RESUMEN – TRABAJO DE GRADO

AUTORES	**ANDRO CABRALES ÁLVAREZ**
FACULTAD	**INGENIERÍAS**
PLAN DE ESTUDIOS	**INGENIERÍA DE SISTEMAS**
DIRECTOR	**YESICA MARÍA PÉREZ PÉREZ**
TÍTULO DE LA TESIS	**GESTIÓN DE RIESGOS PARA LA PARA LA DEPENDENCIA DE ADMISIONES REGISTRO Y CONTROL DE UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA**

RESUMEN

(70 palabras aproximadamente)

LA INVESTIGACIÓN REALIZADA A CONTINUACIÓN PROPONE UNA GESTIÓN DE RIESGOS PARA LA DEPENDENCIA DE ADMISIONES, REGISTRO Y CONTROL DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA, ENFATIZADA EN LA ESTRUCTURA DE LA NORMA ISO 27005:2009, BASADA EN TÉCNICAS PARA LA GESTIÓN DEL RIESGO EN LA SEGURIDAD DE LA INFORMACIÓN.

ANALIZANDO QUE PARA LA CORRECTA REALIZACIÓN DE LA GESTIÓN DE RIESGOS SE HACE NECESARIO UNA AMPLIA CONCEPTUALIZACIÓN DE TERMINOS REFERENTES A SEGURIDAD DE LA INFORMACIÓN, ASI COMO SUS DIFERENTES CONTROLES Y MANEJO DE CADA UNO DE ELLOS.

CARACTERÍSTICAS

PÁGINAS: 37	PLANOS:	ILUSTRACIONES:	CD-ROM: 1

GESTIÓN DE RIESGOS PARA LA DEPENDENCIA ADMISIONES REGISTRO Y CONTROL DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

ANDRO CABRALES ALVAREZ

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERIAS
INGENIERIA DE SISTEMAS
OCAÑA
2016

GESTIÓN DE RIESGOS PARA LA DEPENDENCIA ADMISIONES REGISTRO Y CONTROL DE LA UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

ANDRO CABRALES ALVAREZ

Trabajo de grado para optar el título de Ingeniero de Sistemas

IS. ESP. YESICA MARIA PÉREZ PÉREZ
Director

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA
FACULTAD DE INGENIERIAS
INGENIERIA DE SISTEMAS
OCAÑA
2016

TABLA DE CONTENIDO

INTRODUCCIÓN 7

1.1 TITULO DE LA MONOGRAFÍA 8
1.2 PROBLEMA DE INVESTIGACIÓN 8
1.3 FORMULACIÓN DEL PROBLEMA 9
1.4 OBJETIVOS 9
1.4.1 Objetivo General 9
1.4.2 Objetivos específicos 9
1.5 JUSTIFICACIÓN 9

2.1 ANTECEDENTES 11
2.2 BASES TEÓRICAS 12
2.3 MARCO CONCEPTUAL 14
2.4 MARCO LEGAL 17

3.1 TIPO DE INVESTIGACIÓN 22
3.2 POBLACIÓN 22
3.3 MUESTRA 22
3.4 TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN 22

PRESENTACIÓN DE RESULTADOS 23
4.1 PRIMER OBJETIVO ESPECÍFICO 24
4.2 SEGUNDO OBJETIVO ESPECÍFICO 25
4.3 TERCER OBJETIVO ESPECÍFICO 33

CONCLUSIONES 35

BIBLIOGRAFÍA 36

FUENTES ELECTRÓNICAS 37

INTRODUCCIÓN

La prevención de los riesgos ya sean informáticos, laborales o de cualquier índole, en su sentido más estricto ha sido uno de los objetivos más difíciles de alcanzar a lo largo de la historia. Así, el desarrollo de una actividad sistemática que tienda a perfeccionarse hasta el punto de minimizar la posibilidad que se consoliden accidentes en perdida de información, pérdidas materiales o afectación de procesos derivados de un ambiente desfavorable, debe ser el principal objetivo de la prevención de riesgos.

Es por tanto, una decisión de gestión que debe prevalecer en cualquier actividad en la cultura de la organización. Sin embargo, si bien es cierto que ha habido un cambio de mentalidad en lo que a seguridad se refiere, no es menos cierto que la idea de que la seguridad se paga a sí misma es un concepto que todavía no se ha establecido en todos los niveles de la organización empresarial. Existen todavía hoy aquellos que piensan que una inversión en seguridad elevada y una planificación estructurada de actividades no evita más accidentes limitándose a disponer aquellos elementos de seguridad mínimos marcados por la ley.

Por otro lado, cabe destacar que hasta la fecha no se ha conseguido demostrar el hecho de que una mayor inversión en seguridad conlleve un menor coste en accidentes. Así, el objetivo de la presente investigación es intentar establecer una gestión de riesgos que permita mantener en menor riesgo la seguridad de la información en la dependencia de Admisiones Registro y Control de la Universidad Francisco de Paula Santander Ocaña.

CAPITULO 1

TÍTULO

1.1 TITULO DE LA MONOGRAFÍA

Gestión de riesgos para la dependencia Admisiones, Registro y Control de la Universidad Francisco de Paula Santander Ocaña

1.2 PROBLEMA DE INVESTIGACIÓN

La información en sus más variadas formas, es uno de los activos más valiosos y estratégicos de cualquier empresa hoy, tanto para almacenarse adecuadamente, así como para disponer de datos e información relevante.

La dependencia Admisiones, Registro y Control de la Universidad Francisco de Paula Santander Ocaña, se identifica por ser la encargada de llevar, mantener actualizados y custodiar los registros académicos de los estudiantes que hacen parte de la institución, los datos e información almacenados en esta oficina, no están exentos de sufrir vulnerabilidades que afecten su integridad y disponibilidad.

Analizando el nivel de importancia que significa la información almacenada y registrada en esta dependencia, se hace necesario realizar la gestión de riesgos, permitiendo reducir el nivel de vulnerabilidad a la que pueda estar expuesta la información.

La Gestión de riesgo tiene como principal actividad proteger uno de los principales activos que tiene la Universidad Francisco de Paula Santander Ocaña, ya que la cantidad de eventualidades que pueden poner en peligro la información son cada vez mayor.

El análisis de riesgos según el Decreto 3/2010[1], por el que se regula el Esquema Nacional de Seguridad en el ámbito de la Administración Electrónica, en el Capítulo II de sus principios Básicos establece la Gestión de la seguridad basada en los riesgos, definiendo que el análisis y gestión de riesgos será parte esencial del proceso de seguridad y deberá mantenerse permanentemente actualizado, que 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.
Así mismo el Decreto 3/2010, en su Capítulo III en Requisitos Mínimos establece que cada organización que desarrolle e implante sistemas para el tratamiento de la información y las

[1] BOLETIN OFICIAL DEL ESTADO, Real decreto 3/2010, [En línea]. Disponible desde Internet en: < https://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf>[con acceso el 10-10-2015]

comunicaciones realizará su propia gestión de riesgos. 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 metodología reconocida internacionalmente. 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 mayoría de las decisiones, incluyendo las más sencillas involucran riesgo, por lo tanto al no realizar una gestión de riesgo adecuada a la información, pondrá en peligro no solo el activo principal de la institución, sino también la credibilidad de la misma.

1.3 FORMULACIÓN DEL PROBLEMA

¿Una gestión de riesgos adecuada permitirá que los procesos relacionados con la información sean eficientes y eficaces logrando que la información sea disponible, integra y confiable?

1.4 OBJETIVOS

1.4.1 Objetivo General

Optimizar la gestión de riesgos para la dependencia Admisiones, Registro y Control de la Universidad Francisco de Paula Santander Ocaña.

1.4.2 Objetivos específicos

- ✓ Diagnosticar la situación actual para la identificación de riesgos de la oficina de Admisiones, Registro y Control.
- ✓ Identificar y evaluar los riesgos de la dependencia basado en la norma ISO 27005.
- ✓ Establecer controles para los riesgos encontrados en la dependencia de admisiones registro y control en los niveles medio y alto según la norma ISO 27005.

1.5 JUSTIFICACIÓN

La información en las organizaciones es el activo más importante ya que permite tomar decisiones que generan a las empresas ventajas competitivas, generar estadísticas, mejorar

su productividad y eficiencia operativa, por ello debe ser protegida al máximo para evitar riesgos y áreas de vulnerabilidad en la organización.

En la dependencia de Admisiones, Registro y Control de la Universidad Francisco de Paula Santander de Ocaña se mantienen actualizados los registros académicos de los estudiantes ya que apoya a los procesos de inscripción, admisión y matrícula; debido a esto la dependencia maneja gran cantidad de información personal, que debe ser protegida como lo indica la Ley 1273 de 2009[2], y donde cualquier divulgación de ésta se le podrá dar pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Actualmente en la dependencia se hace necesario realizar una gestión de riesgos que permita evitar y/o mitigar amenazas y vulnerabilidades que impidan el desarrollo de los procesos y actividades relacionadas a la información, evitando que se filtre o se pierda esté activo tan importante, así mismo servirá como medida de seguridad que contribuya a mantener la integridad, confidencialidad y disponibilidad de los datos dentro de los procedimientos que manejan dentro de la oficina.

[2] CONGRESO DE LA REPUBLICA COLOMBIANA. LEY 1273 DE 2009 [En línea]. Disponible desde Internet en: <http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html> [con acceso el 08-09-2015]

CAPITULO 2

MARCO TEÓRICO O REFERENCIAL

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 esta investigación 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[3].

2.1 ANTECEDENTES

La 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)
- 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

La Unidad de Contabilidad de l**a Universidad Francisco de Paula Santander Ocaña**, para esta oficina se diseñó un modelo de gestión del riesgo de las tecnologías de la información.

La Universidad del Valle, Desarrolla en Febrero de 2014 un modelo instrumental para el tratamiento integral y la gestión apropiada de los riesgos, donde concibió una disciplina denominada “Administración de Riesgos” o “Gerencia de Riesgos” que es una función de

[3] 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 Esp Auditoria de Sistemas

muy alto nivel dentro de la organización, para definir un conjunto de estrategias que a partir de los recursos (humanos, físicos, tecnológicos y financieros) busca, en el corto plazo mantener la estabilidad financiera de la empresa protegiendo los activos e ingresos y en el largo plazo minimizar las pérdidas ocasionadas por la ocurrencia de dichos riesgos.

La Universidad Distrital Francisco José de Caldas[4], Diseño sus Políticas para la seguridad de la información para contar con estrategias de alto nivel que permitan el control y administración efectiva de los datos. Debido a que en la institución, los sistemas y red de información enfrentan amenazas de seguridad que incluyen, entre muchas otras: el fraude por computadora, espionaje, sabotaje, vandalismo, fuego, robo e inundación. Las posibilidades de daño y pérdida de información por causa de código malicioso, mal uso o ataques de denegación de servicio se hacen cada vez más comunes. Con la promulgación de la presente Política de Seguridad de la Información la Universidad formaliza su compromiso con el proceso de gestión responsable de información que tiene como objetivo garantizar la integridad, confidencialidad y disponibilidad de este importante activo.

SISTESEG, Empresa Colombiana líder en servicios de seguridad de la información (SGSI), planes para la continuidad del negocio y Auditorías sobre la infraestructura de tecnología con un equipo humano profesional, comprometido y de amplia experiencia, capaz de interpretar los requerimientos de cualquier empresa y convertirlos en servicios de seguridad de la información hechos a su medida. Esta empresa diseñó sus propias políticas de seguridad física[5], donde identifica las amenazas, vulnerabilidades y las medidas que pueden ser utilizadas para proteger físicamente los recursos y la información de la organización. Los recursos incluyen el personal, el sitio donde ellos laboran, los datos, equipos y los medios con los cuales los empleados interactúan, en general los activos asociados al mantenimiento y procesamiento de la información, como por ejemplo activos de información, activos de software y activos físicos.

2.2 BASES TEÓRICAS

Toda organización basada en el contexto de TI, necesita marcos de trabajo para la toma de decisiones orientados por la Gobernabilidad de tecnologías que permiten tomar total ventaja de su información logrando con esto maximizar sus beneficios, capitalizar sus oportunidades y obtener ventaja competitiva, en el caso de esta investigación las siguientes son teorías que dan soporte a la gestión de riesgos y administración del mismo en la oficina de Admisiones, Registro y Control.

---

[4] UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS. Política para la seguridad de la información de la universidad distrital Francisco José de Caldas. [En línea]. Disponible desde Internet en: <http://portalws.udistrital.edu.co/CIT/documentos/NORMATIVIDAD/politica_seguridad/archivos/Politica_para_Seguridad_Informacion_Version_0.0.1.0.pdf>[con acceso el 09-09-2015]

[5] POLITICA DE SEGURIDAD FÍSICA. SISTESEG. [En línea]. Disponible desde Internet en: <http://www.sisteseg.com/files/Microsoft_Word_-_Politica_Seguridad_Fisica.pdf>[con acceso el 08-09-2015]

Desde 1901, y como primera entidad de normalización a nivel mundial, BSI (British Standards Institution) es responsable de la publicación de importantes normas como:
1979 Publicación BS 5750 – hoy ISO 9001.
1992 Publicación BS 7750 - hoy ISO 14001
1996 Publicación BS 8800 - hoy OHSAS 18001.

La norma BS 7799 de BSI aparece por primera vez en 1995, con objeto de proporcionar a cualquier empresa británica, un conjunto de buenas prácticas para la gestión de la seguridad de su información.

La primera parte de la norma (BS 7799-1) es la guía de buenas prácticas, para la que no se establece un modelo de certificación.

La segunda parte (BS 7799-2), publicada por primera vez en 1998, que establece los requisitos de un Sistema de Seguridad de la Información (SGSI) para ser certificable por una entidad independiente.

Las dos partes de la norma BS 7799 se revisaron en 1999 y la primera parte se adopta por ISO, sin cambios sustanciales, como ISO 17799 en el año 2000. En 2002, se revisa BS 7799-2 para adecuarse a la filosofía de normas ISO de sistemas de gestión.

En 2005, y con más de 1700 empresas certificadas en BS7799-2, este esquema se publica por ISO como estándar 27001. También en ese año se revisa ISO17799.

La serie 27000

A semejanza de otras normas ISO, la 27000 es realmente una serie de estándares

2.2.1 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.
Fue publicada el 15 de Octubre de 2005 y sustituye a la BS 7799-2, habiéndose establecido unas condiciones de transición para aquellas empresas certificadas en esta última.

2.2.2 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.

2.2.3 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 es la que actualmente está en vigor.

2.2.4 ISO 27003. Guía de implementación de SGSI e información acerca del uso del modelo PDCA (Planificar, Hacer, Verificar y Actuar) y de los requerimientos de sus diferentes fases.

Tiene su origen en el anexo B de la norma BS7799-2 y en la serie de documentos publicados por BSI a lo largo de los años con recomendaciones y guías de implantación.

2.2.5 ISO 27004. Especifica las métricas y las técnicas de medida aplicables para determinar la eficacia de un SGSI y de los controles relacionados. Estas métricas se usan fundamentalmente para la medición de los componentes de la fase "Do" (Implementar y Utilizar) del ciclo PDCA.

2.2.6 ISO 27005. Guía para la gestión del riesgo de la seguridad de la información y servirá, por tanto, de apoyo a la ISO27001 y a la implantación de un SGSI. Se basará en la BS7799-3 (publicada en Marzo de 2006) e ISO 13335-3.

De igual manera dan soporte a estas teorías

2.2.7 COBIT (Control Objectives for Information and related Technology). Busca desarrollar un conjunto de objetivos de control en tecnologías de información y está orientado a negocios. Indica que los recursos de TI deben administrarse por un conjunto de procesos.

2.2.8 Estándar Australiano/Neozelandés - AS/NZS: 4360. 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.

2.2.9 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.

2.3 MARCO CONCEPTUAL

El estudio de los riesgos de manera más explícita, hace parte del desarrollo mismo de la humanidad y de la civilización, para poder establecer sociedades más seguras, en este sentido, las entidades de la administración pública no pueden ser ajenas al tema de los riesgos y deben buscar cómo manejarlos y controlarlos partiendo de la base de su razón de ser y su compromiso con la sociedad

Teniendo en cuenta, que la presente investigación 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.

Impacto.
Cambio adverso en el nivel de los objetivos del negocio logrados.

Riesgo en la seguridad de la información.
Potencial de que una amenaza determinada explote las vulnerabilidades de los activos o grupos de activos causando así daño a la organización.

Evitación del riesgo.
Decisión de no involucrarse en una situación de riesgo o tomar acción para retirarse de dicha situación.

Comunicación del riesgo.
Intercambiar o compartir la información acerca del riesgo entre la persona que toma la decisión y otras partes interesadas.

Estimación del riesgo.
Proceso para asignar valores a la probabilidad y las consecuencias de un riesgo.

Identificación del riesgo.
Proceso para encontrar, enumerar y caracterizar los elementos de riesgo.

Reducción del riesgo.
Acciones que se toman para disminuir la probabilidad las consecuencias negativas, o ambas, asociadas con un riesgo.

Retención del riesgo.
Aceptación de la pérdida o ganancia proveniente de un riesgo particular.

Transferencia del riesgo.
Compartir con otra de las partes la pérdida o la ganancia de un riesgo

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.

2.4 MARCO LEGAL

La investigación se enmarcará en parámetros legales así:

Constitución Política de Colombia[6].

Artículo 61. El Estado protegerá la propiedad intelectual por el tiempo y mediante las formalidades que establezca la ley**.**

Ley 1273 de 2009 (5 de enero)[7]. El Congreso de la República de Colombia, establece la ley 1273 por medio de la cual se modifica el Código Penal, creando 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.

El proyecto tendrá como bases legales la ley 1273 de 2009, en sus artículos:

Artículo 269A: Acceso abusivo a un sistema informático. El que, sin autorización o por fuera de lo acordado, acceda en todo o en parte a un sistema informático protegido o no con una medida de seguridad, o se mantenga dentro del mismo en contra de la voluntad de quien tenga el legítimo derecho a excluirlo, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269B: Obstaculización ilegítima de sistema informático o red de telecomunicación. El que, sin estar facultado para ello, impida u obstaculice el funcionamiento o el acceso normal a un sistema informático, a los datos informáticos allí contenidos, o a una red de telecomunicaciones, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con una pena mayor.

Artículo 269C: Interceptación de datos informáticos. El que, sin orden judicial previa intercepte datos informáticos en su origen, destino o en el interior de un sistema informático, o las emisiones electromagnéticas provenientes de un sistema informático que los transporte incurrirá en pena de prisión de treinta y seis (36) a setenta y dos (72) meses.

Artículo 269D: Daño Informático. El que, sin estar facultado para ello, destruya, dañe, borre, deteriore, altere o suprima datos informáticos, o un sistema de tratamiento de

[6] REPÚBLICA DE COLOMBIA, Constitución Política De La República De Colombia De 1991, Actualizada hasta el Decreto 2576 del 27 de Julio de 2005

[7] CONGRESO DE LA REPUBLICA COLOMBIANA. Op. cit.

información o sus partes o componentes lógicos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269E: Uso de software malicioso. El que, sin estar facultado para ello, produzca, trafique, adquiera, distribuya, venda, envíe, introduzca o extraiga del territorio nacional software malicioso u otros programas de computación de efectos dañinos, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes.

Artículo 269F: Violación de datos personales. El que, sin estar facultado para ello, con provecho propio o de un tercero, obtenga, compile, sustraiga, ofrezca, venda, intercambie, envíe, compre, intercepte, divulgue, modifique o emplee códigos personales, datos personales contenidos en ficheros, archivos, bases de datos o medios semejantes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1000 salarios mínimos legales mensuales vigentes.

Artículo 269G: Suplantación de sitios web para capturar datos personales. El que con objeto ilícito y sin estar facultado para ello, diseñe, desarrolle, trafique, venda, ejecute, programe o envíe páginas electrónicas, enlaces o ventanas emergentes, incurrirá en pena de prisión de cuarenta y ocho (48) a noventa y seis (96) meses y en multa de 100 a 1.000 salarios mínimos legales mensuales vigentes, siempre que la conducta no constituya delito sancionado con pena más grave.

En la misma sanción incurrirá el que modifique el sistema de resolución de nombres de dominio, de tal manera que haga entrar al usuario a una IP diferente en la creencia de que acceda a su banco o a otro sitio personal o de confianza, siempre que la conducta no constituya delito sancionado con pena más grave.

La pena señalada en los dos incisos anteriores se agravará de una tercera parte a la mitad, si para consumarlo el agente ha reclutado víctimas en la cadena del delito.

Artículo 269H: Circunstancias de agravación punitiva: Las penas imponibles de acuerdo con los artículos descritos en este título, se aumentarán de la mitad a las tres cuartas partes si la conducta se cometiere:

1. Sobre redes o sistemas informáticos o de comunicaciones estatales u oficiales o del sector financiero, nacionales o extranjeros.
2. Por servidor público en ejercicio de sus funciones.
3. Aprovechando la confianza depositada por el poseedor de la información o por quien tuviere un vínculo contractual con este.
4. Revelando o dando a conocer el contenido de la información en perjuicio de otro.
5. Obteniendo provecho para sí o para un tercero.
6. Con fines terroristas o generando riesgo para la seguridad o defensa nacional.
7. Utilizando como instrumento a un tercero de buena fe.

8. Si quien incurre en estas conductas es el responsable de la administración, manejo o control de dicha información, además se le impondrá hasta por tres años, la pena de inhabilitación para el ejercicio de profesión relacionada con sistemas de información procesada con equipos computacionales.

Norma ISO/IEC27002[8]. Tecnología de la información, técnicas de seguridad. Código de práctica para la gestión de la información. Esta norma establece directrices y principios generales para iniciar, implementar, mantener y mejorar la gestión de la seguridad de la información en una organización.

Esta norma puede servir como guía práctica para el desarrollo de normas de seguridad de la organización y para las prácticas eficaces de gestión de la seguridad, así como para crear confianza en las actividades entre las organizaciones.

Ley 599 de 209. Por la Cual se Expide el Código Penal, título VIII de los delitos contra los derechos de autor capitulo único:

Artículo 270. Violación a los derechos morales de autor. Incurrirá en prisión de dos (2) a cinco (5) años y multa de veinte (20) a doscientos (200) salarios mínimos legales mensuales vigentes quien:

1. Publique, total o parcialmente, sin autorización previa y expresa del titular del derecho, una obra inédita de carácter literario, artístico, científico, cinematográfico, audiovisual o fonograma, programa de ordenador o soporte lógico.

Parágrafo. Si en el soporte material, carátula o presentación de una obra de carácter literario, artístico, científico, fonograma, videograma, programa de ordenador o soporte lógico, u obra cinematográfica se emplea el nombre, razón social, logotipo o distintivo del titular legítimo del derecho, en los casos de cambio, supresión, alteración, modificación o mutilación del título o del texto de la obra, las penas anteriores se aumentarán hasta en la mitad.

Artículo 272. Violación a los mecanismos de protección de los derechos patrimoniales de autor y otras defraudaciones. Incurrirá en multa quien:

1. Supere o eluda las medidas tecnológicas adoptadas para restringir los usos no autorizados.
2. Suprima o altere la información esencial para la gestión electrónica de derechos, o importe, distribuya o comunique ejemplares con la información suprimida o alterada.

[8] ISO, Op. cit.

[9] CONGRESO DE COLOMBIA. Ley 599 De 2000 (Julio 24). [En línea] Disponible desde Internet en: <http://www.alcaldiabogota.gov.co/sisjur/normas/Norma1.jsp?i=6388>[con acceso el 08-09-2015]

3. Fabrique, importe, venda, arriende o de cualquier forma distribuya al público un dispositivo o sistema que permita descifrar una señal de satélite cifrada portadora de programas, sin autorización del distribuidor legítimo de esa señal, o de cualquier forma de eludir, evadir, inutilizar o suprimir un dispositivo o sistema que permita a los titulares del derecho controlar la utilización de sus obras o producciones, o impedir o restringir cualquier uso no autorizado de éstos.

Ley 87 de 1993. En Colombia desde la expedición de esta ley 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 metodología 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.

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:

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.

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

CAPITULO 3

METODOLOGIA DE LA INVESTIGACIÓN

3.1 TIPO DE INVESTIGACIÓN

Fundamentada mediante una investigación descriptiva, permitirá determinar aquellos rasgos o características de seguridad de la información para la oficina de Admisiones, Registro y Control de la UFPSO.

3.2 POBLACIÓN

En la presente investigación el universo está conformado por la Universidad Francisco de Paula Santander Ocaña y la población se tomará del capital humano que labora en la parte administrativa en la oficina de Admisiones, Registro y Control.

3.3 MUESTRA

Como tenemos una población objeto de estudio reducida, se ha determinado aplicar a todos el instrumento de recolección de información, siendo entonces esta la muestra. Esto con la finalidad de detectar con mayor precisión lo que puede aportar los encuestados, es decir el personal que labora directamente en la oficina de Admisiones, Registro y Control de la Universidad Francisco de Paula Santander Ocaña.

3.4 TÉCNICAS DE RECOLECCIÓN DE INFORMACIÓN

3.4.1 Fuentes primarias. La recopilación de la información necesaria para la estructuración del proyecto se fundamentará en las técnicas de observación y entrevista aplicadas a funcionarios de la dependencia.

3.4.2 Fuentes secundarias. Apoyo en leyes, estándares y normas relacionadas con la gestión y administración de riesgos.

CAPITULO 4

PRESENTACIÓN DE RESULTADOS

El cumplimiento de los objetivos propuestos, se realizó mediante una serie de actividades que se describen a continuación.

Tabla 1. Actividades por objetivo

OBJETIVO ESPECÍFICO	ACTIVIDAD	INDICADOR
Diagnosticar la situación actual para la identificación de riesgos de la oficina de Admisiones, Registro y Control.	Recopilar información utilizando como instrumentos de recolección la entrevista, análisis de material documental de la dependencia y observación. Analizar los factores de riesgo de la información suministrada en la recopilación de información.	Entrevista con funcionarios de la dependencia. Análisis de matriz de riesgos de la dependencia.
Identificar y evaluar los riesgos de la dependencia basado en la norma ISO 27005:2009	Estudiar la norma ISO 27005:2009 contemplando su estructura para la aplicación de la misma. Clasificar y evaluar los riegos acorde a las actividades del proceso de gestión de riesgo de la seguridad de la información.	Análisis de resultados obtenidos en la aplicación de la norma.
Establecer controles para los riesgos encontrados en la dependencia de admisiones registro y control en los niveles medio y alto según la norma ISO 27005.	Clasificar los controles correspondientes a cada riesgo tratado.	Tabla de controles establecidos.

Fuente: Autor del proyecto

4.1 PRIMER OBJETIVO ESPECÍFICO

Diagnosticar la situación actual para la identificación de riesgos de la oficina de Admisiones, Registro y Control.

Actividades para el cumplimiento del objetivo

- ✓ Recopilar información utilizando como instrumentos de recolección la entrevista, análisis de material documental de la dependencia y observación.
- ✓ Analizar los factores de riesgo de la información suministrada en la recopilación de información.

Realizada la etapa de reconocimiento de la oficina de Admisiones, Registro y Control, se procede a aplicar como herramienta de recolección de información la entrevista lo que permite documentar de manera inicial datos valiosos, que brindan una serie de aportes fundamentales en la realización de la investigación.

De igual manera se realiza un análisis de la matriz de riesgo que en la actualidad maneja la dependencia, suministrando un aporte importante al trabajo que se hizo.

A continuación se describe la información detallada de hallazgos encontrados.

Tabla 2. Hallazgos encontrados

RESULTADO DEL ANALISIS DE LA INFORMACIÓN RECOPILADA		
ORGANIZACIÓN Y SEGURIDAD DE LA INFORMACIÓN		
Organización Interna		
Objetivo:	Gestionar la seguridad de la información y su organización dentro de la Organización.	
	Organización de archivo activo o de consulta	La oficina de admisiones cuenta con una organización inadecuada del archivo activo debido a que no cuenta con archivadores para la seguridad y organización de la misma.
GESTIÓN DE ACTIVOS		
Clasificación de la información		
Objetivo:	Asegurar que la información recibe el nivel de protección adecuado.	

	Etiquetado y manejo de información	Debido a la organización actual del archivo activo o de consulta, se realiza de manera manual, no siendo óptimo el proceso realizado.
GESTIÓN DE INCIDENTES DE LA SEGURIDAD DE LA INFORMACIÓN		
Reporte sobre los eventos y las debilidades de la seguridad de la información		
Objetivo:	Asegurar que los eventos y las debilidades de la seguridad de la información asociados con los sistemas de información se comunican de forma tal que permiten tomar las acciones correctivas oportunamente.	
	Reporte sobre los eventos de seguridad de la información	Según la forma actual de manejo y búsqueda de información en archivo activo, se hace imposible garantizar los reportes de anomalías o pérdida de información.
SEGURIDAD FISICA Y DEL ENTORNO		
Áreas seguras		
Objetivo:	Evitar el acceso físico no autorizado, el daño e interferencia a las instalaciones y a la información de la organización.	
	Controles de acceso físico.	Las áreas de la dependencia no son seguras puesto que no están protegidas con controles de acceso apropiados.
CONTROL DE ACCESO		
Control de acceso a equipos		
Objetivo:	Asegurar el acceso de usuarios autorizados y evitar el acceso de usuarios no autorizados a los sistemas de información.	
	Gestión de contraseñas para usuarios.	La asignación de contraseñas se debe realizar a través de un proceso formal de gestión ya que en la actualidad los equipos no cuentan en su totalidad con este tipo de restricción.

Fuente: Autor del proyecto

4.2 SEGUNDO OBJETIVO ESPECÍFICO

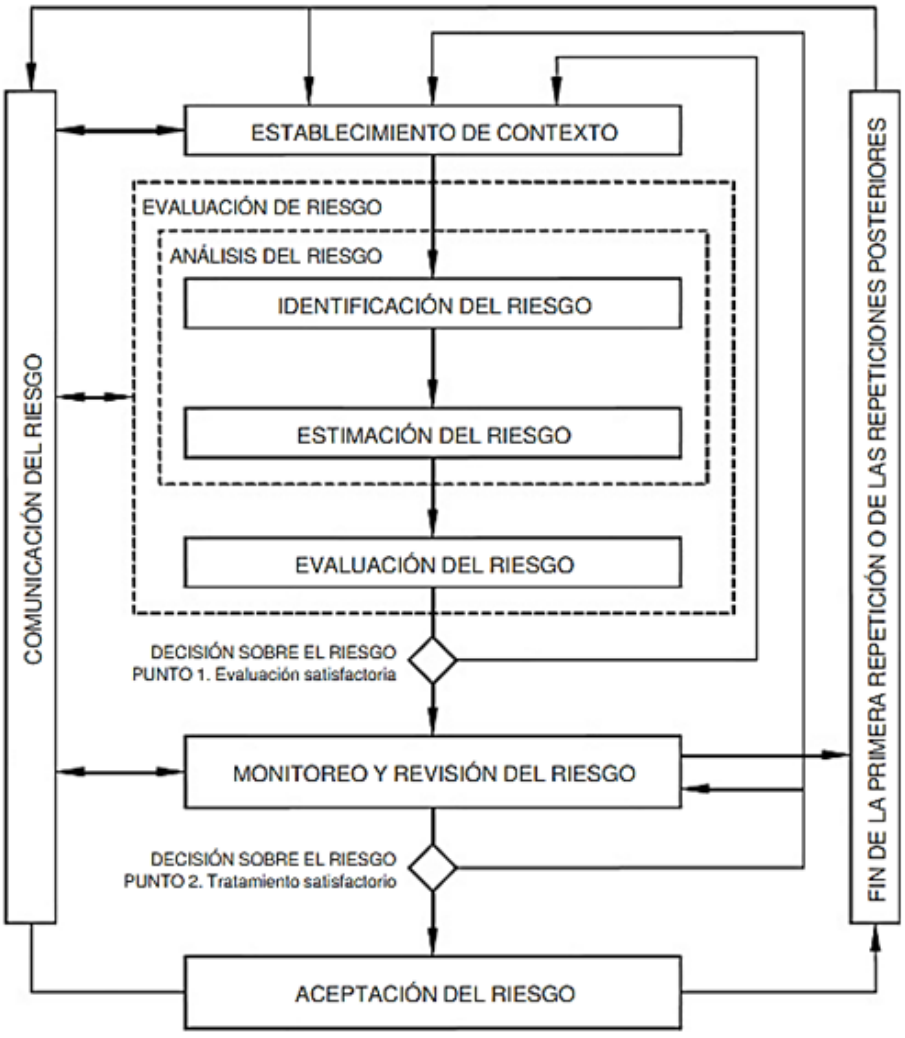
Identificar y evaluar los riesgos de la dependencia basado en la norma ISO 27005:2009

Actividades para el cumplimiento del objetivo

- ✓ Estudiar la norma ISO 27005:2009 contemplando su estructura para la aplicación de la misma.
- ✓ Clasificar y evaluar los riegos acorde a las actividades del proceso de gestión de riesgo de la seguridad de la información.

Estudiada la norma ISO 27005:2009, nos permite enfocar la ejecución de la norma mostrando una visión general del proceso de Gestión del riesgo en la seguridad de la información.

Figura 1. Proceso de gestión del riesgo en la seguridad de la información



Fuente: Norma ISO 27005

Como primera parte del proceso se realizó un establecimiento del contexto de la organización, donde se recolecta información de la empresa para determinar el ambiente en que funciona.

Presentación de la organización. La Oficina de Admisiones, Registro y Control es la dependencia de la Subdirección Académica encargada de llevar, 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 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.

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
- La honradez.

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

Servicios y procesos de la dependencia. Los servicios y procesos que se llevan a cabo en la oficina se describen a continuación:

- Instructivo proceso de inscripción
- Proceso de matrícula alumnos nuevos
- Proceso de matrícula alumnos antiguos
- Solicitud de financiación de matrícula financiera
- Selección de aspirantes
- Brindar información en cuanto a requisitos para traslado de un plan de estudios a otro, así mismo transferencia de otra universidad a la seccional de Ocaña.

Realizado el reconocimiento de la organización mediante el proceso de establecimiento del contexto, procedemos a realizar la valoración de los riesgos que comprende lo siguiente.

- Análisis del riesgo
    - Identificación del riesgo
    - Estimación del riesgo
- Evaluación del riesgo

Los datos contemplados en la siguiente tabla describe el ejercicio realizado.

Tabla 3. Identificación de riesgos

IDENTIFICACIÓN DEL RIESGO				
Identif. de activos		Identif. de amenazas	Identif. de Vulnerabilidades	Identif. de Consecuencias
Procesos realizados	El archivo de la dependencia no cuenta con las condiciones fisicas y de seguridad requeridas para el almacenamiento de los expedientes académicos.	Hurto de documentos Pérdida de información	Susceptibilidad a la humedad, el polvo y la suciedad Almacenamiento sin protección	Congestión en los procedimientos Pérdida o alteración de los expedientes académicos
	Deterioro de los expedientes académicos	Conato de Incendio	Ausencia de copias de respaldo de la información	Daño parcial o total de los archivos contenidos en los expedientes académicos.
	Las instalaciones de la oficina de Admisiones, Registro y Control no cuentan con un espacio de trabajo amplio que garantice una buena atención al público.	Hurto de medios o documentos	Perturbación en las labores realizadas	Bajo rendimiento en atención al usuario
	Hacinamiento de funcionarios	Saturación de procesos y labores	Manejo indebido de equipos de computo	Perdida de información Alteración de procesos realizados Daños informáticos posturas ergonómicas inadecuadas

	Incumplimiento del calendario académico, debido a inconsistencias en los procedimientos de inscripción, admisión y matricula de aspirantes inscritos.	Abuso de los derechos	Falta o insuficiencia de la prueba de software	Insatisfacción del cliente Congestión en los procedimientos Interrupción de la actividad
hardware	Equipos de cómputo Impresoras Teléfonos	Polvo, Corrosión o Congelamiento Hurto de medios	Susceptibilidad a la humedad, el polvo y la suciedad Almacenamiento sin protección	Deterioro en el desempeño del negocio Pérdida del buen nombre Pérdida financiera Incapacidad para prestar el servicio Perdida en la credibilidad de sistema de información interno Alteración de la operación interna Alteración en la propia organización Costo interno adicional Alteración de las terceras partes que tienen transacciones con la organización Peligro para el personal de la organización y los usuarios Costo financiero para pérdidas o reparaciones Despidos Daños materiales
Software	Sistemas operativos Sistema de información académico	Manipulación con software Copia fraudulenta del software Corrupción de datos	Falta de copias de respaldo Descarga y uso no controlado de software	
Redes	Red de voz Red de datos	Escucha subrepticia Falla del equipo de telecomunicaciones Espionaje remoto	Líneas de comunicación sin protección conexión deficiente de los cables Arquitectura insegura de la red	
Personal	Funcionarios de la entidad	Incumplimiento en la d isponibilidad del personal Destrucción de equipos o medios Error de uso Hurto de medios o documentos	Ausencia del personal Procedimientos inadecuados de contratación Uso incorrecto de software y hardware Trabajo no supervisado del personal externo o de limpieza	

Planta física	Oficina	Destrucción de equipo o medios hurto de equipo Inundación	Uso inadecuado o descuidado o del control de acceso físico a las edificaciones y los recintos Falta de protección física de las puertas y ventanas de la edificación Ubicación en un área susceptible de inundación	

Fuente: Autor del proyecto

Así mismo se procede a realizar la evaluación de los riesgos encontrados

Tabla 4. Evaluación del riesgo

IDENTIFICACIÓN DEL RIESGO		Evaluación del Riesgo			
Identif. de activos		Probabilidad	impacto	Valoración del Riesgo	Tipo de Riesgo
Procesos realizados	El archivo de la dependencia no cuenta con las condiciones físicas y de seguridad requeridas para el almacenamiento de los expedientes académicos.	5	4	20	Importante
	Deterioro de los expedientes académicos	3	3	9	Moderado
	Las instalaciones de la oficina de Admisiones, Registro y Control no cuenta con un espacio de trabajo amplio que garantice una buena atención al público.	3	2	6	Tolerable

	Hacinamiento de funcionarios	4	2	8	Moderado
	Incumplimiento del calendario académico, debido a inconsistencias en los procedimientos de inscripción, admisión y matricula de aspirantes inscritos.	3	3	9	Moderado
hardware	Equipos de cómputo Impresoras Teléfonos	3	1	3	Aceptable
Software	Sistemas operativos Sistema de información académico	3	2	6	Tolerable
Redes	Red de voz Red de datos	3	1	3	Aceptable
Personal	Funcionarios de la entidad	2	1	2	Aceptable
Planta física	Oficina	3	2	6	Tolerable

Fuente: Autor del proyecto

4.3 TERCER OBJETIVO ESPECÍFICO

Establecer controles para los riesgos encontrados en la dependencia de admisiones registro y control en los niveles medio y alto según la norma ISO 27005.

Actividades para el cumplimiento del objetivo

- ✓ Clasificar los controles correspondientes a cada riesgo tratado.

Los datos contemplados en la siguiente tabla describe el ejercicio realizado.

Tabla 5. Controles por riesgo

Identif. de activos		Identif. de Consecuencias	Identif. de Controles
Procesos realizados	El archivo de la dependencia no cuenta con las condiciones físicas y de seguridad requeridas para el almacenamiento de los expedientes académicos.	Congestión en los procedimientos Pérdida o alteración de los expedientes académicos	Establecer tablas de retención documental que permitan organizar la información física en un lugar seguro, permitiendo tener la información sistematizada y organizada.
	Deterioro de los expedientes académicos	Daño parcial o total de los archivos contenidos en los expedientes académicos.	Avanzar en la sistematización de la línea base de la información con personal de Beca trabajo de los diferentes programas académicos y/o alianzas con instituciones educativas de carácter técnico comercial.
	Las instalaciones de la oficina de Admisiones, Registro y Control no cuenta con un espacio de trabajo amplio que garantice una buena atención al público.	Bajo rendimiento en atención al usuario	Solicitar a la oficina de planeación la ampliación de las instalaciones de la oficina de Admisiones, registro y Control.

	Hacinamiento de funcionarios	Perdida de información Alteración de procesos realizados Daños informáticos posturas ergonómicas inadecuadas	Solicitar a la oficina de planeación la ampliación de las instalaciones de la oficina de Admisiones, registro y Control.
	Incumplimiento del calendario académico, debido a inconsistencias en los procedimientos de inscripción, admisión y matricula de aspirantes inscritos.	Insatisfacción del cliente Congestión en los procedimientos Interrupción de la actividad	Realizar pruebas de saturación y funcionamiento al sistema semanas antes de iniciar los procesos de inscripción, admisión y matricula.
hardware	Equipos de cómputo Impresoras Teléfonos	Deterioro en el desempeño del negocio Pérdida del buen nombre Pérdida financiera Incapacidad para prestar el servicio Perdida en la credibilidad de sistema de información interno Alteración de la operación interna Alteración en la propia organización Costo interno adicional Alteración de las terceras partes que tienen transacciones con la organización Peligro para el personal de la organización y los usuarios Costo financiero para pérdidas o reparaciones Despidos Daños materiales	
Software	Sistemas operativos Sistema de información académico		Realizar copias de seguridad con tareas programadas de manera periódica.
Redes	Red de voz Red de datos		
Personal	Funcionarios de la entidad		
Planta física	Oficina		Establecer Políticas de acceso al personal de la dependencia Admisiones, Registro y Control con el fin de tener control de entrada y salida exclusiva para los funcionarios que ahí laboran.

Fuente: Autor del proyecto

CONCLUSIONES

Para el diseño de la presente 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, lo cual arrojó insumos valiosos para el análisis correspondiente a la gestión de riesgo de la información.

Se realizó un análisis a los factores de riesgo de la información suministrada en la recopilación de información, permitiendo identificar falencias en la organización del archivo activo, así como también un manejo inadecuado de búsqueda de registros y folios académicos.

Esta indagación brindó soporte fundamental para el proceso de análisis, identificación y aplicación de las normas ISO 27005/2009, donde se establece una serie de procesos que permitió realizar un trabajo enfocado en la mejora de los procesos de la dependencia Admisiones Registro y Control de la Universidad Francisco de Paula Santander Ocaña.

Se logró realizar una gestión detallada de riesgos, identificando y clasificando según el tipo de activo cada una de las amenazas, consecuencias y respectivos controles que permitan reducir el riesgo hasta su nivel de aceptación, permitiendo así minimizar la posibilidad que se consolide algún accidente que llegue afectar algún tipo de proceso en la dependencia.

Con el diseño de la presente gestión de riesgos de la información se establece 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.

BIBLIOGRAFÍA

NTC/ISO 27005 GESTIÓN DEL RIESGO. Principios y Directrices [Libro]. - Bogotá: ICONTEC, 2008.

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

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

FUENTES ELECTRÓNICAS

CONGRESO DE LA REPUBLICA COLOMBIANA. LEY 1273 DE 2009. [En línea]. Disponible en Internet: <http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html> [con acceso el 08-09-2015]

ADMINISTRACIÓN DE RIESGOS. Modelo instrumental para el tratamiento integral y la gestión apropiada de los riesgos en la universidad del valle. [En línea]. Disponible en Internet: <http://secretariageneral.univalle.edu.co/rectoria/resoluciones/2014/MITIGAR%20U.V.%20feb-2014.pdf> [con acceso el 31-08-2015]

UNIVERSIDAD DISTRITAL FRANCISCO JOSÉ DE CALDAS. Política para la seguridad de la información de la universidad distrital Francisco José de Caldas. [En línea]. Disponible desde Internet en: <http://portalws.udistrital.edu.co/CIT/documentos/NORMATIVIDAD/politica_seguridad/archivos/Politica_para_Seguridad_Informacion_Version_0.0.1.0.pdf>[con acceso el 12-09-2015]

POLITICA DE SEGURIDAD FÍSICA. SISTESEG. [En línea]. Disponible desde Internet en: <http://www.sisteseg.com/files/Microsoft_Word_-_Politica_Seguridad_Fisica.pdf>[con acceso el 12-09-2015]

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

ELEJALDE ALVAREZ, Olga Lucía: Noviembre 2009. La gestión del riesgo: una estrategia de administración integral. [En línea]. Disponible en Internet: <http://www.lasallista.edu.co/fxcul/media/pdf/RevistaLimpia/Vol4n2/103-112.pdf> [con acceso el 01-09-2015]

CONGRESO DE LA REPUBLICA COLOMBIANA. LEY 1273 DE 2009 (enero 5). [En línea]. Disponible desde Internet en: <http://www.secretariasenado.gov.co/senado/basedoc/ley/2009/ley_1273_2009.html> [con acceso el 15-09-2015]