	**Supervisa**	**Apoya**
Ingeniero de apoyo SIA	x		
Jefe de Admisiones Registro y Control		x	
Subdirección Administrativa(Tesorería)			x
Consejo Superior Estudiantil			x
Bienestar Universitario			x
Subproceso Hoja de Vida Estudiantil			
Actores	**Ejecuta**	**Supervisa**	**Apoya**
Secretarias	x		
Auxiliares	x		
Jefe de Admisiones Registro y Control		x	
Subdirección Administrativa			x
División de Sistemas			x
Planes de Estudios			x
Subproceso Grados			
Actores	**Ejecuta**	**Supervisa**	**Apoya**
Secretarias	x		
Auxiliares	x		
Ingeniero de apoyo SIA	x		
Jefe de Admisiones Registro y Control		x	
Subdirección administrativa			x
Bienestar Universitario			x
División de Sistemas			x
Planes de Estudios			x
Secretaria General			x
Centro de Idiomas			x

Fuente: Adaptación por Autores del proyecto

4.1.8 Verificación de buenas prácticas del PMBOK

Tomando como un proyecto el desarrollo de cada semestre académico se crea un instrumento de buenas prácticas para la evaluación de las actividades de la oficina de admisiones registro y control

Tabla 1: Verificación de buenas prácticas con base al PMBOK

N	Comprobación	1	2	3	4	5	No Aplica
1	¿Existe un acta de inicio que autoriza formalmente el desarrollo de actividades y en la cual se referencie el nombre del director y se identifique el grupo de personas que participaran activamente en el mismo?			x			
2	¿Se encuentran documentados los requisitos iniciales que satisfacen las necesidades y expectativas de los actores involucrados?			x			
3	¿Existe un acta que evidencie la socialización de los resultados ante los actores involucrados?			x			
4	¿Se elaboró el Plan de Gestión del Proyecto y los documentos involucrados?		x				
5	¿Se encuentran claramente documentadas todas las actividades registradas en el Plan de Gestión del Proyecto?		x				
6	¿En Plan de Gestión se encuentran establecidos y documentados los riesgos de acuerdo a la naturaleza del proyecto?	x					
7	¿Se encuentra claramente definido el alcance del proyecto conforme a las necesidades de los actores involucrados?		x				

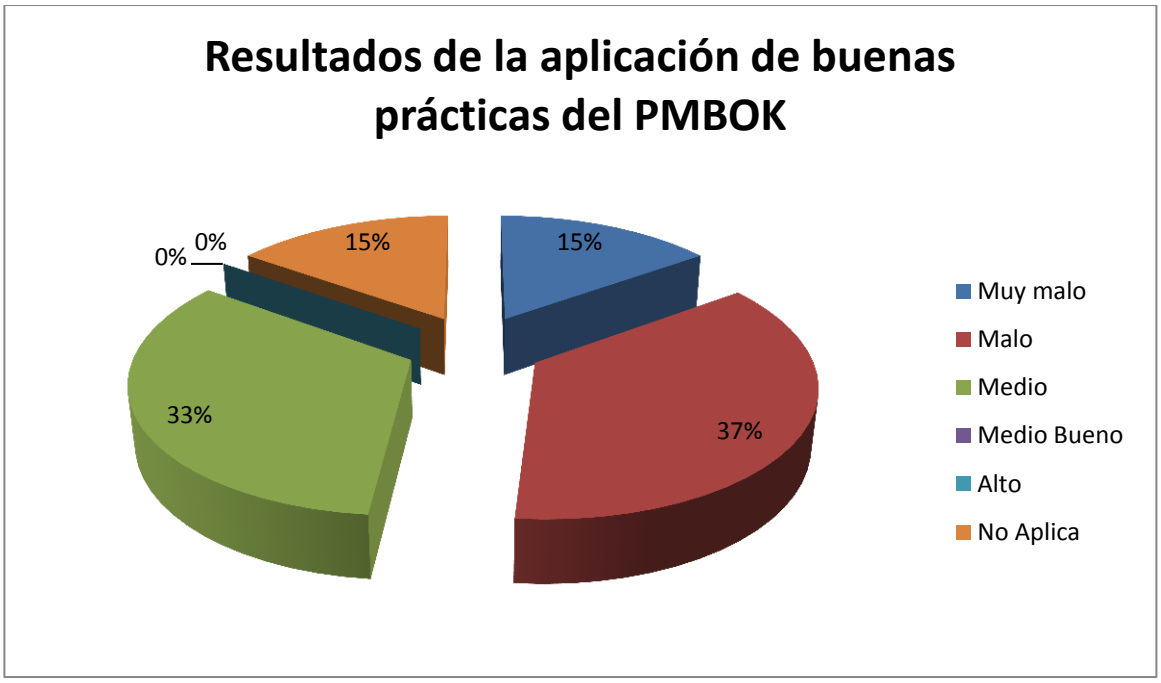
8	¿Se elaboró el documento de estructura de desglose de trabajo (EDT)?	x					
9	¿Se presentó un cronograma de actividades, especificando los recursos necesarios para llevarlas a cabo, su secuencia de ejecución, identificando para cada una el nombre del responsable, fecha inicial, fecha final?			x			
10	¿Por cada fase de la Estructura de Desglose de Trabajo se evidencian documentos entregables que permitan evaluar el cumplimiento de cada una de ellas?	x					
11	¿Existe una herramienta de control diseñada para registrar los cambios aprobados que se puedan presentar durante el proceso de ejecución del proyecto?		x				
12	¿Se presentó el documentó en el que se registre el presupuesto estimando cuantitativamente el costo del proyecto?						x
13	¿Existe un documento en el que se evidencien y se justifiquen los cambios aplicados al presupuesto inicial del proyecto?						x
14	¿Se evidencia el Plan de Administración de riesgos con los procedimientos claramente documentados?	xx					
15	¿Se evidencia el Plan de respuesta de riesgos?	x					
16	¿Existe un mecanismo para evaluar los riesgos inherentes al proyecto?			x			
17	¿Existe una persona a cargo del sistema de control de calidad?			x			

18	¿Existe un mecanismo de respuesta para las no conformidades?		x				
19	¿Existe un mecanismo de registro de avances para cada una de las actividades establecidas en el cronograma?		x				
20	¿Se estableció un Plan de recurso humano?		x				
21	¿Existen documentos que evidencie el nivel de desempeño del recurso humano contratado?		x				
22	¿Se aplicó un instrumento de evaluación para cada colaborador que permita diseñar programas de capacitación al recurso humano?		x				
23	¿Se diseñó un plan de compras y adquisiciones conforme al presupuesto establecido para el proyecto?						x
24	¿Existe una herramienta que permita llevar control del salida de los elementos establecidos en el Plan de compras?						x
25	¿Existe Plan de comunicaciones?						
26	¿Existen herramientas que permite realizar seguimiento a las actividades del plan de comunicaciones?		x				
27	¿Los medios de comunicaciones empleados fueron pertinentes para que los actores involucrados en el proyecto conocieran los avances del mismo?						
28	¿La selección de los proveedores se llevó basada en políticas previamente estipuladas?						x
29	¿Existen actas de seguimiento?		x				
30	¿Existe formalmente un equipo responsable del seguimiento de			x			

	ejecución de las actividades?						
31	¿En las actas de seguimiento se identifica plenamente el nivel de avance y los compromisos pendientes en sus operaciones?			x			
32	¿Existe un mecanismo que permita evaluar en términos generales a los operarios de la oficina?			x			
33	¿Existe un documento formal de cierre de cada actividad?		x				

Fuente: Autores del proyecto

Ilustración 9: Resultados de la aplicación de buenas prácticas del PMBOK



Fuente: Autores del proyecto

4.1.9 Diagnóstico de la gestión de Riesgos de TI en la oficina de Admisiones Registro y Control.

Aplicación de la encuesta

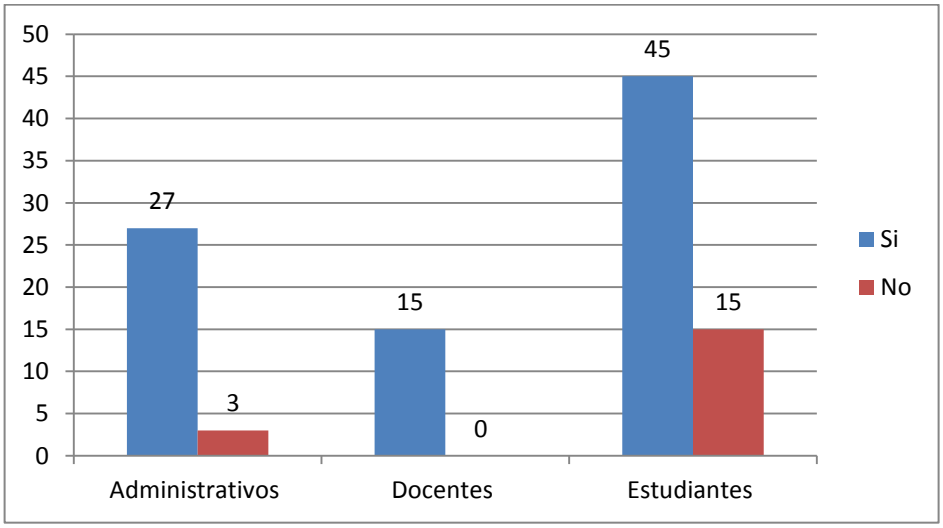
Determinar el nivel de sensibilidad de la información manipulada en la oficina de admisiones registro y control, los riesgos a los que está expuesta y los controles y vulnerabilidades a las que presenta.

¿La información empleada para el desarrollo de sus funciones es importante?

Tabla 2: ¿La información empleada para el desarrollo de sus funciones es importante?

Personal Encuestado		
	Si	**No**
Administrativos	**27**	**3**
Docentes	**15**	**0**
Estudiantes	**45**	**15**

Grafica 1: Resultado de la importancia de la información



Fuente: Desarrollada por los autores del proyecto

Como se evidencia en la gráfica anterior la información utilizada y manipulada en la oficina de admisiones registro y control por parte del personal administrativo es de vital importancia para el desarrollo de la misma.

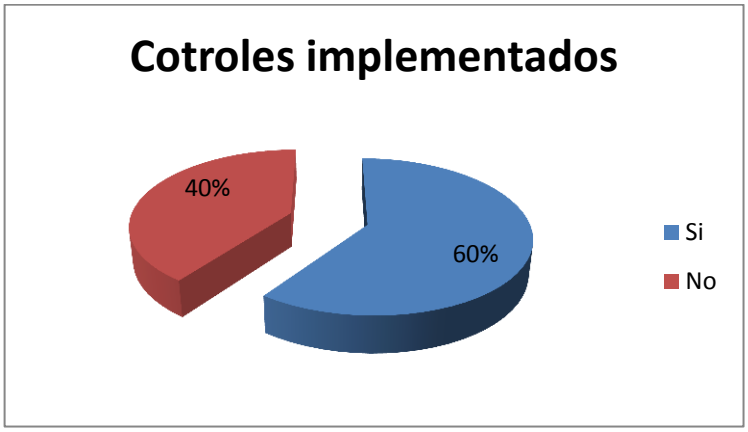
Tabla 3: ¿Están implementados controles para garantizar la información?

Criterio	**Encuestados**
Si	**6**

No	**4**

Fuente: Desarrollada por los autores del proyecto

Grafica 2: Implementación de controles para garantizar la información



Fuente: Desarrollada por los autores del proyecto

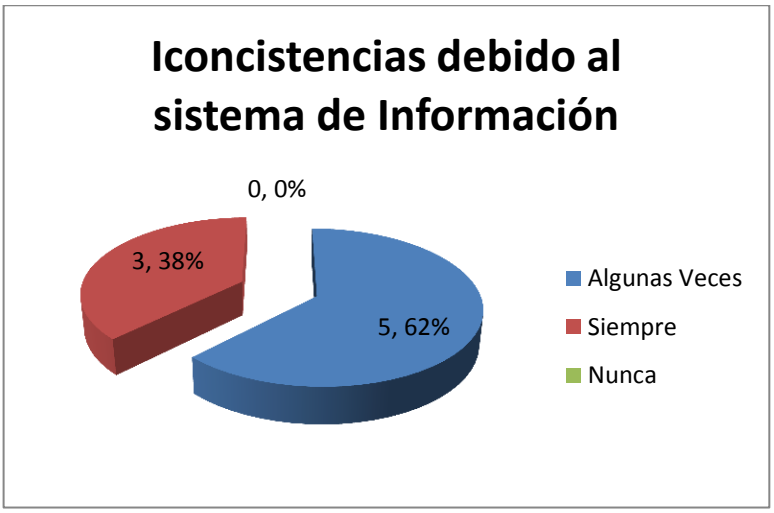
La grafica anterior nos muestra que el personal administrativo se encuentra dividido en cuanto a la percepción de los controles establecidos, donde un 60% dice que si existen controles el otro 40% afirma que no.

Tabla 4: ¿Se presentan inconsistencias debido al sistema de información utilizado?

Criterio	Encuetados
Algunas Veces	**5**
Siempre	**3**
Nunca	**0**

Fuente: Desarrollada por los autores del proyecto

Grafica 3: Inconsistencias debido al sistema de información.



Fuente: Desarrollada por los autores del proyecto

La grafica nos muestra que el hecho de que la oficina utilice sistemas de información para el registro sistemático de la información no garantiza la seguridad de la información debido a las inconsistencias ocasionadas por el mismo.

Tabla 5: ¿Existen registros de los riesgos detectados en la oficina de admisiones registro y control?

Tabla 6: Registro de los riesgos en la oficina de admisiones registro y control

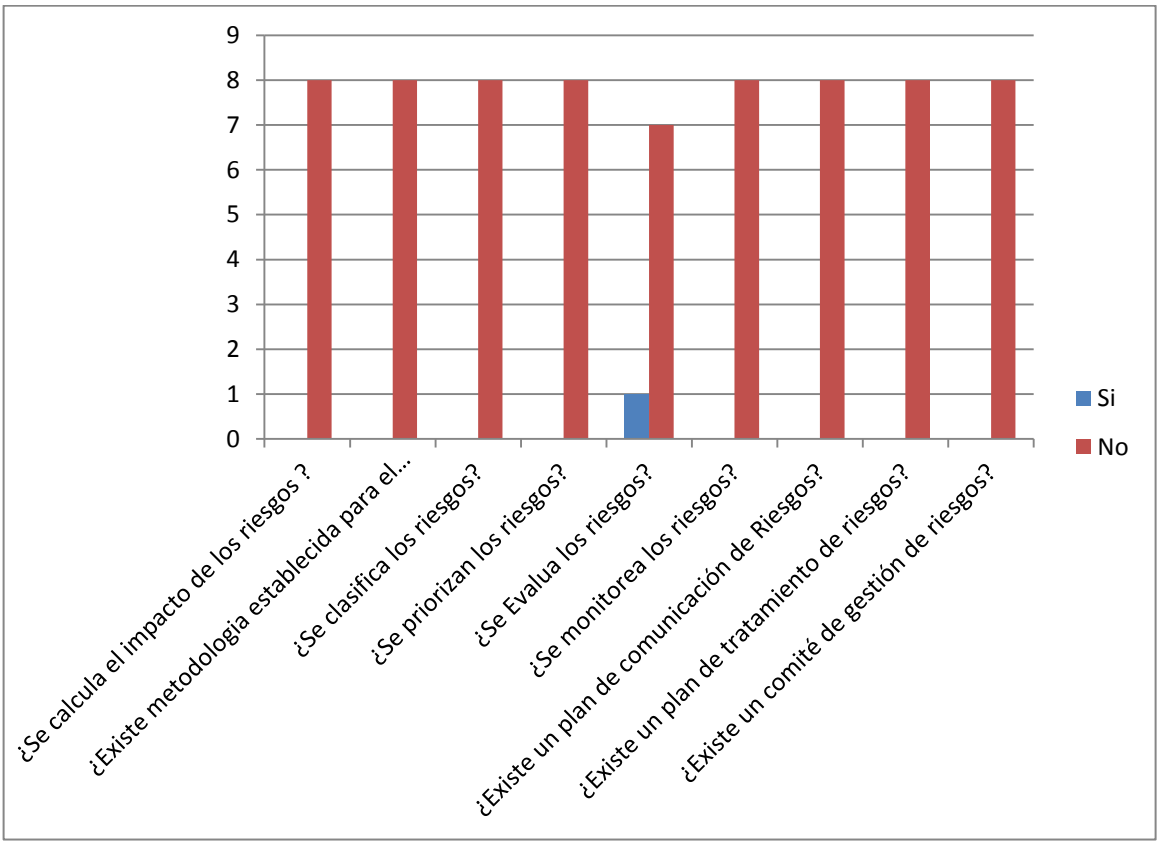
ítem	Frecuencia
Si	**6**
No	**2**

Fuente: Desarrollada por los autores del proyecto

Fuente: Desarrollada por los autores del proyecto

La grafica anterior nos muestra que no siempre son documentados los riesgos que se presentan en la oficina de admisiones registro y control.

Grafica 4: Reconocimiento del Análisis de Riesgos



Fuente: Desarrollada por los autores del proyecto

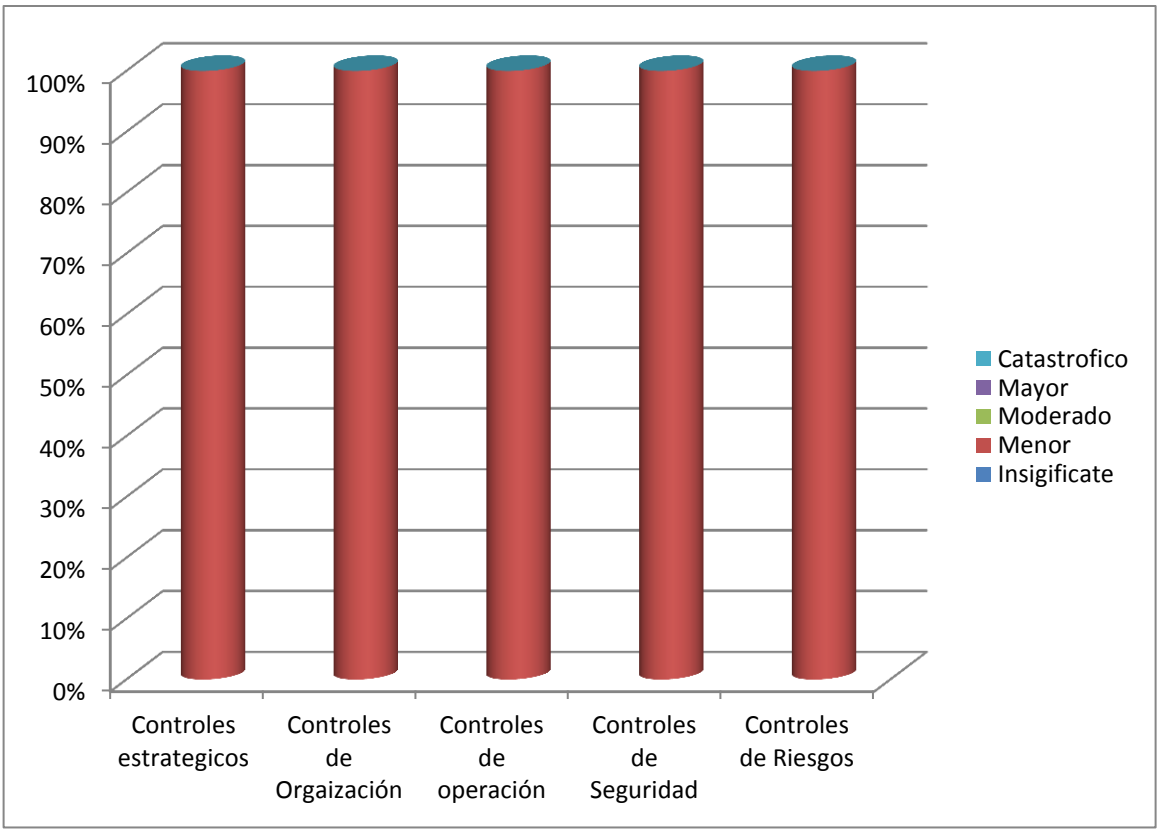
Según la información recolectada en la oficina de admisiones registro y control no se identifican los riesgos ni son tratados, evidenciando de esta forma la necesidad de una política como paso inicial para la debida gestión de riesgos e la oficina de admisiones registro y control.

4.1.10 Auditoria de Gestión de Riesgos de TI

Se realizó una auditoria de cumplimiento de la gestión de riesgos de TI de la oficina de admisiones registro y control aplicando listas de chequeo basada en normas estándares y buenas prácticas como NTC ISO/IEC 27001, NTC ISO/ IEC 31000 y Cobit.

A través de este análisis se evidencio que la oficina de admisiones registró y control presenta los siguientes resultados.

Grafica 5: Controles establecidos



Fuente: Desarrollada por los autores del proyecto

4.1.11 Mapa de riesgos

Contexto estratégico de la oficina de admisiones registro y control

Propender por que la información académica relacionada con Admisiones, matriculas, Novedades académicas, reconocimientos y sanciones académicas grados y demás aspectos relacionados se realicen dentro del marco legal vigente y con base en la programación establecida mediante calendario académico adoptado por el consejo académico y demás autoridades competentes.

Tabla 7: Contexto estratégico

FORMATO CONTEXTO ESTRATÉGICO				
Nombre del Proceso		ADMISIONES, REGISTRO Y CONTROL ACADÉMICO		
No.	**Factores**	**Internos (Debilidad)**	**Externos (Amenazas)**	**Ampliación / Causa**
1	Procesos Tecnología	x		Recepción de documento adulterados o con inconsistencias Fallas en la plataforma utilizada para la verificación de los puntajes del ICFES Incumplimiento de los cronogramas establecidos para el desarrollo de los procesos de admisiones Dificultades en la divulgación de los resultados de los procesos de admisión
2	Procesos Tecnología	x		Incumplimiento de calendario Académico. Errores en registros de matrícula de asignaturas Registro inoportuno de notas en el sistema Fallas en la asignación académicas.

				Suspensión de clases por efecto de paros estudiantiles Entrega extemporánea de documentos por parte de los estudiantes o Directores de Programa Fallas en la plataforma en la que se administra la información de los estudiantes
3	Procesos Tecnología	x		Dificultad para la ubicación de la información existente en los archivos de la Universidad Pérdida o daño de documentos o soportes para la expedición de certificación Incumplimiento de los términos para la expedición de certificación Suministro inexacto de datos para la expedición de certificaciones y constancias Desactualización de los datos del estudiante, como cédula de ciudadanía Historial académico desactualizado
4	Procesos Tecnología	x		Fallas en la plataforma utilizada para el registro de calificaciones de los estudiantes Registro de notas con inconsistencias o errores Entrega de notas por fuera de las fechas programadas Fallas en la creación de la carga académica de los cursos

				Entrega de notas por fuera de las fechas programadas Proceso de matrículas por fuera de las fechas programadas

4.1.12 Identificación de los riesgos

Tabla 8: Identificación del Riesgo

Nombre del Proceso		**ADMISIONES, REGISTRO Y CONTROL**			
Objetivo del Proceso		Propender por que la información académica relacionada con Admisiones, matriculas, planes de estudio, Novedades académicas, reconocimientos y sanciones académicas grados y demás aspectos relacionados se realicen dentro del marco legal vigente y con base en la programación establecida mediante calendario académico adoptado por el consejo académico y demás autoridades competentes.			
No.	**CAUSAS Factores Internos y Externos. Incluye Agente Generador**	**RIESGO**	**DESCRIPCIÓN**	**EFECTOS (Consecuencias)**	**TIPO / IMPACTO**
1	Recepción de documento adulterados o con inconsistencias Fallas en la plataforma utilizada para la verificación	Inconsistencias en la admisión de nuevos estudiantes	Reclamaciones por parte de los aspirantes a los distintos programas ofrecidos por la Universidad, con la consecuente expedición de	Admisión de personas que no reúnen requisitos o que no cuenta con el puntaje suficiente para ser admitido Reclamaciones e insatisfacción de los aspirantes rechazados	Operativo Cumplimiento Estratégico

	de los puntajes del ICFES Incumplimiento de los cronogramas establecidos para el desarrollo de los procesos de admisiones Dificultades en la divulgación de los resultados de los procesos de admisión		notas aclaratorias, rectificaciones y/o modificaciones de los listados de admitidos por parte del área de registro y control.	Sanciones para la Universidad y sus funcionarios por la falla en los procesos de admisiones Detrimento o daño de la de la imagen institucional de la Universidad	
2	Incumplimiento de calendario Académico. Errores en registros de matrícula de asignaturas Registro inoportuno de notas en el sistema Fallas en la asignación académicas. Suspensión de clases por efecto de paros	Inconsistencias en el proceso de matriculas	Presencia de dificultades por parte de los estudiantes y autoridades académicas para la formalización de la matrícula en los diferentes programas de la modalidades presencial y Distancia ofrecidos por la Universidad	Afectación de los procesos académicos Inconvenientes para la iniciación de calendario académico Inconveniente para el registro de las asignaturas por parte de los estudiantes antiguos Insatisfacción de docentes y estudiantes frente al proceso de matriculas	operativo Estratégico

	estudiantiles Entrega extemporánea de documentos por parte de los estudiantes o Directores de Programa Fallas en la plataforma en la que se administra la información de los estudiantes				
3	Dificultad para la ubicación de la información existente en los archivos de la Universidad Pérdida o daño de documentos o soportes para la expedición de certificación Incumplimiento de los términos para la expedición de certificación	Inconsistencia en certificaciones elaboradas.	Errores en los datos registrados en las constancias y hojas de vida académicas	Perjuicios para el solicitante por la no entrega o entrega inoportuna de la constancia o certificación requerida Insatisfacción del solicitante manifestada en peticiones, quejas o reclamos Deterioro o daño de la imagen institucional de la universidad	Estratégico

	Suministro inexacto de datos para la expedición de certificaciones y constancias Desactualización de los datos del estudiante, como cédula de ciudadanía Historial académico desactualizado				

4.1.13 Análisis del Riesgo

El resultado de este análisis de riego nos arroja

Tabla 9: Calificación y Evaluación del Riesgo

Nombre del Proceso		ADMISIONES, REGISTRO Y CONTROL ACADÉMICO						
Objetivo del Proceso		Propender por que la información académica relacionada con Admisiones, matriculas, planes de estudio, Novedades académicas, reconocimientos y sanciones académicas grados y demás aspectos relacionados se realicen dentro del marco legal vigente y con base en la programación establecida mediante calendario académico adoptado por el consejo académico y demás autoridades competentes.						
No.	**RIESGO**	**CALIFICACIÓN DEL RIESGO**					**EVALUACIÓN RIESGO**	
		Probabilidad		**Impacto**		**VALOR**		
1	Inconsistencias en la admisión de nuevos estudiantes	C	Posible	3	Moderado	C3	A	Zona de Riesgo Alta

2	Inconsistencias en el proceso de matriculas	C	Posible	3	Moderado	C3	A	Zona de Riesgo Alta
3	Inconsistencia en certificaciones elaboradas.	C	Posible	3	Moderado	C3	A	Zona de Riesgo Alta
4	Inconsistencias en el registro de calificaciones por asignatura.	C	Posible	3	Moderado	C3	A	Zona de Riesgo Alta

TABLA DE PROBABILIDAD

Nivel	Concepto	Descripción
A	Casi Certeza	Se espera que ocurra en la mayoría de las circunstancias
B	Probable	Probablemente ocurrirá en la mayoría de las circunstancias
C	Posible	Podría ocurrir en algún momento
D	Improbable	Pudo ocurrir en algún momento
E	Raro	Puede ocurrir solo en circunstancias excepcionales

TABLA DE IMPACTO

Nivel	Concepto	Descripción
1	Insignificante	Afectaría el desarrollo de tareas, actividades y procedimientos
2	Menor	Afectaría el desarrollo de otros procesos institucionales
3	Moderado	Generaría paro intermitente del proceso
4	Mayor	Generaría el paro total del proceso
5	Catastrófico	Generaría el paro total de la entidad

Mapa de Riesgos por Procesos

Tabla 10: Mapa de Riesgos Por procesos

No.	RIESGO	IMPACTO	PROBABILIDAD	EVALUACIÓN RIESGO	CONTROLES EXISTENTES	ESTADO DEL CONTROL	VALORACIÓN RIESGO	OPCIONES DE MANEJO	ACCIONES
1	Inconsistencias en la admisi	Moderado	Posible	Zona de Riesgo Alta	Verificación de documentos al momento	Los controles son efectiv	Zona de Riesgo Moder	Asumir o Reducir el	Actualización del procedimiento de admisiones

	ón de nuevos estudiantes				de la recepción Verificación puntajes ICFES por plataforma Control al cronograma de admisiones Verificación de los listados de admitidos Tramitación y respuesta a las reclamaciones	os y están documentados	ada	Riesgo	Revisión periódica de la plataforma y actualización del acceso y perfiles de los usuarios Control y seguimiento al cronograma de admisiones Implementación del procedimiento para la atención y solución de reclamaciones Publicación de notas aclaratorias ante las reclamaciones resueltas
2	Inconsistencias en el proceso de matriculas	Moderado	Posible	Zona de Riesgo Alta	Cumplimiento efectivo del Calendario Académico. Aplicación adecuada de procedimientos Verificación de	Los controles son efectivos y están documentados	Zona de Riesgo Moderada	Asumir o Reducir el Riesgo	Socialización y aplicación del calendario académico en las facultades Seguimiento y control del calendario Académico Reporte oportuno de la las notas en linea por parte de los

					documentos				docentes
3	Inconsistencia en certificaciones elaboradas.	Moderado	Posible	Zona de Riesgo Alta	Verificación datos del solicitante Verificación información disponible en archivos Verificación certificaciones antes de su entrega No préstamo de las hojas de vida Revisión periódica del estado del Archivo de la Oficina	Los controles son efectivos y están documentados	Zona de Riesgo Moderada	Asumir o Reducir el Riesgo	Revisión y actualización periódica de notas y de datos del estudiante Documentación del procedimiento de solicitud y entrega de Certificados de estudio Actualización y modernización del sistema de archivo Automatizar y estandarizar la elaboración de certificados de estudio
Tabla 9. Continuación)									
4	Inconsistencias en el registro de calificaciones	Moderado	Posible	Zona de Riesgo Alta	Verificación de las calificaciones antes de su ingreso al sistema	Los controles existentes son efectivos pero	Zona de Riesgo Moderada	Asumir o Reducir el Riesgo	Establecer y divulgar controles sobre el reporte de las novedades académicas.

	por asignatura.				Capacitación a Docentes y Tutores en el manejo e importancia de la Plataforma Rectificación de notas en caso de inconsistencias Verificación de la carga académica creada por Planeación Institucional Verificación de la plataforma Académico	no están documentados			Capacitación y sensibilización de los Docentes en el reporte oportuno de calificaciones en línea con base en el calendario académico. Establecer filtros de control por parte de la s unidades académicas Verificación de la asignación académica antes y después de ingresarla a plataforma

Formato de evaluación del nivel de madurez

Tabla 11: Nivel de Madurez PO9

DOMINIO: PLANEACIÓN Y ORGANIZACIÓN					
PO9: Evaluar y Administrar los Riesgos de TI					
Niveles de los modelos de madurez		Cumple	Parcialmente	No cumple	Observaciones
Nivel	La evaluación de riesgos para los procesos y las decisiones de negocio no ocurre. La				

0	organización no toma en cuenta los impactos en el negocio asociados a las vulnerabilidades de seguridad y a las incertidumbres del desarrollo de proyectos. La administración de riesgos no se ha identificado como algo relevante para adquirir soluciones de TI y para prestar servicios de TI.				
Nivel 1	Los riesgos de TI se toman en cuenta de manera ad hoc. Se realizan evaluaciones informales de riesgos según lo determine cada proyecto. En algunas ocasiones se identifican evaluaciones de riesgos en un plan de proyectos pero se asignan rara vez a gerentes específicos. Los riesgos específicos relacionados con TI tales como seguridad, disponibilidad e integridad se toman en cuenta ocasionalmente proyecto por proyecto. Los riesgos relativos a TI que afectan las operaciones del día a día, son rara vez discutidas en reuniones gerenciales. Cuando se toman en cuenta los riesgos, la mitigación es inconsistente. Existe un entendimiento emergente de que los riesgos de TI son importantes y necesitan ser considerados.				
Nivel 2	Existe un enfoque de evaluación de riesgos en desarrollo y se implementa a discreción de los gerentes de proyecto. La administración de riesgos se da por lo general a alto nivel y típicamente se aplica solo a proyectos grandes o como respuesta a problemas. Los procesos de mitigación de riesgos están empezando a ser implementados donde se identificar riesgos.				
Nivel 3	Una política de administración de riesgos para toda la organización define cuándo y cómo realizar las evaluaciones de riesgos. La administración de riesgos sigue un proceso definido, el cual está documentado. El entrenamiento sobre administración de riesgos está disponible para todo el personal. La decisión de seguir el proceso de administración				

	de riesgos y de recibir entrenamiento se deja a la discreción del individuo. La metodología para la evaluación de riesgos es convincente y sólida, y garantiza que los riesgos claves para el negocio sean identificados. Un proceso para mitigar los riesgos clave por lo general se institucionaliza una vez que los riesgos se identifican. Las descripciones de puestos consideran las responsabilidades de Administración de riesgos.				
Nivel 4	Una política de administración de riesgos para toda la organización define cuándo y cómo realizar las evaluaciones de riesgos. La administración de riesgos sigue un proceso definido, el cual está documentado. El entrenamiento sobre administración de riesgos está disponible para todo el personal. La decisión de seguir el proceso de administración de riesgos y de recibir entrenamiento se deja a la discreción del individuo. La metodología para la evaluación de riesgos es convincente y sólida, y garantiza que los riesgos claves para el negocio sean identificados. Un proceso para mitigar los riesgos clave por lo general se institucionaliza una vez que los riesgos se identifican. Las descripciones de puestos consideran las responsabilidades de administración de riesgos.				
Nivel 5	La administración de riesgos ha evolucionado al nivel en que un proceso estructurado está implantado en toda la organización y es bien administrado. Las buenas prácticas se aplican en toda la organización. La captura, análisis y reporte de los datos de administración de riesgos están altamente automatizados. La orientación se toma de los líderes en el campo y la organización de TI participa en grupos de interés para intercambiar experiencias. La administración de riesgos está altamente				

	integrada en todo el negocio y en las operaciones de TI, está bien aceptada, y abarca a los usuarios de servicios de TI. La dirección detecta y actúa cuando se toman decisiones grandes de inversión o de operación de TI, sin considerar el plan de administración de riesgos. La dirección evalúa las estrategias de mitigación de riesgos de manera continua.				

4.1.14 Resultados del Análisis de Madurez

Tabla 12: Resultados del Análisis del nivel de madurez

Resultados de Análisis de Nivel de Madurez basado en Cobit 4.1 a la oficina de Admisiones Registro y Control de la Universidad Francisco de Paula Santander Ocaña			
Objetivo: Evaluar el nivel de la capacidad (CMM)		**Alcance:**	
Dominio		**Proceso**	**Nivel de Madurez**
Planear y Organizar	PO1	Definir un plan estratégico de TI.	0
	PO2	Definir la arquitectura de la información.	0
	PO3	Determinar la dirección tecnológica.	0
	PO4	Definir procesos, organización y relaciones de TI.	1
	PO6	Comunicar las aspiraciones y la dirección de la gerencia	1
	PO7	Administrar recursos humanos de TI	1
	PO9	Evaluar y administrar riesgos de TI	1
	PO10	Administrar proyectos	1
Adquirir e Implementar	AI2	Adquirir y mantener el software aplicativo	1
	AI3	Adquirir y mantener la infraestructura tecnológica	1
	AI4	Facilitar la operación y el uso	1
	AI5	Adquirir recursos de TI	1
Entregar y Dar Soporte	DS1	Definir y administrar niveles de servicio	1
	DS5	Garantizar la seguridad de los sistemas	1
	DS7	Educar y entrenar a los usuarios.	1
	DS10	Administrar los problemas	1
	DS13	Administrar las operaciones	1
Monitorear y Evaluar	ME1	Monitorear y evaluar el desempeño de TI.	1
	ME4	Proporcionar gobierno de TI.	1

Conclusiones:

1. No se encuentra definida la responsabilidad y propietarios de la información.
2. No se cuenta con un comité estratégico de Tecnología Informática.
3. Las funciones operativas no se encuentran separadas de las administrativas.
4. La parametrización de los sistemas de apoyo debe ser decidida por la subdirección académica.

4.2 NORMAS Y BUENAS PRÁCTICAS PARA LA GESTIÓN DE RIESGOS

Existe una lista de normas y buenas prácticas que orientan como se debe analizar los riesgos en una organización, para el desarrollo de este trabajo se analizaron y compararon 4 normas de las más reconocidas y utilizadas. Para ellos se establece un cuadro comparativo donde se resaltan los puntos más representantes en cada una de ellas.

Tabla 13: Cuadro comparativo de normas para la administración de riesgos

CUADRO COMPARATIVO COBIT 4.1/ISO 31000/2009 //ISO-IEC 27002//MAGERIT-V 3.0 **Riesgos de la información.**			
COBIT 4,1	**ISO 31000/2009**	**ISO/IEC 27002**	**MAGERIT – versión 3.0**
Crea y mantiene un marco de gestión de riesgos de TI, define estrategias de mitigación riesgos, identifica, analiza y evalúa cualquier impacto potencial en las metas de la organización, permite alinear el riesgo a un nivel de tolerancia aceptable.	Este estándar tiene como objetivo ayudar a las organizaciones de todo tipo y tamaño a destinar el riesgo con efectividad.	El estándar ISO/IEC 27002 contiene 11 cláusulas de control de seguridad, las cuales colectivamente contienen un total de 39 categorías de seguridades principales y una clausula introductoria que representa la evaluación y tratamiento del riesgo.	Metodología de Análisis y Gestión de riesgos de los sistemas de información. Implementa el Proceso de Gestión de Riesgos dentro de un marco de trabajo, insumo importante para la toma decisiones en la continuidad del negocio.

PO9.1 Marco de trabajo de gestión de riesgos	Establece una serie de principios de carácter genérico, fundamentales que se deben cumplir para hacer una gestión eficaz de riesgo.	14.1.1 Incluye la seguridad de la información en el proceso de gestión de continuidad del negocio.	Se basa en los principios de mandato, compromiso, diseño del marco de trabajo, implementación de la gestión del riesgo, seguimiento y revisión del marco, y mejora continua del marco. Se enfatiza en:
PO9.2 Establecimiento del contexto del riesgo	Recomienda que las organizaciones desarrollen, implementen y mejoren continuamente un marco de trabajo (framework), que conlleve a integrar los procesos de gestión del riesgo con el gobierno corporativo de la organización.	14.1.2 Continuidad del negocio y evaluación de riesgos.	Determinación del contexto: - Determina los activos de la organización, su interrelación y valor, y qué perjuicios o costos representarían para la organización.
PO9.3 Identificación de eventos	Estructura el proceso de gestión del riesgo.	13.1.1 Reporte de eventos de seguridad de información	Determina a que amenazas se exponen los activos.
PO9.4 Evaluación de riesgos de TI	Aumenta la probabilidad del logro de los objetivos misionales de las organizaciones	13.1.2 Reporte de debilidades de la seguridad	Determina salvaguardas y cuales son eficaces frente al riesgo.
PO9.5 Respuesta a los riesgos	Mejora la identificación de oportunidades y amenazas.	5.1.2 Revisión de la política de seguridad de la información.	Estima el impacto del daño sobre el activo, derivado de la materialización de las amenaza.
PO9.6 Mantenimiento y monitoreo de un plan de acción de riesgos	Brinda soporte fundamental y confiable para la toma de decisiones.		Estima el riesgo, impacto ponderado con la tasa de ocurrencia o expectativa de materialización de la amenaza.

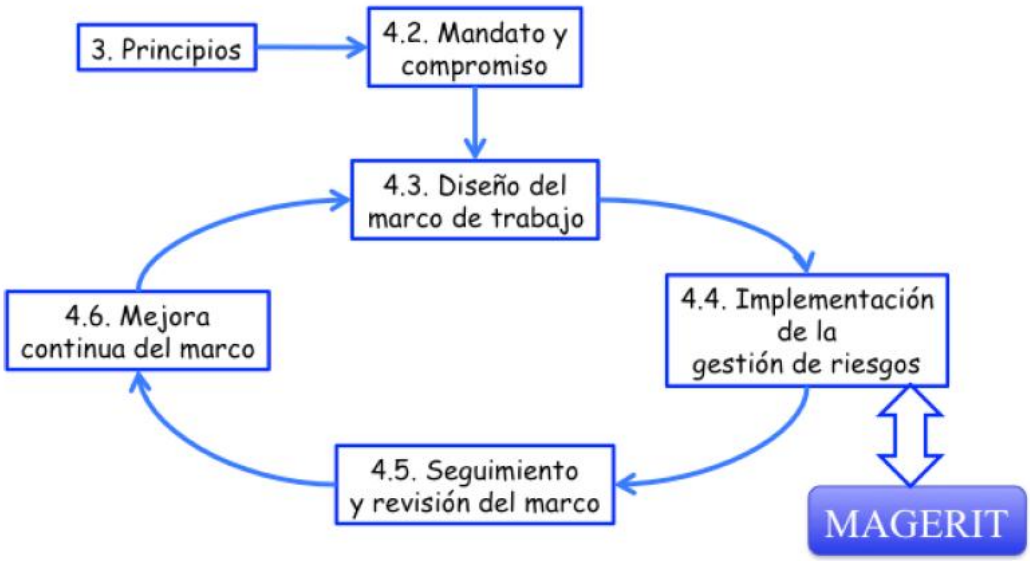
	Ayuda a cumplir con las exigencias legales y reglamentarias pertinentes, así como con las normas internacionales		Análisis y gestión de riesgos

Fuente: Autores del proyecto

4.2.1 Selección de las normas

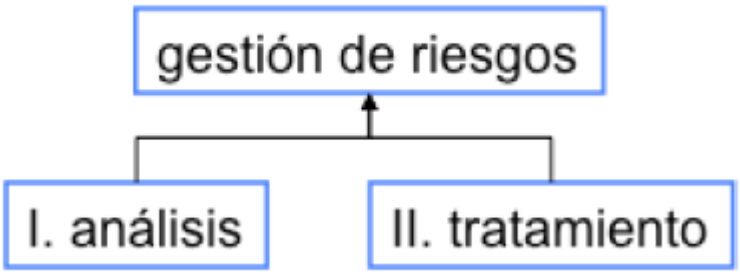
Existe una relación muy extrecha entre la norma ISO 31000 y Magerit. Donde Magerit continuando con la terminología de la normativa ISO 31000, responde a lo que se denomina "Proceso de Gestión de Riesgos" es decir implementa el proceso de Gestión de Riesgos dentro de un marco de trabajo para que los órganos de gobierno tomen decisiones teniendo en cuenta los riesgos derivados del uso de tecnologías de la información

Ilustración 10: ISO 31000 – Metodología de trabajo para la gestión de riesgos



Hablar de gestión de riesgos abarca dos puntos importantes donde se debe analizar los riesgos y luego tratados como lo está establecido en la metodología de Magerit.

Ilustración 11: Gestión de riesgo



Método de análisis de Riesgos definida por MAGERIT:

- Objetivos de Magerit
  - Que los responsables de las organizaciones reconozcan la existencia de riesgos de la información y la necesidad de gestionarlos.
  - Ofrecer un método sistemático para analizar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).
  - Ayudar a descubrir y planificar el tratamiento oportuno para mantener los riesgos bajo control indirectos.
  - Preparar a la organización para procesos de evaluación, auditoría, certificación o Acreditación, según corresponda en cada caso.

El análisis de riesgos proporciona un modelo de sistemas en términos de activos, amenazas y salvaguardas, y esa es la piedra angular para controlar todas las actividades con fundamento.
La Gestión de Riesgos está dividida en 2 tareas representativas ***Análisis de Riesgos*** el cual permite determinar qué tiene la organización y que podría pasar *y* ***Tratamiento de Riesgos*** permite garantizar la defensa para atajar las emergencias, sobrevivir a los incidentes y seguir operando en las mejores condiciones; como nada es perfecto, se dice que el riesgo se reduce a un nivel residual que la dirección asume[10].

- El análisis de riesgos considera los siguientes elementos:

- Activos, que son los elementos del sistema de información (o estrechamente relacionados con este) que soportan la misión de la Organización

[10] (Direción General de Modernización Administrativa, Octubre de 2012)

- Amenazas, que son cosas que les pueden pasar a los activos causando un perjuicio a la Organización
- Salvaguardas (o contra medidas), que son medidas de protección desplegadas para que aquellas amenazas no causen [tanto] daño.

Con estos elementos se puede estimar:

- El impacto: lo que podría pasar
- El riesgo: lo que probablemente pase

El análisis de riesgos permite analizar estos elementos de forma metódica para llegar a conclusiones con fundamento y proceder a la fase de tratamiento.

Informalmente, se puede decir que la gestión de la seguridad de un sistema de información es la gestión de sus riesgos y que el análisis permite racionalizar dicha gestión[11].

[11] (Direción General de Modernización Administrativa pág. 127)

Paso 1: Activos: La información y los servicios prestados son los activos esenciales pero estos activos dependen de otros activos más prosaicos.
Figura 1: Activos definidos por Magerit ordenados según su dependencia

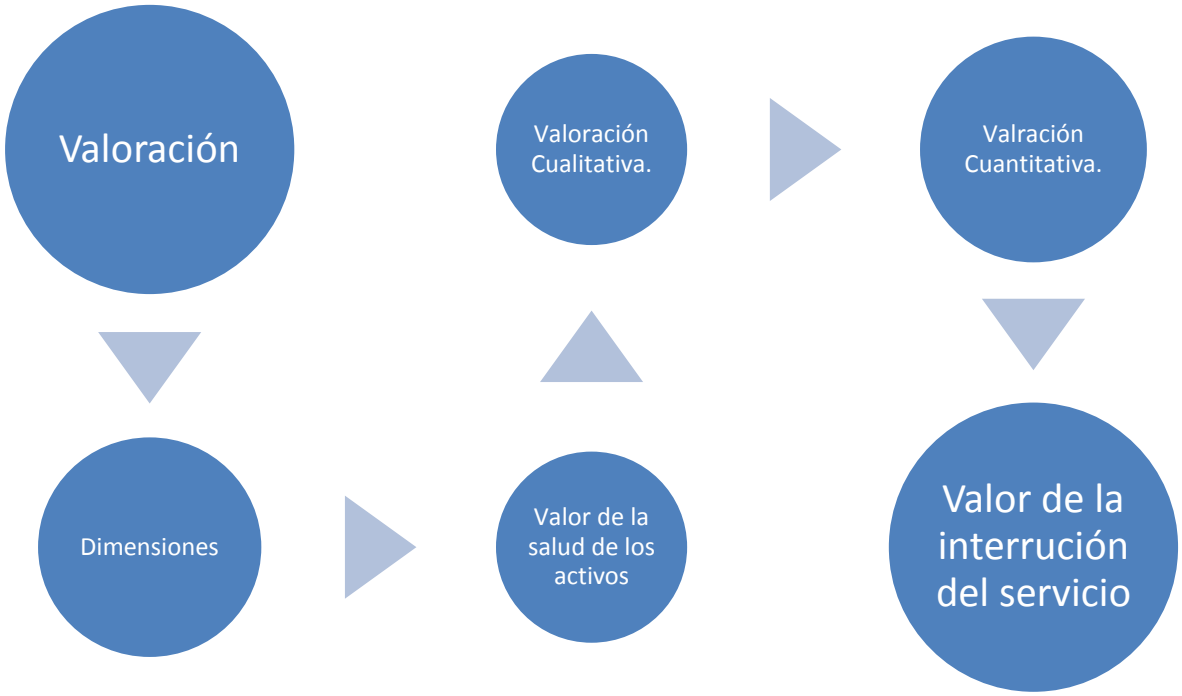
Fuente: Magerit, adaptación del autor

Tabla 14: Clasificación de Activos

Tipo de Activos:	*1. X*	*2.*	*3.*	*4.*	*5.*	*6.*	*7.*
Muestra del Activo	Datos clasificados						
Descripción del Activo	Dícese de aquellos que son esenciales para la supervivencia de la Organización; es decir que su carencia o daño afectaría directamente a la existencia de la Organización. Se pueden identificar aquellos que son imprescindibles para que la Organización supere una situación de emergencia, aquellos que permiten desempeñar o reconstruir las misiones críticas, aquellos sustancian la naturaleza legal o los derechos financieros de la Organización o sus usuarios.						

Fuente: Magerit, adaptación del autor

Figura 2: Criterios de Valoración



Fuente: Magerit, Adaptación de autor

- **Dimensiones**

- Su confidencialidad (C) : ¿Qué daño causaría que lo conociera quien no debe?
- Su integridad (I): ¿Qué perjuicio causaría que estuviera dañado o corrupto?
- Su disponibilidad (D) : ¿qué perjuicio causaría no tenerlo o no poder utilizarlo?
- La Autenticidad(A): ¿Qué prejuicio causaría no saber exactamente quien hace o ha hecho cada cosa?
- La trazabilidad del uso del servicio (T) : ¿Qué daño causaría no saber a quién se le presenta tal servicio? O sea ¿quién hace qué y cuándo?

- **Valoración de la salud de los activos**

Una vez determinadas qué dimensiones (de seguridad) interesan de un activo hay que proceder a valorarlo. La valoración es la determinación del coste que supondría recuperarse de una incidencia que destrozara el activo. Hay muchos factores a considerar:

- Coste de reposición: adquisición e instalación
- Coste de mano de obra (especializada) invertida en recuperar (el valor) del activo
- Lucro cesante: pérdida de ingresos

- Capacidad de operar: confianza de los usuarios y proveedores que se traduce en una pérdida de actividad o en peores condiciones económicas
- Sanciones por incumplimiento de la ley u obligaciones contractuales
- Daño a otros activos, propios o ajenos
- Daño a personas
- Daños medioambientales

La valoración puede ser cuantitativa (con una cantidad numérica) o cualitativa (en alguna escala de niveles). Los criterios más importantes a respetar son:

- La **homogeneidad**: es importante poder comparar valores aunque sean de diferentes dimensiones a fin de poder combinar valores propios y valores acumulados, así como poder determinar si es más grave el daño en una dimensión o en otra
- La **relatividad**: es importante poder relativizar el valor de un activo en comparación con otros activos

Valoración Cuantitativa

Las escalas cualitativas permiten avanzar con rapidez, posicionando el valor de cada activo en un orden relativo respecto de los demás. Es frecuente plantear estas escalas como "órdenes de magnitud" y, en consecuencia, derivar estimaciones del orden de magnitud del riesgo.

La limitación de las valoraciones cualitativas es que no permiten comparar valores más allá de su orden relativo. No se pueden sumar valores.

Valoración Cuantitativa

Las valoraciones numéricas absolutas cuestan mucho esfuerzo; pero permiten sumar valores numéricos de forma absolutamente "natural". La interpretación de las sumas no es nunca motivo de controversia.

Si la valoración es dineraria, además se pueden hacer estudios económicos comparando lo que se arriesga con lo que cuesta la solución respondiendo a las preguntas:

¿Vale la pena invertir tanto dinero en esta salvaguarda?

¿Qué conjunto de salvaguardas optimizan la inversión?

¿En qué plazo de tiempo se recupera la inversión?

¿Cuánto es razonable que cueste la prima de un seguro?

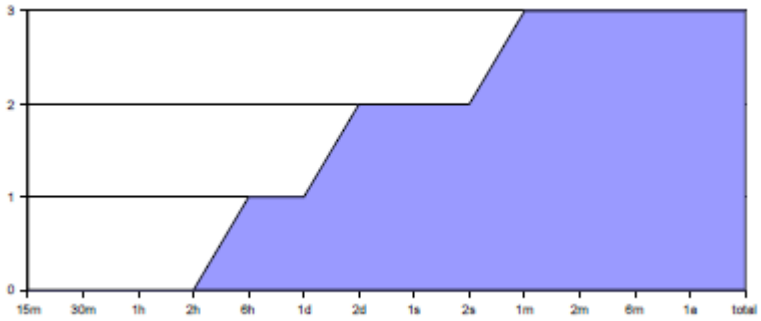
Valoración de la Interrupción del Servicio

Casi todas las dimensiones mencionadas anteriormente permiten una valoración simple, cualitativa o cuantitativa. Pero hay una excepción, la disponibilidad.

No es lo mismo interrumpir un servicio una hora o un día o un mes. Puede que una hora de detención sea irrelevante, mientras que un día sin servicio causa un daño moderado; pero un mes detenido suponga la terminación de la actividad. Y lo malo es que no existe proporcionalidad entre el tiempo de interrupción y las consecuencias.

En consecuencia, para valorar la [interrupción de la] disponibilidad de un activo hay que usar una estructura más compleja que se puede resumir en algún gráfico como el siguiente:

Figura 3: Coste de la interrupción de la disponibilidad



Fuente: Magerit

Figura 4: Escala estándar de valoración, Magerit

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

5	5.pi1	probablemente afecte gravemente a un individuo
	5.pi2	probablemente quebrante seriamente leyes o regulaciones
4	4.pi1	probablemente afecte a un grupo de individuos
	4.pi2	probablemente quebrante leyes o regulaciones
3	3.pi1	probablemente afecte a un individuo
	3.pi2	probablemente suponga el incumplimiento de una ley o regulación
2	2.pi1	pudiera causar molestias a un individuo
	2.pi2	pudiera quebrantar de forma leve leyes o regulaciones
1	1.pi1	pudiera causar molestias a un individuo

[lpo] Obligaciones legales		
9	9.lro	probablemente cause un incumplimiento excepcionalmente grave de una ley o regulación
7	7.lro	probablemente cause un incumplimiento grave de una ley o regulación
5	5.lro	probablemente sea causa de incumplimiento de una ley o regulación
3	3.lro	probablemente sea causa de incumplimiento leve o técnico de una ley o regulación
1	1.lro	pudiera causar el incumplimiento leve o técnico de una ley o regulación

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

[cei] Intereses comerciales o económicos		
9	9.cei.a	de enorme interés para la competencia
	9.cei.b	de muy elevado valor comercial
	9.cei.c	causa de pérdidas económicas excepcionalmente elevadas
	9.cei.d	causa de muy significativas ganancias o ventajas para individuos u organizaciones
	9.cei.e	constituye un incumplimiento excepcionalmente grave de las obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
7	7.cei.a	de alto interés para la competencia
	7.cei.b	de elevado valor comercial
	7.cei.c	causa de graves pérdidas económicas
	7.cei.d	proporciona ganancias o ventajas desmedidas a individuos u organizaciones
	7.cei.e	constituye un serio incumplimiento de obligaciones contractuales relativas a la seguridad de la información proporcionada por terceros
3	3.cei.a	de cierto interés para la competencia
	3.cei.b	de cierto valor comercial
	3.cei.c	causa de pérdidas financieras o merma de ingresos
	3.cei.d	facilita ventajas desproporcionadas a individuos u organizaciones
	3.cei.e	constituye un incumplimiento leve de obligaciones contractuales para mantener la seguridad de la información proporcionada por terceros
2	2.cei.a	de bajo interés para la competencia
	2.cei.b	de bajo valor comercial
1	1.cei.a	de pequeño interés para la competencia
	1.cei.b	de pequeño valor comercial
0	0.3	supondría pérdidas económicas mínimas

[da] Interrupción del servicio		
9	9.da	Probablemente cause una interrupción excepcionalmente seria de las actividades propias de la Organización con un serio impacto en otras organizaciones
	9.da2	Probablemente tenga un serio impacto en otras organizaciones
7	7.da	Probablemente cause una interrupción seria de las actividades propias de la Organización con un impacto significativo en otras organizaciones
	7.da2	Probablemente tenga un gran impacto en otras organizaciones
5	5.da	Probablemente cause la interrupción de actividades propias de la Organización con impacto en otras organizaciones
	5.da2	Probablemente cause un cierto impacto en otras organizaciones
3	3.da	Probablemente cause la interrupción de actividades propias de la Organización
1	1.da	Pudiera causar la interrupción de actividades propias de la Organización

[po] Orden público		
9	9.po	alteración seria del orden público
6	6.po	probablemente cause manifestaciones, o presiones significativas
3	3.po	causa de protestas puntuales
1	1.po	pudiera causar protestas puntuales

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

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

[lg] Pérdida de confianza (reputación)		
9	9.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con otras organizaciones
	9.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar de forma excepcionalmente grave a las relaciones a las relaciones con el público en general
7	7.lg.a	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con otras organizaciones
	7.lg.b	Probablemente causaría una publicidad negativa generalizada por afectar gravemente a las relaciones con el público en general
5	5.lg.a	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con otras organizaciones
	5.lg.b	Probablemente sea causa una cierta publicidad negativa por afectar negativamente a las relaciones con el público
3	3.lg	Probablemente afecte negativamente a las relaciones internas de la Organización
2	2.lg	Probablemente cause una pérdida menor de la confianza dentro de la Organización
1	1.lg	Pudiera causar una pérdida menor de la confianza dentro de la Organización
0	0.4	no supondría daño a la reputación o buena imagen de las personas u organizaciones

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

[rto] Tiempo de recuperación del servicio		
7	7.rto	RTO < 4 horas
4	4.rto	4 horas < RTO < 1 día
1	1.rto	1 día < RTO < 5 días
0	0.rto	5 días < RTO

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

Pasó 2: Amenazas:

Causa potencial de un incidente que puede causar daños a un sistema de información o a una organización. [UNE 71504:2008]
Identificación de Amenazas

Figura 5: Tipo de amenazas

Fuente: Magerit, Adaptación de autor

- **De origen natural** Hay accidentes naturales (terremotos, inundaciones, ...). Ante esos avatares el sistema de información es víctima pasiva, pero de todas formas tendremos en cuenta lo que puede suceder.
- **Del entorno (de origen industrial)** Hay desastres industriales (contaminación, fallos eléctricos, ...) ante los cuales el sis-tema de información es víctima pasiva; pero no por ser pasivos hay que permanecer indefensos.
- **Defectos de las aplicaciones** Hay problemas que nacen directamente en el equipamiento propio por defectos en su diseño o en su implementación, con consecuencias potencialmente negativas sobre el sistema. Frecuentemente se denominan vulnerabilidades técnicas o, simplemente, 'vulnerabilidades'13.
- **Causadas por las personas de forma accidental** Las personas con acceso al sistema de información pueden ser causa de problemas no intencionados, típicamente por error o por omisión.

- **Causadas por las personas de forma deliberada** Las personas con acceso al sistema de información pueden ser causa de problemas intencionados: ataques deliberados; bien con ánimo de beneficiarse indebidamente, bien con ánimo de causar daños y perjuicios a los legítimos propietarios.

No todas las amenazas afectan a todos los activos, sino que hay una cierta relación entre el tipo de activo y lo que le podría ocurrir.

➢ **Valoración de Amenazas**

- **Degradación:** Cuan perjudicado resultaría el valor del activo
- **Probabilidad:** Cuán probable o improbable es que se materialice la amenaza

Figura 6: Degradación del Valor

MA	muy alta	casi seguro	fácil
A	alta	muy alto	medio
M	media	posible	difícil
B	baja	poco probable	muy difícil
MB	muy baja	muy raro	extremadamente difícil

Figura 7: Probabilidad de Ocurrencia

MA	100	muy frecuente	a diario
A	10	frecuente	mensualmente
M	1	normal	una vez al año
B	1/10	poco frecuente	cada varios años
MB	1/100	muy poco frecuente	siglos

➢ **Determinación del impacto potencial**

Se denomina impacto a la medida del daño sobre el activo derivado de la materialización de una amenaza. Conociendo el valor de los activos (en varias dimensiones) y la degradación que causan las amenazas, es directo derivar el impacto que estas tendrían sobre el sistema.

La única consideración que queda hacer es relativa a las dependencias entre activos. Es frecuente que el valor del sistema se centre en la información que maneja y los servicios que presta; pero las amenazas suelen materializarse en los medios. Para enlazar unos con otros recurriremos al grafo de dependencias.

Impacto Acumulado

Es el calculado sobre un activo teniendo en cuenta:

- Su valor acumulado (el propio mas el acumulado de los activos que dependen de él).
- Las amenazas a que está expuesto.

El impacto acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado y de la degradación causada.

El impacto es tanto mayor cuanto mayor es el valor propio o acumulado sobre un activo.

El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado.

El impacto acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc.

Impacto repercutido

Es el calculado sobre un activo teniendo en cuenta

- Su valor propio
- Las amenazas a que están expuestos los activos de los que depende

El impacto repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio y de la degradación causada.

El impacto es tanto mayor cuanto mayor es el valor propio de un activo.

El impacto es tanto mayor cuanto mayor sea la degradación del activo atacado.

El impacto es tanto mayor cuanto mayor sea la dependencia del activo atacado.

El impacto repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

Agregación de valores de impacto

Los párrafos anteriores determinan el impacto que sobre un activo tendría una amenaza en una cierta dimensión. Estos impactos singulares pueden agregarse bajo ciertas condiciones:

- Puede agregarse el impacto repercutido sobre diferentes activos,
- Puede agregarse el impacto acumulado sobre activos que no sean dependientes entre sí, y no hereden valor de un activo superior común,
- No debe agregarse el impacto acumulado sobre activos que no sean independientes, pues ello supondría sobre ponderar el impacto al incluir varias veces el valor acumulado de activos superiores,

- Puede agregarse el impacto de diferentes amenazas sobre un mismo activo, aunque con-viene considerar en qué medida las diferentes amenazas son independientes y pueden ser concurrentes,
- Puede agregarse el impacto de una amenaza en diferentes dimensiones.

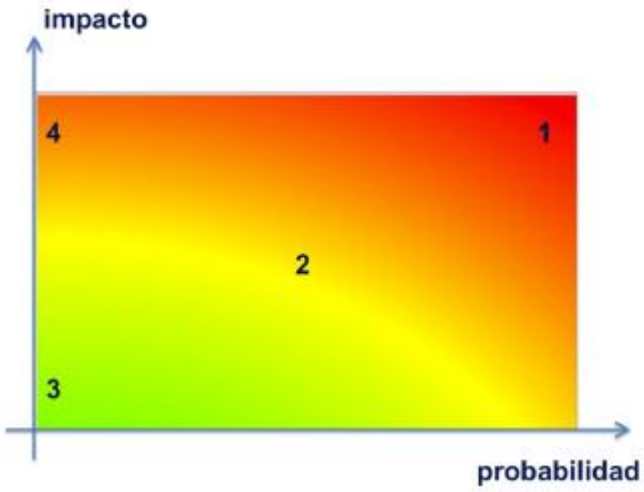
➢ **Determinación del riesgo Potencial**

Se denomina riesgo a la medida del daño probable sobre un sistema. Conociendo el impacto de las amenazas sobre los activos, es directo derivar el riesgo sin más que tener en cuenta la probabilidad de ocurrencia.

El riesgo crece con el impacto y con la probabilidad, pudiendo distinguirse una serie de zonas a tener en cuenta en el tratamiento del riesgo.

- zona 1 – riesgos muy probables y de muy alto impacto
- zona 2 – franja amarilla: cubre un amplio rango desde situaciones improbables y de impacto medio, hasta situaciones muy probables pero de impacto bajo o muy bajo
- zona 3 – riesgos improbables y de bajo impacto.
- zona 4 – riesgos improbables pero de muy alto impacto

Figura 8: El riesgo en Función del impacto y probabilidad



Riesgo acumulado Es el calculado sobre un activo teniendo en cuenta

- el impacto acumulado sobre un activo debido a una amenaza y
- la probabilidad de la amenaza

El riesgo acumulado se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor acumulado, la degradación causada y la probabilidad de la amenaza.
El riesgo acumulado, al calcularse sobre los activos que soportan el peso del sistema de información, permite determinar las salvaguardas de que hay que dotar a los medios de trabajo: protección de los equipos, copias de respaldo, etc.

Riesgo repercutido Es el calculado sobre un activo teniendo en cuenta

- el impacto repercutido sobre un activo debido a una amenaza y
- la probabilidad de la amenaza

El riesgo repercutido se calcula para cada activo, por cada amenaza y en cada dimensión de valoración, siendo una función del valor propio, la degradación causada y la probabilidad de la amenaza.
El riesgo repercutido, al calcularse sobre los activos que tienen valor propio, permite determinar las consecuencias de las incidencias técnicas sobre la misión del sistema de información. Es pues una presentación gerencial que ayuda a tomar una de las decisiones críticas de un análisis de riesgos: aceptar un cierto nivel de riesgo.

Agregación de riesgos Los párrafos anteriores determinan el riesgo que sobre un activo tendría una amenaza en una cierta dimensión. Estos riesgos singulares pueden agregarse bajo ciertas condiciones:

- Puede agregarse el riesgo repercutido sobre diferentes activos,
- Puede agregarse el impacto acumulado sobre activos que no sean dependientes entre sí, y no hereden valor de un activo superior común,
- No debe agregarse el riesgo acumulado sobre activos que no sean independientes, pues ello supondría sobre ponderar el riesgo al incluir varias veces el valor acumulado de activos superiores,
- Puede agregarse el riesgo de diferentes amenazas sobre un mismo activo, aunque conviene considerar en qué medida las diferentes amenazas son independientes y pueden ser concurrentes,
- Puede agregarse el riesgo de una amenaza en diferentes dimensiones.

Figura 9: Formato de presentación de Resultados

[código] descripción sucinta de lo que puede pasar	
Tipos de activos: • que se pueden ver afectados por este tipo de amenazas	**Dimensiones:** 1. de seguridad que se pueden ver afectadas por este tipo de amenaza, ordenadas de más a menos relevante
Descripción: complementaria o más detallada de la amenaza: lo que le puede ocurrir a activos del tipo indicado con las consecuencias indicadas	

Paso 3: Salvaguardas

- **Selección de Salvaguardas**: Se toman los salvaguardas relevantes
  - Tipo de activos a proteger, pues cada tipo se protege de una forma específica
  - Dimensión o dimensiones de seguridad que requieren protección
  - Amenazas de las que necesitamos protegernos
  - Si existen salvaguardas alternativas

Es prudente establecer un principio de proporcionalidad y tener en cuenta:

- El mayor o menor valor propio o acumulado sobre un activo, centrándonos en lo más valioso y obviando lo irrelevante.
- La mayor o menor probabilidad de que una amenaza ocurra, centrándonos en los riesgos más importantes (ver zonas de riesgo) .
- La cobertura del riesgo que proporcionan salvaguardas alternativas

Esto lleva a dos tipos de declaraciones para excluir una cierta salvaguarda del conjunto de las que conviene analizar:

- **No aplica** – se dice cuando una salvaguarda no es de aplicación porque técnicamente no es adecuada al tipo de activos a proteger, no protege la dimensión necesaria o no protege frente a la amenaza en consideración
- **No se justifica** – se dice cuando la salvaguarda aplica, pero es desproporcionada al riesgo que tenemos que proteger.

Como resultado de estas consideraciones dispondremos de una **"declaración de aplicabilidad"** o relación de salvaguardas que deben ser analizadas como componentes nuestro sistema de protección.

- **Efectos de las salvaguardas**

  Las salvaguardas entran en el cálculo del riesgo de dos formas:

  Reduciendo la probabilidad de las amenazas. Se llaman salvaguardas preventivas. Las ideales llegan a impedir completamente que la amenaza se materialice.

  ***Limitando el daño causado*.** Hay salvaguardas que directamente limitan la posible degradación, mientras que otras permiten detectar inmediatamente el ataque para frenar que la degradación avance. Incluso algunas salvaguardas se limitan a permitir la pronta recuperación del sistema cuando la amenaza lo destruye. En cualquiera de las versiones, la amenaza se materializa; pero las con-secuencias se limitan.

- **Tipos de Salvaguardas**

  Esta aproximación a veces resulta un poco simplificadora, pues es habitual hablar de diferentes tipos de protección prestados por las salvaguardas:

  - **[PR] prevención** Diremos que una salvaguarda es preventiva cuando reduce las oportunidades de que un incidente ocurra. Si la salvaguarda falla y el incidente llega

a ocurrir, los daños son los mismos. Ejemplos: autorización previa de los usuarios, gestión de privilegios, planificación de capa-cidades, metodología segura de desarrollo de software, pruebas en pre-producción, segre-gación de tareas, ...

- **[DR] disuasión** Diremos que una salvaguarda es disuasoria cuando tiene un efecto tal sobre los atacantes que estos no se atreven o se lo piensan dos veces antes de atacar. Son salvaguardas que actúan antes del incidente, reduciendo las probabilidades de que ocurra; pero que no tie-nen influencia sobre los daños causados caso de que el atacante realmente se atreva. Ejemplos: vallas elevadas, guardias de seguridad, avisos sobre la persecución del delito o persecución del delincuente, ...
- **[EL] eliminación** Diremos que una salvaguarda elimina un incidente cuando impide que éste tenga lugar. Son salvaguardas que actúan antes de que el incidente se haya producido. No reducen los daños caso de que la salvaguarda no sea perfecta y el incidente llegue a ocurrir.

  Ejemplos: eliminación de cuentas estándar, de cuentas sin contraseña, de servicios inne-cesarios, …; en general, todo lo que tenga que ver con la fortificación o bastionado, ..., ci-frado de la información, ..., armarios ignífugos, ...

- **[IM] minimización del impacto / limitación del impacto** Se dice que una salvaguarda minimiza o limita el impacto cuando acota las consecuencias de un incidente.

  Ejemplos: desconexión de redes o equipos en caso de ataque, detención de servicios en caso de ataque, seguros de cobertura, cumplimiento de la legislación vigente

- **[CR] corrección** Diremos que una salvaguarda es correctiva cuando, habiéndose producido un daño, lo re-para. Son salvaguardas que actúan después de que el incidente se haya producido y por tanto reducen los daños.

  Ejemplos: gestión de incidentes, líneas de comunicación alternativas, fuentes de alimentación redundantes, ...

- **[RC] recuperación** Diremos que una salvaguarda ofrece recuperación cuando permite regresar al estado anterior al incidente. Son salvaguardas que no reducen las probabilidades del incidente, pero acotan los daños a un periodo de tiempo.

- **[MN] monitorización** Son las salvaguardas que trabajan monitorizando lo que está ocurriendo o lo que ha ocurrido. Si se detectan cosas en tiempo real, podemos reaccionar atajando el incidente para limitar el impacto; si se detectan cosas a posteriori, podemos aprender del incidente y me-jorar el sistema de salvaguardas de cara al futuro.

- **[DC] detección** Diremos que una salvaguarda funciona detectando un ataque cuando informa de que el ataque está ocurriendo. Aunque no impide el ataque, sí permite que entren en operación otras medidas que atajen la progresión del ataque, minimizando daños.

  Ejemplos: anti-virus, IDS, detectores de incendio, ...

- **[AW] concienciación** Son las actividades de formación de las personas anexas al sistema que pueden tener una influencia sobre él. La formación reduce los errores de los usuarios, lo cual tiene un efecto preventivo. También mejora las salvaguardas de todo tipo pues los que las operan lo hacen con eficacia y rapidez, potenciando su efecto o, al menos, no menoscabándolo por una mala operación.

  Ejemplos: cursos de concienciación, cursos de formación.

- **[AD] administración** Se refiere a las salvaguardas relacionadas con los componentes de seguridad del sistema. Una buena administración evita el desconocimiento de lo que hay y por tanto impide que hayan puertas desconocidas por las que pudiera tener éxito un ataque. En general pueden considerarse medidas de tipo preventivo.

  Ejemplos: inventario de activos, análisis de riesgos, plan de continuidad, ...

Figura 10: Tipo de Salvaguardas, Magerit

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

- **Eficacia de la protección**

Las salvaguardas se caracterizan, además de por su existencia, por su eficacia frente al riesgo que pretenden conjurar. La salvaguarda ideal es 100% eficaz, eficacia que combina 2 factores:

Desde el punto de vista técnico

- Es técnicamente idónea para enfrentarse al riesgo que protege
- Se emplea siempre

Desde el punto de vista de operación de la salvaguarda

- Está perfectamente desplegada, configurada y mantenida
- Existen procedimientos claros de uso normal y en caso de incidencias
- Los usuarios están formados y concienciados
- Existen controles que avisan de posibles fallos

Entre una eficacia del 0% para aquellas que faltan y el 100% para aquellas que son idóneas y que están perfectamente implantadas, se estimará un grado de eficacia real en cada caso concreto. Para medir los aspectos organizativos, se puede emplear una escala de madurez que recoja en forma de factor corrector la confianza que merece el proceso de gestión de la salvaguarda:

Figura 11: Eficacia y madurez de los salvaguardas, Magerit

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

Figura 12: Catalogo de Salvaguardas Magerit M2

Protecciones generales u horizontales
H Protecciones Generales
H.IA Identificación y autenticación
H.AC Control de acceso lógico
H.ST Segregación de tareas
H.IR Gestión de incidencias
H.tools Herramientas de seguridad
H.tools.AV Herramienta contra código dañino
H.tools.IDS IDS/IPS: Herramienta de detección / prevención de intrusión
H.tools.CC Herramienta de chequeo de configuración
H.tools.VA Herramienta de análisis de vulnerabilidades
H.tools.TM Herramienta de monitorización de tráfico
H.tools.DLP DLP: Herramienta de monitorización de contenidos
H.tools.LA Herramienta para análisis de logs
H.tools.HP Honey net / honey pot
H.tools.SFV Verificación de las funciones de seguridad
H.VM Gestión de vulnerabilidades

H.AU Registro y auditoría

Protección de los datos / información
D Protección de la Información
D.A Copias de seguridad de los datos (backup)
D.I Aseguramiento de la integridad
D.C Cifrado de la información
D.DS Uso de firmas electrónicas
D.TS Uso de servicios de fechado electrónico (time stamping)

Protección de las claves criptográficas
K Gestión de claves criptográficas
K.IC Gestión de claves de cifra de información
K.DS Gestión de claves de firma de información
K.disk Gestión de claves para contenedores criptográficos
K.comms Gestión de claves de comunicaciones
K.509 Gestión de certificados

Protección de los servicios
S Protección de los Servicios
S.A Aseguramiento de la disponibilidad
S.start Aceptación y puesta en operación
S.SC Se aplican perfiles de seguridad
S.op Explotación
S.CM Gestión de cambios (mejoras y sustituciones)
S.end Terminación
S.www Protección de servicios y aplicaciones web
S.email Protección del correo electrónico
S.dir Protección del directorio
S.dns Protección del servidor de nombres de dominio (DNS)
S.TW Teletrabajo
S.voip Voz sobre IP

Protección de las aplicaciones (software)
SW Protección de las Aplicaciones Informáticas
SW.A Copias de seguridad (backup)
SW.start Puesta en producción
SW.SC Se aplican perfiles de seguridad

SW.op Explotación / Producción
SW.CM Cambios (actualizaciones y mantenimiento)
SW.end Terminación

Protección de los equipos (hardware)
HW Protección de los Equipos Informáticos
HW.start Puesta en producción
HW.SC Se aplican perfiles de seguridad
HW.A Aseguramiento de la disponibilidad
HW.op Operación
HW.CM Cambios (actualizaciones y mantenimiento)
HW.end Terminación
HW.PCD Informática móvil
HW.print Reproducción de documentos
HW.pabx Protección de la centralita telefónica (PABX)

Protección de las comunicaciones
COM Protección de las Comunicaciones
COM.start Entrada en servicio
COM.SC Se aplican perfiles de seguridad
COM.A Aseguramiento de la disponibilidad
COM.aut Autenticación del canal
COM.I Protección de la integridad de los datos intercambiados
COM.C Protección criptográfica de la confidencialidad de los datos intercambiados
COM.op Operación
COM.CM Cambios (actualizaciones y mantenimiento)
COM.end Terminación
COM.internet Internet: uso de ? acceso a
COM.wifi Seguridad Wireless (WiFi)
COM.mobile Telefonía móvil
COM.DS Segregación de las redes en dominios

Protección de las comunicaciones
COM Protección de las Comunicaciones
COM.start Entrada en servicio
COM.SC Se aplican perfiles de seguridad
COM.A Aseguramiento de la disponibilidad
COM.aut Autenticación del canal

COM.I Protección de la integridad de los datos intercambiados
COM.C Protección criptográfica de la confidencialidad de los datos intercambiados
COM.op Operación
COM.CM Cambios (actualizaciones y mantenimiento)
COM.end Terminación
COM.internet Internet: uso de ? acceso a
COM.wifi Seguridad Wireless
(WiFi) COM.mobile Telefonía móvil
COM.DS Segregación de las redes en dominios

Protección en los puntos de interconexión con otros sistemas
IP Puntos de interconexión: conexiones entre zonas de confianza
IP.SPP Sistema de protección perimetral
IP.BS Protección de los equipos de frontera

Protección de los soportes de información
MP Protección de los Soportes de Información
MP.A Aseguramiento de la disponibilidad
MP.IC Protección criptográfica del contenido
MP.clean Limpieza de contenidos
MP.end Destrucción de soportes

Protección de los elementos auxiliares
AUX Elementos Auxiliares
AUX.A Aseguramiento de la disponibilidad
AUX.start Instalación
AUX.power Suministro eléctrico
AUX.AC Climatización
AUX.wires Protección del cableado

Seguridad física – Protección de las instalaciones
L Protección de las Instalaciones
L.design Diseño
L.depth Defensa en profundidad
L.AC Control de los accesos físicos
L.A Aseguramiento de la disponibilidad
L.end Terminación

Salvaguardas relativas al personal: Son aquellas que se refieren a las personas que tienen relación con el sistema de información.
PS Gestión del Personal PS.AT Formación y concienciación PS.A Aseguramiento de la disponibilidad

Salvaguardas de tipo organizativo: Son aquellas que se refieren al buen gobierno de la seguridad.
G Organización G.RM Gestión de riesgos G.plan Planificación de la seguridad G.exam Inspecciones de seguridad

Continuidad de operaciones: Prevención y reacción frente a desastres.
BC Continuidad del negocio BC.BIA Análisis de impacto (BIA) BC.DRP Plan de Recuperación de Desastres (DRP)

Adquisición y desarrollo
NEW Adquisición / desarrollo NEW.S Servicios: Adquisición o desarrollo NEW.SW Aplicaciones: Adquisición o desarrollo NEW.HW Equipos: Adquisición o desarrollo NEW.COM Comunicaciones: Adquisición o contratación NEW.MP Soportes de Información: Adquisición NEW.C Productos certificados o acreditados

4.2.2 Pasó 5: Vulnerabilidades:

Se denomina vulnerabilidad a toda debilidad que puede ser aprovechada por una amenaza, o más detalladamente a las debilidades de los activos o de sus medidas de protección que facilitan el éxito de una amenaza potencial.

Traducido a los términos empleados en los párrafos anteriores, son vulnerabilidades todas las ausencias o ineficacias de las salvaguardas pertinentes para salvaguardar el valor propio o acumulado sobre un activo. A veces se emplea el término “insuficiencia” para resaltar el hecho de que la eficacia medida de la salvaguarda es insuficiente para preservar el valor del activo expuesto a una amenaza.

4.2.3 Paso 6: impacto residual

Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de posible impacto que se denomina residual. Se dice que hemos modificado el impacto, desde un valor potencial a un valor residual.

El cálculo del impacto residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación, se repiten los cálculos de impacto con este nuevo nivel de degradación.

La magnitud de la degradación tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

El impacto residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

4.2.4 Paso 7: riesgo residual

Dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de riesgo que se denomina residual. Se dice que hemos modificado el riesgo, desde un valor potencial a un valor residual.

El cálculo del riesgo residual es sencillo. Como no han cambiado los activos, ni sus dependencias, sino solamente la magnitud de la degradación y la probabilidad de las amenazas, se repiten los cálculos de riesgo usando el impacto residual y la probabilidad residual de ocurrencia.

La magnitud de la degradación se toma en consideración en el cálculo del impacto residual.

La magnitud de la probabilidad residual tomando en cuenta la eficacia de las salvaguardas, es la proporción que resta entre la eficacia perfecta y la eficacia real.

El riesgo residual puede calcularse acumulado sobre los activos inferiores, o repercutido sobre los activos superiores.

4.2.5 METODOLOGÍA DE ANALISIS DE RIESGOS DE ACUERDO A LA ISO/IEC 31000:

Principios

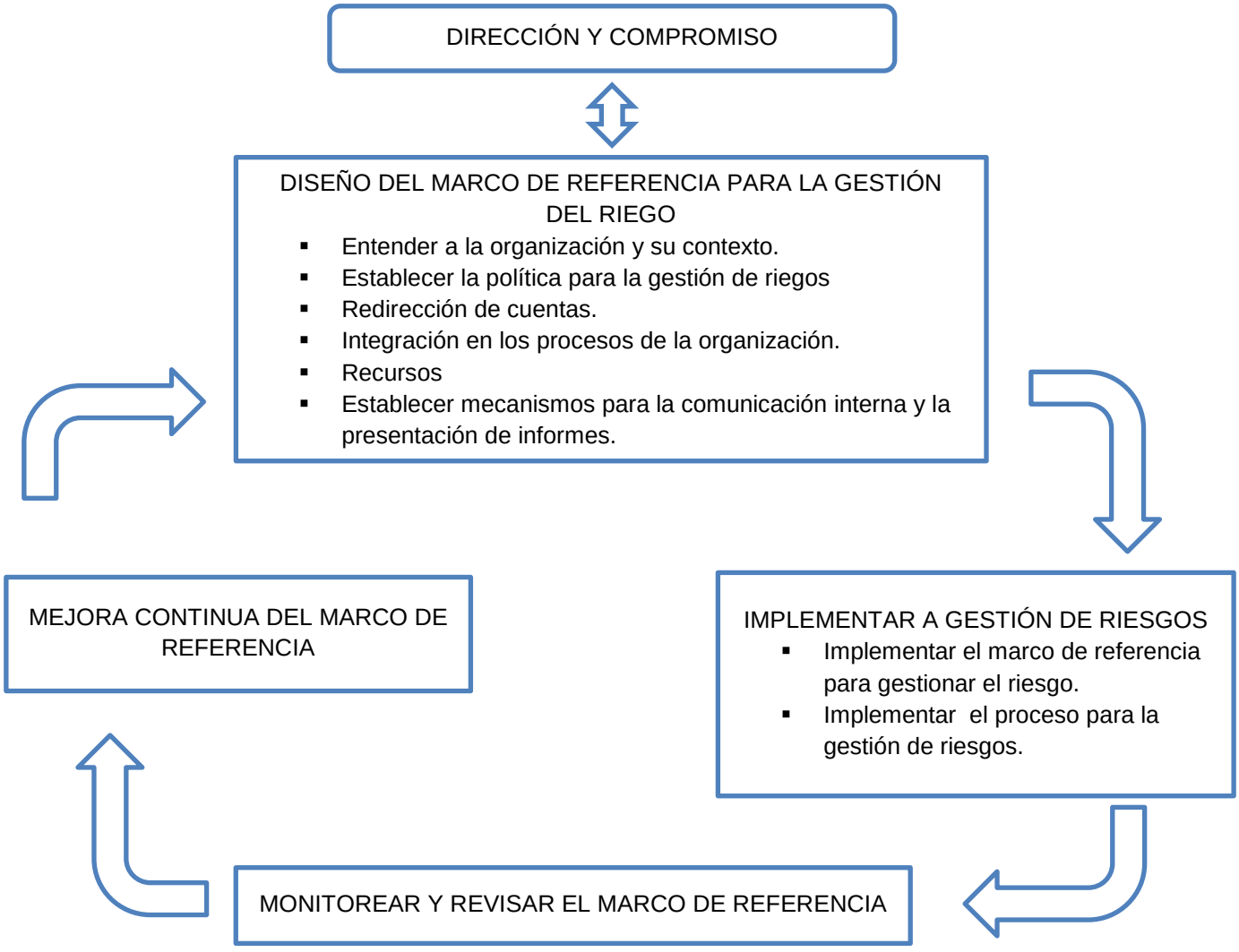
Para que la gestión de riesgos sea eficaz, la organización deberá cumplir con todos los siguientes principios en todos los niveles:

- La gestión del riesgo crea y protege el valor.
- La gestión de riesgos es una parte integral de todos los procesos de la organización.
- La gestión de riesgos es parte de la toma de decisiones.
- La gestión de riesgo aborda explícitamente la incertidumbre.

- La gestión de riesgos es sistemática, estructurada y oportuna.
- La gestión de riesgos se basa en la mejor información disponible.
- La gestión del riesgo está adaptada.
- La gestión del riesgo es transparente e inclusiva.
- La gestión del riesgo es dinámica, reiterativa y receptiva al cambio.
- La gestión del riesgo facilita la mejora continua de la organización.

Marco de Referencia

Figura 13: Relación entre los componentes del marco de referencia para la gestión de riesgos



Proceso:
El proceso para la gestión de riesgos 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.

Figura 14: Proceso para la gestión del riesgo

Fuente: ISO 31000

- **Comunicación y consulta:** Un enfoque de equipo consultor puede:
  - Ayudar a establecer correctamente el contexto.
  - Garantizar que se entienden y se toman en consideración los intereses de las partes involucradas.
  - Ayudar a garantizar que los riesgos estén correctamente identificados.
  - Reunir diferentes áreas de experticia para analizar los riesgos.
  - Garantizar que los diversos puntos de vista se toman en consideración adecuadamente al definir los criterios del riesgo y al evaluar los riesgos.
  - Asegurar la aprobación y el soporte para el plan de tratamiento.
  - Fomentar la gestión adecuada del cambio durante el proceso para la gestión del riesgo y desarrollar un plan adecuado de comunicación y consulta externo e interno.

- **Establecimiento del contexto:** La organización articula sus objetivos, define los parámetros externos e internos que se va a considerar al gestionar el riesgo y establecer el alcance y los criterios del riesgo para el resto del proceso.
  - Establecer el contexto externo

- Establecer el contexto interno.
- Establecer el contexto del proceso para la gestión del riesgo
- Definir los criterios del riesgo.

- **Valoración del riesgo:** La valoración del riesgo es el proceso total de identificación del riesgo, análisis del riesgo y evaluación del riesgo.

- **Tratamiento del riesgo:** El tratamiento del riesgo involucra una o más opciones para modificar los riesgos y la implementación de tales opciones. Una vez implementado, el tratamiento suministra controles o los modifica.

- **Monitoreo y revisión:** Debe ser una parte planificada del proceso para la gestión del riesgo e incluir verificación o vigilancia regular.

El análisis de riesgos considera los siguientes elementos:

- Activos, que son los elementos del sistema de información (o estrechamente relacionados con este) que soportan la misión de la Organización
- Amenazas, que son cosas que les pueden pasar a los activos causando un perjuicio a la Organización
- Salvaguardas (o contra medidas), que son medidas de protección desplegadas para que aquellas amenazas no causen [tanto] daño.

Con estos elementos se puede estimar:

- El impacto: lo que podría pasar
- El riesgo: lo que probablemente pase

El análisis de riesgos permite analizar estos elementos de forma metódica para llegar a conclusiones con fundamento y proceder a la fase de tratamiento.

Informalmente, se puede decir que la gestión de la seguridad de un sistema de información es la gestión de sus riesgos y que el análisis permite racionalizar dicha gestión[12].

4.3 POLÍTICA PARA LA GESTIÓN DE RIESGOS

Introducción

La política para la gestión de riesgos diseñada se enfoca en procesos, actividades y tareas, definidas bajo la normativa de la ISO 31000 para el gobierno corporativo de los riesgos de

[12] (Direción General de Modernización Administrativa pág. 127)

la organización y la metodología Magerit para la gestión de los riesgos de la seguridad de la información, de esta forma se facilita la gestión de los riesgos ocasionados sobre el funcionamiento de la oficina y como le afecta a la organización. Por tal razón La oficina de Admisiones Registro y Control de la UFPSO tiene la responsabilidad de proteger la información garantizando su disponibilidad, integridad y confidencialidad.

Objetivo

Esta política tiene como objetivo identificar los criterios necesarios para el control y la gestión del riego de seguridad de la información en la oficina de admisiones registro y control de la Universidad Francisco de Paula Santander Ocaña.

Alcance

La política de gestión de riesgos de la información para la oficina de admisiones registro y control de la Universidad Francisco de Paula Santander Ocaña abarca todos los activos de la información incluso los físicos.

Principios básicos

- Protección de los activos de la Oficina de admisiones registro y control
- Integración de la gestión de riesgos a los procesos de la oficina de admisiones registro y control.
- Toma de decisiones basada en riesgos, acorde con la mejor información disponible.
- Desarrollo de un esquema que priorice los riesgos y procedimientos de avance continúo.
- Implementación de un enfoque proactivo, orientado a la mejora continua en la administración de riesgos que enfrenta al aseguramiento de que la política de riesgos siga siendo adecuada y pertinente.

Responsabilidad

El comité de subdirección académica junto con el comité de admisiones, registro y control son responsables por:

- Generar las condiciones adecuadas para la ejecución y comunicación de la presente política, así como establecer el alcance para su aplicación.
- Formar un equipo responsable para la gestión del riesgo de la seguridad de la información.

El jefe de la oficina de admisiones, registró y control es responsable de:

- Dar aplicación a la presente política y a la identificación, estimación, valoración y tratamiento de los riesgos identificados.

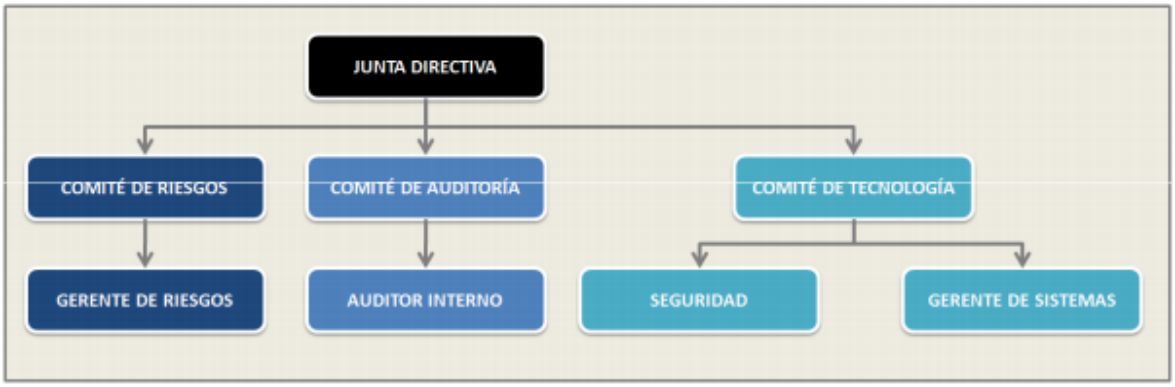
La persona designada responsable de la seguridad de la información es responsable por:

- Brindar asesoría en la identificación de las amenazas que puedan afectar a los activos de información y las vulnerabilidades que propician las mismas.

Las tres partes mencionadas anteriormente, serán responsables por la definición de las acciones de tratamiento de los riesgos de seguridad de la información en la oficina de admisiones registro y control.

Estructura Organizacional

Ilustración 12: Estructura organizacional ISACA



Fuente: ISACA 2013

Junta Directiva: Deben encargarse de aprobar las estrategias e inversiones de tecnología, así como los planes de continuidad de negocio y recuperación ante perdidas.
Comité de riesgos: Desarrolla políticas para su gestión, las cuales deben ser formalmente aprobadas y comunicadas, a través de un manual de gestión de riesgos.
Gerente de riesgos: Analiza, revisa y lleva un registro de los controles que deberá ser implementados para debida administración del riesgo asociado a las iniciativas y recursos de TI.
Comité de tecnología: Desarrollan un plan estratégico de tecnología alineando a los planes estratégicos de la organización.

Auditoría interna: Tiene como responsabilidad la ejecución de auditorías de sistemas de manera regular a través de un plan de trabajo revisado y aprobado por el comité de auditorías.
Gerencia de Sistemas: Pone en ejecución la estrategia de tecnología que permita alinear sus iniciativas e inversiones, así como velar por implementación de los recursos de tecnología y los controles necesarios para mitigar los riesgos de tecnología identificados.
Seguridad de la información: Establece, revisa y actualiza de manera periódica las políticas y procedimientos de seguridad de la información.
Criterios de la política

- Establecer, formalizar y poner en práctica una metodología para la gestión del riesgo.
- Definir y establecer en forma explícita el nivel de aceptación del riesgo por parte de la dirección.
- Contar con la aprobación explicita de los planes de tratamiento del riesgo residual.
- Realizar evaluaciones periódicas de riesgo en seguridad de la información.
- Mantener informadas a las partes involucradas sobre el estado del riesgo

4.3.1 Desarrollo de la política

En el inciso 4.4 y 4.5 se describen las metodologías que de acuerdo al análisis e investigaciones, y con referentes bibliográfico en sus aplicaciones se considera que un hibrido de estas 2 metodologías planteadas en Magerit y la norma ISO/IEC 31000 sería una metodología adecuada para la oficina de admisiones registro y control.

Se plantea que la gestión de riesgos de debe tomar como un proyectos con 3 procesos que incorporan las actividades correspondientes a cada procesos.

Los 3 procesos en los que se desarrolla esta metodología son:

- **Proceso P1** Planificación del proyecto de análisis y gestión de riesgos
- **Proceso P2:** Análisis de riesgos
- **Proceso P3:** Gestión de riesgos

Planificación del proyecto de análisis y gestión de riesgos

Actividad A1.1 Estudio de oportunidad: Los estudios de oportunidad y documentos preventivos estarán conformados por los documentos definidos que sirvan de soporte para

la elaboración del pliego de condiciones de manera que los proponentes puedan valorar adecuadamente el alcance de lo requerido por la entidad, así como el de la distribución de riesgos que la entidad propone.

Tarea T1.1.1 Determinar la oportunidad: Se propone una secuencia de pasos para determinar la oportunidad.

- Listar los recursos disponibles de la oficina.
- Listar las regiones y sectores que proporcionan demanda.

Se debe focalizar en los 3 ítems más relevantes de cada lista, analizarlas y crear una porción de ideas de negocios.

Actividad A1.2 Determinar el alcance: Se propone una secuencia de pasos para determinar el alcance del proyecto del análisis de riesgos se deben tener en cuenta las siguientes definiciones para abarcar en su totalidad los parámetros del proyecto.

- Iniciación del Alcance: Comprometer a la oficina para iniciar las fases del proyecto.
- Planificación del alcance: Desarrollo de un plan escrito del alcance que sirva de base para futuras decisiones a tomar.
- Definición del alcance: Identificar las entregas de los productos en cada fase del proyecto.
- Verificación del alcance: Confirmar que el alcance del proyecto es exacto, completo y cubre todas las fases del proyecto de análisis y gestión de riesgos.
- Control de cambios en el alcance: Asegurar que se dispone de los controles que perite gestionar los cambios del alcance una vez que se ha fijado el alcance del proyecto.

Tarea T1.2.1 Determinar los objetivos y restricciones generales

Se debe formular objetivos que sean medibles en el tiempo para determinar con precisión su cumplimiento, realistas y coherentes teniendo en cuenta que estos deben responder a una necesidad destacada y no deben contradecirse entre sí.

Tarea T1.2.2 Determinación del dominio y límites
Tarea T1.2.3 Identificación del Entorno
El grupo de trabajo debe identificar las cadenas de funciones y las relaciones existentes mediante un mapeo participativo, con el fin de clasificar la información de cada etapa y

actores, reconocer que información se necesita recolectar y como obtenerla, además, de recolectar y analizara datos secundarios sobre procesos alternos.

Tarea T1.2.4 **Estimación de dimensiones y coste.**

Se deben tener

Actividad A1.3 Planificación del proyecto:

Es el proceso de establecer metas y elegir los medios de alcanzarlos, se tienen en cuanta el tiempo, recursos y objetivos para el desarrollo de cada fase del proyecto del análisis y gestión de riesgos.

Tarea T1.3.1 Evaluar cargas y planificar entrevistas:

Para el desarrollo del proyecto de análisis y gestión de riesgos se debe contar con un grupo de trabajo con capacidades específicas para desenvolverse en el rol establecido. Con este objetivo se crea un perfil para cada rol y se diseña la entrevista correspondiente a cada rol, garantizando un grupo de trabajo idóneo.

Se debe estudiar de la oficina tópicos como el personal que trabaja en ella y sus condiciones, la información de la oficina y sus condiciones y finalmente los usuarios finales. Es necesario conocer la opinión de las personas relacionadas con la oficina por ello se diseñan entrevista que nos permitan conocer el criterio de cada una de las partes.

Tarea T1.3.2 Organizar a los participantes

Tarea T1.3.3 Planificar el trabajo

Actividad A1.4: Lanzamiento del proyecto de análisis y gestión de riesgos

En esta actividad es cuando se da inicio al proyecto de análisis y gestión de riesgos, debemos preparar todos los instrumentos y materiales para un buen desarrollo.

Tarea T1.4.1: **Adaptar los cuestionarios**

Tarea T1.4.2: **Criterios de evaluación**

Tarea T1.4.3: **Recursos necesarios**

Tarea T1.4.4: **Sensibilización**

4.3.2 Proceso P2: Análisis de riesgos

Con este proceso entramos en materia a la identificación y valoración de los riesgos de una forma organizada, que su completa aplicación nos garantizara un excelente resultado.

Actividad A2.1: Caracterización de los activos

Para la caracterización de los activos tomamos aspectos del paso 1 definido por magerit la cual nos dice que la información y los servicios prestados son los activos esenciales pero estos activos depende de otros activos más prosaicos.

Tarea T2.1.1: Identificación de los activos

Tarea T2.1.2: Dependencias entre activos

Tarea T2.1.3: Valoración de los activos

Actividad A2.2: Caracterización de las amenazas

Para la caracterización de las amenazas tomamos el paso 2 definido por magerit donde nos indica que la causa potencial de un incidente que puede causar daños a un sistema de información o una organización es denominado como amenaza.

Tarea T2.2.1: Identificación de las amenazas

Tarea T2.2.2: Valoración de las amenazas

Actividad A2.3: Caracterización de las salvaguardas

Para la caracterización de los salvaguardas se toma el paso 3 definido por magerit donde nos orientan los criterios para el efectivo cumplimiento de las tareas.

Tarea T2.3.1: Identificación de las salvaguardas existentes

Tarea T2.3.2: Valoración de las salvaguardas existentes

Actividad A2.4: Estimación del estado de riesgo

En la estimación del riesgo nos apoyamos en el paso 6 de magerit dado un cierto conjunto de salvaguardas desplegadas y una medida de la madurez de su proceso de gestión, el sistema queda en una situación de riesgo que se denomina residual.

Tarea T2.4.1: Estimación del impacto

Tarea T2.4.2: Estimación del riesgo

Tarea T2.4.3: Interpretación de los resultados

Proceso P3: Gestión de riesgos

En este proceso nos apoyamos de la norma ISO/NTC 31000 la cual nos dice que se debe entender la organización y su contexto.

Actividad A3.1: Toma de decisiones

Con base en los resultados obtenidos por el análisis de riesgos tomar decisiones de cuál es la mejor forma de gestionarlos.

Tarea T3.1.1: Calificación de los riesgos

Actividad A3.2: Plan de seguridad

Se debe establecer un escenario y objetivos específicos que deriven de la asignación de tareas, responsabilidades y recursos necesarios para salvaguardar la información.

Tarea T3.2.1: Programas de seguridad

Tarea T3.2.2: Plan de ejecución

Actividad A3.3: Ejecución del plan

Tarea T3.3.1: Ejecución de cada programa de seguridad

Cumplimiento del Marco normativo

La política de gestión de riesgos para la oficina de admisiones registro y control de la Universidad Francisco de Paula Santander Ocaña cumple con las normativas legales vigentes

- **Norma Técnica Colombiana para la gestión de riesgos NTC/ISO 31000:** Principios y directrices[13].

- **Ley 734 de 2002, Numeral 21 y 22 del Art. 34,** son deberes de los servidores Públicos "vigilar y salvaguardar los bienes y valores que le han sido encomendados y cuidar que sean utilizados debida y racionalmente", y "responder por la conservación de los útiles, equipos, muebles y bienes confiados a su guarda o administración y rendir cuenta oportuna de su utilización[14]

- **Protección de datos de carácter personal**.
  LOPD, Ley Orgánica 15/1999, de 13 de diciembre, de Protección de Datos de Carácter Personal[15].
  Real Decreto 1720/2007, de 21 de diciembre, por el que se aprueba el Reglamento de desarrollo de la Ley Orgánica 15/1999, de 13 de diciembre, de protección de datos de carácter personal.

[13] *NTC/ISO 31000 GESTIÓN DEL RIESGO.Principios y Directrices.* Bogotá: ICONTEC, 2009. http://l.corporinoquia.gov.co/calidad/15%20SEGUIMIENTO%20Y%20MEDICION/NORMOGRAMA%20SEGUIMIENTO%20Y%20MEDICI%C3%93N/NTC-ISO31000.pdf
[14] SOCIEDADES, SUPERINTENDENCIAS DE. . *Manual Manejo y Control Administrativo de los Bienes de Propiedad. , . [en línea]*. Bogotá D.C., Colombia, 2009. 29h
[15] (1999) http://www.protecciondedatos.urjc.es/proteccion_de_datos/PD/legislacion/legislacion/LOPD.pdf

CONCLUSIONES

Para el diseño de la presente política de gestión de riesgos de la información de realizó un reconocimiento a la oficina de Admisiones, registro y Control de la UFPSO, donde se aplicaron instrumentos de recolección de información (entrevistas, encuestas, listas de chequeo, lista de verificación de buenas prácticas), lo cual arrojó insumos valiosos para el análisis correspondiente a la gestión de riesgo de la información.

Esta indagación brindó soporte fundamental para el proceso de análisis, identificación y aplicación de las normas que se relacionan con la gestión del riesgo de la información. Dentro del estudio realizado para la identificación de la norma se tuvo en cuenta COBIT 4.1, ISO/IEC 27002, ISO 31000/2009 y MAGERIT – versión 3.0. En el diseño de la presente política, se aplicaron lineamientos de la norma ISO 31000/2009 donde se establece una serie de principios de carácter genérico, fundamentales que se deben cumplir para hacer una gestión eficaz de riesgo, también se tomaron en cuenta los lineamientos de MAGERIT – versión 3.0, este estándar se basa en los principios de mandato, compromiso, diseño del marco de trabajo, implementación de la gestión del riesgo, seguimiento y revisión del marco, y mejora continua del marco, hace énfasis en método sistemático para analizar tratar los riesgos derivados del uso de tecnologías de la información y comunicaciones (TIC).

Con el diseño de la presente política de gestión de riesgos de la información se pretende establecer un marco de trabajo donde se identifique, se valoren, analicen y se traten los riesgos de la información del entorno, que amenazan la misión de la dependencia de admisiones, registro y control de la UFPSO. Se busca brindar información confiable para que los responsables del proceso reconozcan la existencia de los riesgos a que se enfrenta la dependencia cada día y se tomen las mejores decisiones en busca del logro de los objetivos institucionales.

RECOMENDACIONES

Socializar el presente documento con los directivos de las diferentes dependencias de la UFPSO.

Implementar una política de gestión del riesgo de la información para proteger los objetivos misionales de la UFPSO.

Capacitar a los diferentes estamentos de la UFPSO, en la importancia de la administración del riesgo de la información para el logro de los objetivos misionales.

Brindar completo apoyo y respaldo por parte de la alta Dirección de la UFPSO a los líderes de los procesos de gestión del riesgo de TI.

Es necesario el abordaje del tema de la gestión de riesgos de la información entre los diferentes estamentos de la UFPSO.

Establecer coordinaciones entre las diferentes dependencias de la UFPSO para la ejecución compartida de los acciones de reducción de riesgos de la información.

BIBLIOGRAFÍA

DINAEL ACOSTA PORTILLO INGRID LORENA ALVAREZ PRADA, JORGE ALBERTO CAMARGO BARBOSA, KAREN LORENA NÚÑEZ ASCANIO Diseño de un modelo de Gestión de Riesgos de Tecnologias de información para la unidad de contabilidad de la universidad Francisco de Paula Santader Ocaña [Libro]. - Ocaña : UFPSO, 2012.

DINAEL ACOSTA PORTILLO INGRID LORENA ALVAREZ PRADA,JORGE ALBERTO CAMARGO BARBOSA,KAREN LORENA NÚÑEZ ASCANIO DISEÑO DE UN MODELO DE GESTIÓN DEL RIESGO DE TECNOLOGÍAS DE INFORMACIÓN PARA LA UNIDAD DE CONTABILIDAD DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER [Libro]. - OCAÑA : Tesis de grado para la Esp Auditoria de Sistemas, 2013.

Direción General de Modernización Administrativa Procedimientos e Impulso de la Administración Electronica MARGERIT - Versión 3.0 Metodologia de Analisis y Gestión de Riesgos de los Sistemas de Información [Libro]. - Madrid : Ministerio de Hacienda y Administraciones Públicas, Octubre de 2012.

Institute IT Governance MARCO DE TRABAJO DE COBIT [Libro]. - [s.l.] : www.itgi.org, 2007.

LEY ORGANICA 15/99 PROTECCION DE DATOS DE CARACTER PERSONAL [Publicación periódica]. - 1999.

NTC/ISO 31000 GESTIÓN DEL RIESGO.Principios y Directrices [Libro]. - Bogotá : ICONTEC, 2009.

Perez Torcoroma Velasquez Modulo de Inducción [Libro]. - Ocaña : www.ufpso.edu.co, 2012.

Perez Yesica Maria Perez Guia para la implementación de gobierno corporativo de TI [Libro]. - Ocaña : [s.n.], 2014.

SOCIEDADES SUPERINTENDENCIAS DE . Manual Manejo y Control Administrativo de los Bienes de Propiedad. , . [en línea] [Libro]. - Bogotá D.C., Colombia : [s.n.], 2009. 29h.

UFPSO Admisiones, Registro y Control [Libro]. - Ocaña : www.ufpso.edu.co, 2014.

FUENTES ELECTRÓNICAS

MINISTERIO DEL INTERIOR Y DE JUSTICIA DE COLOMBIA. Dirección Nacional del Derecho de Autor. Unidad Administrativa Especial. [en línea].
http:/ SUPERINTENDENCIAS DE SOCIEDADES. Manual Manejo y Control Administrativo de los Bienes de Propiedad. Bogotá D.C., Colombia, 2009. 29h. [en línea]. http://www.supersociedades.gov.co/web/Ntrabajo/SISTEMA_INTEGRADO/Documentos%20Infraestructura/DOCUMENTOS/GINF-M-001%20MANUAL%20ADMINISTRATIVO.pdf/www.propiedadintelectualcolombia.com/Site/LinkClick.aspx?fileticket=yDsveWsCdGE%3D&tabid=

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER. Consejo Superior Universitario. Acuerdo No. 126. Diciembre 9 de 1994. [en línea]. http://www.ufpso.edu.co/ftp/pdf/acuerdos/acuerdo_126.pdf

UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA. Gerencia de Innovación y Desarrollo Tecnológico. Última actualización el Lunes, 22 de Abril de 2013 09:05. [en línea]. http://www.unad.edu.co/gidt/index.php/leyesinformaticas

ISO/IEC 27002:2005 Tecnología de la información - Técnicas de seguridad - Código de buenas prácticas para la gestión de seguridad de la información. [en línea]. http://www.iso.org/iso/home/search.htm?qt=iso+27002&sort=rel&type=simple&published=on

GÓMEZ, Humberto. Gerencia Estratégica Planeación y Gestión - Teoría y metodología. Santa Fé de Bogotá: 3R Editores, 1994.

http://www.sistemas.ith.mx/raymundo/Cobit/IntroduccionAlRiesgoInformatico.pdf

ANEXOS.

Anexo A. Encuestas

ENCUESTA DIRIGIDA AL PERSONAL ADMINISTRATIVO DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

¿Existe en la Universidad una Política de administración de Riesgos?
SI_____ NO_____
Cual?_____
_____
__
¿Recibió usted Capacitación o socialización de la Política de administración de Riesgos?
SI_____ NO_____

¿Actualmente este Política de administración de Riesgos se está aplicando en la Universidad?
SI_____ NO_____

GRACIAS.

ENCUESTA DIRIGIDA AL JEFE DE LA OFICINA DE ADMISIONES REGISTRO Y CONTROL DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

¿Existe en la Universidad un Política de administración de Riesgos?
SI_____ NO_____
Cual?_____
_____
__
¿Recibió usted Capacitación o socialización de la Política de administración de Riesgos?
SI_____ NO_____

¿Actualmente esta Política de administración de Riesgos se está aplicando en la Universidad?
SI_____ NO_____
¿En qué año fue creado la Política de administración de Riesgos? _____
¿Esta Política de administración de Riesgos?

SI_____ NO_____
¿Cuántas versiones? _____
¿Cuál fue la ultima?_____

Anexo B. Entrevistas

Entrevista para realizar al personal de la empresa

Entrevista 1
Gerencia de TI

1 ¿Cómo está estructurada el área de tecnologías de la información?
2 ¿Existe una planificación estratégica?
3 ¿Cómo se realiza el plan estratégico y quienes son los involucrados?
4 La planificación estratégica de ti se comparte con la gerencia del negocio?
5 ¿Cada cuánto tiempo se reestructura la planificación estratégica?
6 ¿Para la contratación del personal interviene el personal de ti?
7 ¿Cuántas personas conforman el área de ti?
8 ¿El personal recibe capacitaciones?¿cada cuánto?
9 ¿Cómo se manejan las vacaciones del personal?
10 ¿Cómo se maneja la seguridad personal, física, legal, lógica y de datos en la oficina?
11 ¿A qué problemas se ha enfrentado el área de ti?

Entrevista 2
Infraestructura de TI
1. ¿Existe personal encargado para la infraestructura de TI?
2. ¿Cómo es la topología de la red o esquema?
3. ¿Qué políticas de seguridad se manejan?
4. ¿Existe seguridad al acceso de servidores?
5. Que sistemas operativos usan para servidor/usario?
6. ¿El software esta licenciado?
7. ¿Existe detección de vulnerabilidades?
8. ¿Existen restricción de usuarios que se conecten a la red?
9. ¿Cuántas personas trabajan en el área?
10. ¿Existen planes de adquisición y mantenimiento de la Arquitectura de TI?

Entrevista 3
Ingeniería de SW
1. ¿Existe grupo de ingeniería de software?
2. Que función desempeña esta área?
3. ¿Cuántas personas trabajan en esta área?
4. ¿Qué aplicaciones son desarrolladas o adquiridas por esta oficina?
5. ¿Las aplicaciones desarrolladas tienen soporte, mantenimiento, código fuente documentado y manuales de usuario?
6. ¿Qué seguridad existe en los sistemas?
7. Que problemas han sido enfrentados por esta area?
8. ¿Se da capacitaciones a los usuarios para el uso de las aplicaciones?
9. ¿Cómo se manejan los cambios de requerimientos?
10. ¿Se satisfacen los requerimientos del usuario?

11. ¿Existe documentación de todas las aplicaciones?
12. ¿Cómo se maneja los cambios de requerimientos?
13. ¿Se satisface los requerimientos de los usuarios?
14. ¿Existen políticas para la adquisición de software?
15. ¿Cómo se selecciona los proveedores de software?
16. ¿Existe una administración de contratos con los proveedores?
17. ¿En qué leguaje de programación se desarrolla y que metodologías de desarrollo se usan?

Entrevista 4
Help Desk

1. ¿Existe un grupo de soporte?
2. ¿Qué funciones desempeña?
3. ¿Cuántas personas trabajan?
4. ¿Qué problemas han sido afrontados por esta área?

Entrevista 5
1. ¿Existe una administración de datos definida formalmente?
2. Existe planeación de la infraestructura tecnológica?
3. ¿Antes de realizar una compra la gerencia está totalmente de acuerdo?
4. ¿Existe gestión de riegos/cambios?
5. ¿Las actividades de TI son reactivas o proactivas?
6. ¿Se define un ambiente de control interno?
7. ¿La división de roles y responsabilidades está definida formalmente?
8. ¿Existen políticas, procedimientos, estándares y procesos de cumplimiento?
9. ¿Existe manejo de inventario?
10. ¿Para los proyectos que se realizan se hace alguna evaluación de riesgos o se implementa cuando se identifican los riesgos?¿Existe un proceso definido?
11. ¿Existe gestión de proyectos?¿Se toman en cuenta el impacto?
12. ¿Se definen roles y responsabilidades para proyectos?
13. ¿Se hace un seguimiento al tiempo, gastos en equipo y presupuestos para proyectos?

Entrevista 6
Adquirir y mantener software aplicativo
1. ¿Existe un diseño y especificaciones de aplicaciones?
2. ¿Existe consistencia de la necesidad de contar con un proceso de adquisición y mantenimiento de aplicación?
3. ¿El mantenimiento es problemático?
4. ¿Se tiene consideraciones para la seguridad y disponibilidad de aplicaciones?

5. ¿Existe un proceso claro y definido para la adquisición y mantenimiento de software aplicativo?
6. ¿Este proceso va de acuerdo a la estrategia de TI y del negocio?
7. ¿las actividades de mantenimiento se planean, programan y coordinan?
8. ¿Qué metodologías de desarrollo utilizan?¿Son flexibles?
9. ¿Existe un proceso de documentación?
10. ¿Las prácticas de adquisición y mantenimiento de software aplicativo se alinean con el proceso definido?

Adquirir y mantener infraestructura tecnológica
1. ¿Se realizaron cambios en la infraestructura para cada nueva aplicación de acuerdo a un plan conjunto?
2. ¿Existe un ambiente diferente de producción y ambiente de prueba?
3. ¿Se considera la adquisición y mantenimiento de la infraestructura de TI cono una estrategia definida para satisfacer las necesidades de la aplicación del negocio?¿ En qué porcentaje se lo realiza?
4. ¿Se maneja procedimientos formales?

Entrevista 7
Garantizar la seguridad de los sistemas
1. ¿Las responsabilidades y rendición de cuentas están asignadas?
2. ¿Qué medidas están implementadas paras oportar la administración de seguridad de TI?
3. ¿Existen reportes de Seguridad de TI?
4. ¿Qué medidas están implementadas para soportar la administración de seguridad de TI?
5. ¿Existen reportes de seguridad de TI?
6. ¿La seguridad se lleva acabo de forma reactiva?
7. ¿Los sistemas producen información relevante respecto a seguridad?¿Esta información es actualizada?
8. ¿Existe un plan de Seguridad de TI?¿Qué aspectos Están considerados?
9. ¿Se desarrolla pruebas de seguridad?
Educar y entrenar a los usuarios
1. ¿Se imparte clases formales acerca de temas como conducta ética, concienciación y práctica de seguridad en los sistemas?

Entrevista 9
Administración de operaciones
1. ¿La infraestructura de TI puede resistir y recuperarse a errores?
2. ¿Los procesos de operaciones son programados se manera formal o informal?
3. ¿Existe dependencia de las habilidades de los individuos?
4. ¿La programación de tareas se documenta, comunican tanto a la función interna de TI como a los clientes del negocio?

5. ¿Las operaciones de soporte de TI son efectivas, eficientes y suficientemente flexibles para cumplir con las necesidades de niveles de servicio sin pérdida de productividad?
6. ¿Los procesos automatizados que soportan los sistemas contribuyen a tener un ambiente estable?
7. ¿Se considera a los problemas e incidentes diferentes?
8. ¿La resolución de problemas son formales o informales?
9. ¿La administración de problemas de maneja en todos los niveles de la organización?

Anexo C.

Tabla 15. Matriz de Cumplimiento Misión Actual

	MATRIZ DE CUMPLIMIENTO							
	Misión Actual: Prestar un buen servicio a los estudiantes y demás estamentos en cada uno de los requerimientos que se hagan ya que ésta dependencia es un pilar fundamental por los documentos que allí reposan y hacer cumplir las normas del Reglamento Estudiantil en materia de desempeño académico.							
	Criterios	**Min**				**Max**	**Total**	**Observación**
		1	2	3	4	5		
1	El enunciado de la misión es claro y comprensible para todo el personal, incluyendo a los empleados de base.	1					2	El enunciado no es claro para todo el personal, solo se harán una idea las personas que conozcan el reglamento estudiantil.
2	La declaración de la misión es tan breve como para que la mayoría de las personas la recuerden. Por lo general, contiene 100 palabras o menos, en lo posible.					1	10	No es extensa
3	El enunciado de la misión específica con claridad en qué negocio se encuentra la organización. Esto incluye una declaración detallada acerca de:						0	
3.1	"Qué" necesidades del consumidor o cliente trata de satisfacer la compañía, y no cuáles productos o servicios ofrece.	1					0.5	
3.2	"Quienes" son los consumidores o clientes principales de la organización.		1				1	El público en general también necesita de la información
3.3	"Cómo" plantea la organización emprender su negocio, es decir, cuáles son sus tecnologías primarias.	1					0.5	No describe sus tecnologías primarias
3.4	"Por qué" existe la empresa, es decir, el propósito	1					0.5	

Tabla 1. (Continuación)

	predominante que trata de cumplir y sus metas transcendentales.							
4	La declaración de la misión debe identificar las fuerzas que impulsa la visión estratégica de la empresa.	1					2	
5	La declaración de la misión debe reflejar las ventajas competitivas de la organización.	1					2	
6	La declaración de la misión debe ser suficientemente amplia como para permitir flexibilidad en la implementación, pero no tanta como para permitir la carencia de enfoque.	1					2	
7	La declaración de la misión debe servir como el modelo y medio con el cual los gerentes y demás individuos en la empresa puedan tomar decisiones.		1				4	
8	8. La declaración de la misión debe reflejar los valores, las creencias y la filosofía de operaciones de la empresa.	1					2	
9	La declaración de la misión debe ser lograble, y suficientemente realista como para que los miembros de la organización se involucren en ella.			1			6	
10	El texto de la declaración de la misión debe servir como fuente de energía y punto de unión de la organización.	1					2	
				Total:			34.5	65.5
	Fuente: Leonard D. Timothy M. William P. Planeación Estratégica Aplicada pág. 220, 221 (año 1998) Editorial Mc							

	Graw Hill.							

Fuente. Autor del proyecto

Tabla 16. Matriz de Cumplimiento de la Misión Propuesta

	MATRIZ DE CUMPLIMIENTO							
	Misión propuesta: La oficina de admisiones registro y control es la encargada de recopilar, articular, monitorear y salvaguardar la historia académica de la Universidad al servicio de la comunidad en general, de acuerdo a la normatividad vigente, tecnologías de la información y comunicación, el sistema de gestión de calidad y un talento humano calificado, que contribuya al cumplimiento de los propósitos misionales.							
	Criterios	**Min**				**Max**	**Total**	**Observación**
		1	2	3	4	5		
1	El enunciado de la misión es claro y comprensible para todo el personal, incluyendo a los empleados de base.					1	10	
2	La declaración de la misión es tan breve como para que la mayoría de las personas la recuerden. Por lo general, contiene 100 palabras o menos, en lo posible.					1	10	
3	El enunciado de la misión específica con claridad en qué negocio se encuentra la organización. Esto incluye una declaración detallada acerca de:						0	
3	"Qué" necesidades del consumidor o cliente trata de satisfacer la compañía, y no cuáles productos o servicios ofrece.					1	2.5	
3	"Quienes" son los consumidores o clientes principales de la organización.					1	2.5	
3	"Cómo" plantea la organización emprender su negocio, es decir, cuáles son sus tecnologías primarias.					1	2.5	
3	"Por qué" existe la empresa, es decir, el propósito predominante que trata de cumplir y sus metas					1	2.5	

	transcendentales.							
4	La declaración de la misión debe identificar las fuerzas que impulsa la visión estratégica de la empresa.			1			6	
5	La declaración de la misión debe reflejar las ventajas competitivas de la organización.			1			6	
6	La declaración de la misión debe ser suficientemente amplia como para permitir flexibilidad en la implementación, pero no tanta como para permitir la carencia de enfoque.				1		8	
7	La declaración de la misión debe servir como el modelo y medio con el cual los gerentes y demás individuos en la empresa puedan tomar decisiones.					1	10	
8	8. La declaración de la misión debe reflejar los valores, las creencias y la filosofía de operaciones de la empresa.					1	10	
9	La declaración de la misión debe ser lograble, y suficientemente realista como para que los miembros de la organización se involucren en ella.					1	10	
10	El texto de la declaración de la misión debe servir como fuente de energía y punto de unión de la organización.				1		8	
							88	12

Fuente: Perez, Y. M. (2014). Guia para la implementación de gobierno corporativo de TI. Ocaña.