RESUMEN – TRABAJO DE GRADO

AUTORES	**MILSEN SANCHEZ ARIAS**
FACULTAD	**FACULTAD DE INGENIERIAS**
PLAN DE ESTUDIOS	**ESPECIALIZACION EN AUDITORIA DE SISTEMAS**
DIRECTOR	**TORCOROMA VELASQUEZ PEREZ**
TÍTULO DE LA TESIS	**ANALISIS DE RIESGO DE LA INFORMACIÓN DEL PROGRAMA DE EGRESADOS DE LA UNIVERSIDAD POPULAR DEL CESAR SECCIONAL AGUACHICA**

RESUMEN
(70 palabras aproximadamente)

POR MEDIO DEL ANÁLISIS DE RIESGOS REALIZADO EN EL PROGRAMA DE EGRESADOS DE LA UNIVERSIDAD POPULAR DEL CESAR SECCIONAL AGUACHICA, SE PUDO IDENTIFICAR QUE EL NIVEL DE RIESGO PARA LA INFORMACIÓN ES ALTO. ESTE MISMO ANÁLISIS, PERMITIÓ EVALUAR QUE SE DEBE TOMAR MEDIDAS DE REDUCCIÓN, ELIMINACIÓN O TRANSFERENCIA DEL RIESGO.

CARACTERÍSTICAS

PÁGINAS:	PLANOS:	ILUSTRACIONES:	CD-ROM:

ANALISIS DE RIESGO DE LA INFORMACIÓN DEL PROGRAMA DE EGRESADOS DE LA UNIVERSIDAD POPULAR DEL CESAR SECCIONAL AGUACHICA

AUTORA

MILSEN SANCHEZ ARIAS

Trabajo de grado presentado para obtener el título de especialista en auditoria de sistemas

DIRECTORA

PhD. TORCOROMA VELASQUEZ PEREZ

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERIAS

ESPECIALIZACION EN AUDITORIA DE SISTEMAS

Ocaña, Colombia **Octubre, 2017**

Dedicatoria

Mi trabajo de grado está dedicada Dios quien guía el camino de mi vida a mi esposo Ariel Contreras Orte, mis hijos Esneider y Sebastian Contreras Sanchez

Agradecimientos

*Agradezo la ayuda incondicional para el logro de mis objetivos a mi directora la Docente Torcoroma Velasque Perez***.**

Índice

Lista de Figuras

Lista de Ilustraciones

Lista de Tablas

Introducción

En Colombia y en el mundo, las universidades están llamadas a ser referentes de buenas prácticas sobre el manejo de la información, puesto que ésta es su principal materia prima, es así que en el sistema de educación superior colombiano existen cuatro sistemas de información para consolidar una estructura robusta, que permita su gestión y articulación en las diferentes etapas de los procesos. Actualmente el Programa de Egresados de la Universidad Popular del Cesar Seccional Aguachica quien es el principal proveedor de información del sistema Observatorio Laboral para la Educación (OLE), no cuenta con estudios, ni análisis, para identificar y evaluar el nivel de riesgo de su información. Es decir la información producida y reportada por el Programa de Egresados se encuentra vulnerable, pues no existen análisis para detectar sus amenazas.

La presente investigación tiene como objetivo evaluar el nivel de riesgo de la información del programa de egresados de la Universidad Popular del Cesar Seccional Aguachica, con el fin de generar controles para su buena gestión, por medio de la construcción de un análisis de riesgos fundamentado en las normas internacionales ISO 27000 e ISO 27005, así como en las guías técnicas proporcionadas por el MINTIC para el tema de la seguridad de la información.

Capítulo 1. Análisis de riesgo de la información del programa de egresados de la Universidad Popular del Cesar seccional Aguachica

1.1 Planteamiento del problema

En Colombia y en el mundo, las universidades están llamadas a ser referentes de buenas prácticas sobre el manejo de la información, puesto que ésta es su principal materia prima, es así que en el sistema de educación superior colombiano existen cuatro sistemas de información para consolidar una estructura robusta, que permita su gestión y articulación en las diferentes etapas de los procesos. Dentro de estos sistemas encontramos:

Sistema Nacional de Información de Educación Superior (SNIES), el cual ofrece datos confiables sobre las instituciones de educación superior en Colombia y los programas que ofrecen; En este sistema se recopila y organiza la información relevante sobre la educación superior que permite hacer planeación, monitoreo, evaluación, asesoría, inspección y vigilancia del sector (Ministerio de Educación Nacional, 2017)

Observatorio Laboral para la Educación, que ofrece un seguimiento permanente de los graduados de la Educación Superior en Colombia. Reúne una variedad de datos para interpretar las relaciones entre el mundo de la educación superior y el mundo laboral. Ha sido concebido para orientar, de manera más acertada, políticas de educación pertinencia y mejoramiento de la calidad de los programas y decisiones de los estudiantes frente a los estudios a seguir; Ofrece información estadística sobre el nivel de formación académica de los egresados, sus aportes a seguridad social y los salarios promedio de enganche que reciben. Además, entrega un panorama sobre cuánto tiempo les toma conseguir empleo, las ciudades en las que trabajan y la demanda de

egresados que tienen en el mercado laboral una mayor o menor acogida (Ministerio de Educación Nacional, 2017)

Sistema de Información para el Aseguramiento de la Calidad (SACES), el cual contiene información para el proceso de Registro Calificado de programas académicos; En el sistema SACES se deja el registro de cada una de las actividades cumplidas en cada uno de los procesos, hasta su culminación con la emisión del acto administrativo correspondiente que otorga o niega la solicitud presentada por las IES, por lo tanto, el seguimiento y la generación de reportes sobre los avances, estados, finalización etc. Se pueden extraer del sistema SACES (Ministerio de Educación Nacional, 2017)

Sistema de Prevención y Análisis de la Deserción en las Instituciones de Educación Superior (SPADIES), que permite el seguimiento a cada estudiante para calcular el riesgo de la deserción y prevenirlo; El SPADIES, hace parte del Sistema Nacional de Información de la Educación Superior ―SNIES― y puede entenderse como un módulo particular de este último aplicado al seguimiento especializado de un fenómeno de especial interés del sector como lo es la deserción estudiantil (Ministerio de Educación Nacional, 2017)

Sin embargo, el registro de la información en estos sistemas lo hacen directamente las universidades, es decir, sus fuentes de información son las Instituciones de Educación Superior, donde cada una reporta y da fe sobre que la información registrada es veraz y confiable; pero a su vez el Ministerio de Educación Superior (MEN) no cuenta con herramientas inmediatas para la verificacion de dicha informacion sino que lo hace a posteriori por medio de las visitas de renovacion o auditorias anuales, por lo que sin un previo control los sistemas de información son vulnerables a registros no veraces.

Se puede inferir, que estos sistemas de información abarcan todas las actividades de la educación superior desde el registro de programas académicos hasta el seguimiento a sus egresados. Estos últimos son finalmente el producto o salida de todas los procesos, es decir una universidad existe para que existan sus egresados, por lo que se convierte en la salida del proceso y en ultimas en el más importante de los sistemas de información de educación superior. De acuerdo con (Ministerio de Educación Superior, 2013).

Los egresados constituyen el principal fruto de la educación superior, ya que por su intermedio y con su desempeño, la institución y sus programas influyen en el entorno, con lo cual se pueden valorar la pertinencia laboral y el impacto social de su formación; además, en la interacción del egresado con otras personas y grupos, la IES lleva a la sociedad su modelo de valores. Adicionalmente, la IES se enriquece con los aportes de sus egresados los cuales le permiten hacer ajustes a los perfiles, actualizar el currículo y estar articulados con las necesidades del sector laboral y profesional, entre otros.

Actualmente el Programa de Egresados de la Universidad Popular del Cesar Seccional Aguachica quien es el principal proveedor de información del sistema Observatorio Laboral para la Educación (OLE), no cuenta con estudios, ni análisis, para identificar y evaluar el nivel de riesgo de su información. Es decir la información producida y reportada por el Programa de Egresados se encuentra vulnerable, pues no existen análisis para detectar sus amenazas.

1.2 Formulación del Problema

¿Cuál es el nivel de riesgo de la Información del Programa de Egresados de la Universidad Popular del Cesar Seccional Aguachica?

1.3 Objetivos

1.3.1 General. Evaluar el nivel de riesgo de la información del programa de egresados de la Universidad Popular del Cesar Seccional Aguachica, con el fin de generar controles para su buena gestión.

1.3.2 Específicos.

Identificar los riesgos de los activos de la información del programa de egresados de la Universidad Popular del Cesar Seccional Aguachica

Determinar los impactos y las probabilidades de los riesgos de la información del programa de egresados de la Universidad Popular del Cesar Seccional Aguachica

Establecer los posibles controles para la mitigación de los riesgos de la información del programa de egresados de la Universidad Popular del Cesar Seccional Aguachica

1.4 Justificación

En la actualidad el principal activo de las empresas y las organizaciones se centra en la Información, de acuerdo a (Nepomuceno, Quesada, & Francisco, 2001):

> El concepto de información es un concepto fundamental de la cibernética, ciencia que estudia las máquinas y los seres vivos desde el punto de vista de su capacidad para percibir y conservar información, transformarla en señales y trasmitirlas por canales de comunicación de manera que cumplan un fin de terminado.

Con esta premisa, todo lo que ocurre dentro de las organizaciones, tanto económicamente como en el desarrollo de sus procesos depende de la manera en que gestionen su información, es decir que a partir de ésta, se cumpla la misión de la organización. Es así que es imprescindible establecer herramientas más eficaces para la protección, seguridad y buen uso de la información

como entrada y salida de todos los procesos organizacionales. En búsqueda de implementar herramientas más eficaces para dicha gestión, las organizaciones están llamadas a gestionar su información de acuerdo a los estándares nacionales e internacionales y efectuar seguimientos y monitoreo de las mismas.

En el Sistema de Educación Superior en Colombia, realiza seguimiento a sus procesos por medio de diferentes herramientas tanto tecnológicas como metodológicas, es por esto que es tan importante enfocarse en el tipo de información que se está entregando por parte de las Universidades puesto que los indicadores resultantes de su procesamiento son la principal fuente para la toma de decisiones respecto a el cumplimiento de requisitos, mejoras en el sistema, valoraciones de programas y universidades.

Una de las principales fuentes de información para la verificación de que las Universidades cono IES están cumpliendo con su misión y objetivos de formación, investigación y extensión son los EGRESADOS por lo que "en este sentido refleja en la sociedad la calidad del programa y de la institución que lo tituló" (Ministerio de Educación Superior, 2013). Para llevar el registro de información de los Egresados en Colombia el MEN dispuso de la herramienta Observatorio Laboral para la Educación (OLE), con el cual busca interpretar las relaciones entre el mundo de la educación superior y el mundo laboral. Cada Universidad debe realizar un seguimiento interno a sus egresados para luego reportarlo en el OLE.

Este seguimiento interno se realiza por medio de las unidades conocidas como PROGRAMA DE EGRESADOS, estas unidades deben consolidar de manera general como mínimo: Documentos con las políticas institucionales para valorar los egresados que incluyan estrategias de seguimiento en el corto y mediano plazo. Deben permitir conocer su desempeño y

el impacto social de los programas, Estrategias previstas para la vinculación de los egresados para favorecer el mejoramiento y la actualización de los programas, Programas de intermediación laboral de la IES para sus egresados, Existencia de bases de datos con información sobre egresados de la IES, Evidencia de relaciones de la IES con empleadores de sus egresados, Evidencias de actividades que vinculen a los egresados con la IES o a los programas de los que se graduaron, Información estadística sobre actividades y tipos de programas para los egresados de la institución, entre otros.

Ya que toda esta información consolida el desempeño final de las IES, se convierte en un activo muy importante para las mismas, pues representa la valoración de los impactos sociales de la institución. Realizar un seguimiento y control a la calidad de esta información garantiza entonces evidenciar de manera veraz los logros de los programas y las instituciones, así como el posicionamiento de los egresados y amplía la oportunidad para el mejoramiento de los mismos, ya que con información confiable sobre sus egresados se pueden "*hacer ajustes a los perfiles, actualizar el currículo y estar articulados con las necesidades del sector laboral y profesional"* (Ministerio de Educación Superior, 2013)

Asi mismo, el analisis de riesgos se justifica desde la norma internacional ISO/IEC 27005, que exhorta sobre la importancia de la gestión de riesgos en la información, y establece los procedimientos para, sino garantizar, establecer de la mejor manera los controles ante las necesidades de evaluación de riesgos.

La importancia de este tipo de análisis de riesgos sobre la información del programa de egresados, también radica en la naturaleza de dicha información, pues en su mayoría son datos

personales y académicos de los egresados, lo que implica un buen manejo de los mismos, en el uso, publicación y conservación.

1.5 Hipótesis

El análisis de riesgos de la información del programa de egresados de la Universidad Popular del Cesar Seccional Aguachica, identifica los riesgos de los activos de la información, determina los impactos y las probabilidades de los riesgos y establece los posibles controles para su mitigación

1.6 Delimitaciones

1.6.1 Delimitación Operativa.

Se delimita la operación del proyecto los procesos del Programa de Egresados de la Universidad Popular del Cesar Seccional Aguachica

1.6.2 Delimitación Conceptual.

Se delimita la conceptualización del proyecto al Análisis de Riesgos de la Información

1.6.3 Delimitación Geográfica.

Se delimita la implementación del proyecto a la Seccional de la Universidad Popular del Cesar ubicada en Aguachica Cesar

1.6.4 Delimitación Temporal.

Se delimita el análisis de información de los años 2012 a 2016 del Programa de Egresados de la Universidad Popular del Cesar Seccional Aguachica

Capítulo 2. Marco Referencial

2.1 Marco Histórico

El activo más importante para una organización es la Información, muchos autores concuerdan que en la sociedad globalizada la información debe considerarse además que un recurso como un proceso.

> La información en la gestión empresarial moderna no puede ser considerada como un mero apoyo o soporte de las actividades operativas de la empresa, sino que debe tratarse como uno de sus principales recursos o activos. La información es un elemento imprescindible para el funcionamiento de las organizaciones, un recursos básico e importante que requiere por tanto que se le apliquen las tradicionales técnicas de gestión de recursos, es decir planificación, organización, dirección y control. (De Pablos Heredero, 2006, pág. 32)

A raíz de esto, las organizaciones han procurado iniciar la tarea de gestionar su información desde su producción, por lo que para ello requiere que la misma cuente con la seguridad respectiva. A nivel histórico la seguridad de la información nace en el Reino Unido, con la fundación del Centro de Seguridad de Informática para el Comercio (CCSC - Comercial Computer Security Centre) por parte del Departamento de Comercio e Industria del Reino Unido (DTI - Departamento of Tarde and Industria).

El trabajo realizado en este centro dio origen a la normativa más moderna para gestionar la seguridad de la información conocida como ISO 27000 y su familia. El blog (seguridad27000, 2013) presenta la historia de esta norma así:

> El Centro de Seguridad de Informática para el Comercio (CCSC - Comercial Computer Security Centre) por parte del Departamento de Comercio e Industria del Reino Unido (DTI - Department of Trade and Industry) se crea con el objetivo de cubrir dos tareas fundamentales.

- Apoyar a los vendedores de productos de seguridad de TI a establecer un criterio de evaluación de la seguridad de la información que fuera mundialmente reconocido y aceptado, mediante un esquema de certificación y evaluación.
- El segundo, fue apoyar a los usuarios mediante el denominado "Código de prácticas para los usuarios" que se publicó en 1989.

En 1993 se publicó la guía Británica conocida como PD0003 como resultado de las revisiones del código, y con el nombre de "Código de prácticas para la gestión de la seguridad de la información". En 1995, se rebautizaría como estándar británico o BS 7799.

A causa de su buena acogida, y acorde a las crecientes necesidades de la industria, provocó en 1998 la publicación de una segunda parte denominada BS 7799-2 que llego a complementar aspectos no contemplados en el BS 7799, principalmente el ciclo de mejora continua.

Luego en abril de 1999 se publican la revisión de las dos partes en su conjunto (BS 7799 y BS 7799-2), bajo la nomenclatura BS7799-1:1999 y BS7799-2:1999 respectivamente.

La necesidad de los países, especialmente en los industrializados por disponer de estándares de este tipo, fue tal que, provoca que la primera parte del estándar denominado BS7799-1:1999 se proponga en octubre de 1999 como norma internacional aprobada por la Organización Internacional de Estandarización (ISO) y por la Comisión Electrotécnica Internacional (IEC).

La principal función de ambos organismos (ISO e IEC) es la de buscar la estandarización de normas de productos y seguridad para las empresas u organizaciones a nivel internacional.

Después de leves modificaciones, el 1 de diciembre del 2000 se publica la norma internacional ISO/IEC 17799:2000 que desde ese momento sustituirá al estándar Británico BS 7799-1:1999.
En su época, recibía críticas ya que la norma sólo indicaba como construir un SGSI siguiendo el ciclo de deming, pero carecía de las instrucciones necesarias para saber cómo utilizarlo, mantenerlo y mejorarlo.

> Tras la revisión de la norma BS7799-2, se publicó la norma BS7799-2:2002 el cual reflejaba a través del modelo PDCA, los principios recientemente establecidos en la guía de la OCDE (Organización para la Cooperación y el Desarrollo Económico).
>
> El 14 de octubre de 2005, el estándar BS 7799-2 queda sustituido finalmente con la aprobación y publicación del estándar internacional ISO/IEC 27001:2005, junto a la reserva de la numeración 27000 para la publicación en el futuro de toda la serie de estándares relacionado con la seguridad de la información.
>
> Se publica el ISO/IEC 27002:2005 con el objetivo de una mejor comprensión en su relación con el ISO/IEC 27001 y la posterior serie de estándares que se han ido publicado bajo la serie 27000.

La gestión del riesgo de la información aparece de forma explícita en la norma ISO/IEC 27005, publicada por primera vez en 2008 y cuya segunda edición apareció en Junio de 2011.

> Proporciona directrices para la gestión del riesgo en la seguridad de la información. Apoya los conceptos generales especificados en la norma ISO/IEC 27001:2005 y está diseñada para ayudar a la aplicación satisfactoria de la seguridad de la información basada en un enfoque de gestión de riesgos. Su primera publicación revisó y retiró las normas ISO/IEC TR 13335-3:1998 e ISO/IEC TR 13335-4:2000. (iso27000.es, 2005)

La generación de estas normas y su trazabilidad en el tiempo dan cuenta de cómo ha sido el proceso para definir e identificar los procesos asociados a la información, en cuanto a seguridad y ha evaluación y gestión del riesgo.

Antecedentes

Para el caso de estudio, es importante tener en cuenta los precedentes investigativos asociados a la evaluación o análisis de riesgos de la información, con el fin de proporcionar un marco de antecedentes históricos y contar con referencias tanto conceptuales como teóricas.

Un primer caso corresponde a (Del Carpio Gallego, 2006) quien realizó el estudio "Análisis del riesgo en la administración de proyectos de tecnología de información", en esté, se presenta una propuesta para que los gerentes de proyectos de tecnología de información cuenten con una metodología que les permita proponer un plan para enfrentar los riesgos y de esta manera tener una mayor probabilidad de éxito, como conclusión se establece que los gerentes de proyectos de tecnología de información deberían dedicar más recursos a la generación de un plan coherente para identificar y enfrentar adecuadamente los riesgos.

Este estudio se relaciona con la investigación en curso, pues presenta un proceso sistemático para la administración de los riesgos.

Un segundo caso lo presenta (De Freitas, 2009), con su estudio "Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar". En este trabajo se propone conocer las fortalezas y debilidades a las que pudieran estar sometidos los activos de información que están en custodia en la Dirección de Servicios Telemáticos (DST) de la Universidad Simón Bolívar ubicada en Caracas, Venezuela, con el fin de sugerir estrategias que minimicen la ocurrencia de posibles amenazas que en la mayoría de los casos explotan las vulnerabilidades organizacionales. Basado en una metodología de estudio de caso, este estudio permitió recoger información detallada usando una variedad de sistemas de recolección de datos, como entrevistas semi-estructuradas, estructuradas y en profundidad, revisión bibliográfica y arqueo de fuentes. Igualmente, se realizaron visitas a las instalaciones de la dirección evaluada y se revisaron aspectos de seguridad física previstos en las Normas ISO-27001:2007. Se concluye que cada uno de los elementos en custodia de la DST es de suma importancia para la

Universidad Simón Bolívar, por lo que se sugiere la aplicación de algunos controles establecidos en las normas ISO, para cada uno de dichos activos.

Esta investigación se relaciona de manera directa con la investigación en curso, pues la información analizada corresponde con información asociada a la Educación Superior, adicionalmente establece una metodología de estudio clara para la recolección de datos.

Para ampliar el análisis y abordar también la información digital, (Merchán Paredes & Gómez Mosquera, 2011) realizaron el estudio "Validación de un método ágil para el análisis de riesgos de la información digital", aquí se plantea que frecuentemente se observa en las pequeñas empresas de tecnología la carencia de una cultura de análisis de riesgo para los activos digitales; en gran medida, debido al alto costo de la implementación de métodos conocidos que requieren compromisos en tiempo y esfuerzo que muchas veces superan la capacidad empresarial. Por ello se diseñó y validó un método que de manera ágil permite a las pequeñas empresas implantar el análisis de riesgo de la información digital en sus procesos. El método evita la destinación excesiva de recursos que es característica de los métodos y metodologías tradicionales. El método y su herramienta informática se aplicaron y validaron en cinco empresas con características diferentes. Los resultados fueron satisfactorios, como lo reflejan los indicadores de productividad, eficiencia y efectividad desarrollados para evaluar el diseño experimental aplicado.

Esta investigación se relaciona con la investigación en curso, pues aborda una aproximación asía la pequeña empresa, indicadores de riesgo medidos y un modelo de análisis.

Finalmente se consideró el estudio de (Abril, Pulido, & Bohada, 2013) con su estudio denominado "Análisis De Riesgos En Seguridad De La Información", este artículo se enfoca en exponer algunas opciones y permitir generar argumentos sólidos para identificar cuál es la metodología de análisis de riesgos que proporciona una mejor oportunidad de toma de decisiones dentro de una organización frente a la custodia de la información, la cual se ha convertido en uno de los activos más importantes del ámbito empresarial e implica una adecuada utilización y preservación para garantizar la seguridad y la continuidad del negocio.

Esta investigación se relaciona con la investigación en curso, pues plantea diferentes metodologías, que de manera técnica se pueden implantar en las empresas para la gestión del riesgo de la información.

2.2 Marco conceptual

- Aceptación del riesgo: decisión de asumir un riesgo. [Guía ISO/IEC 73:2002]
- Activo: cualquier cosa que tiene valor para la organización. [NTC 5411-1:2006]
- Análisis de riesgo uso sistemático de la información para identificar las fuentes y estimar el riesgo. [Guía ISO/IEC 73:2002]
- Confidencialidad: propiedad que determina que la información no esté disponible ni sea revelada a individuos, entidades o procesos no autorizados. [NTC 5411-1:2006]
- Evaluación del riesgo: proceso de comparar el riesgo estimado contra criterios de riesgo dados, para determinar la importancia del riesgo. [Guía ISO/IEC 73:2002]
- Evento de seguridad de la información: presencia identificada de una condición de un sistema, servicio o red, que indica una posible violación de la política de seguridad de la

información o la falla de las salvaguardas, o una situación desconocida previamente que puede ser pertinente a la seguridad. [ISO/IEC TR 18044:2004]

- Gestión del riesgo: actividades coordinadas para dirigir y controlar una organización en relación con el riesgo. [Guía ISO/IEC 73:2002]
- Incidente de seguridad de la información: un evento o serie de eventos de seguridad de la información no deseados o inesperados, que tienen una probabilidad significativa de comprometer las operaciones del negocio y amenazar la seguridad de la información. [ISO/IEC TR 18044:2004]
- Integridad: propiedad de salvaguardar la exactitud y estado completo de los activos. [NTC 5411-1:2006]
- Riesgo residual: nivel restante de riesgo después del tratamiento del riesgo. [Guía ISO/IEC 73:2002]
- Seguridad de la información: preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad. [NTC-ISO/IEC 17799:2006] Sistema de gestión de la seguridad de la información SGSI: parte del sistema de gestión global, basada en un enfoque hacia los riesgos globales de un negocio, cuyo fin es establecer, implementar, operar, hacer seguimiento, revisar, mantener y mejorar la seguridad de la información
- Tratamiento del riesgo proceso de selección e implementación de medidas para modificar el riesgo. [Guía ISO/IEC 73:2002] NOTA En la presente norma el término “control” se usa como sinónimo de “medida”.

- Valoración del riesgo: proceso global de análisis y evaluación del riesgo. [Guía ISO/IEC 73:2002]

2.3 Marco Contextual

La investigación en curso establece un análisis de riesgo de la información del programa de egresados de la Universidad Popular Del Cesar Seccional Aguachica, entonces pues, se considera que el contexto de la investigación se relaciona directamente con el contexto institucional de la Universidad.

En referencia a la seguridad de la información, la UPC Seccional Aguachica aún no ha implementado un SISTEMA DE GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (SGSI), sin embargo se han realizado diferentes análisis y propuestas para ello, por medio de trabajos de grado, en especial de los estudiantes del programa Ingeniería de Sistemas.

La Seccional por ser una ampliación regional de la academia de la Universidad Popular del Cesar requiere e implementa la consolidación de su información principal por medio de los sistemas de información que de parte de la sede central y el gobierno nacional se han dispuesto.

Los sistemas de información conciernen a los procesos misionales de la educación superior, así:

Sistemas de información externos:

Corresponden a los dispuestos por el gobierno nacional y que como institución de educación superior del orden oficial debemos alimentar:

- SNIES Sistema Nacional de Información de la Educación Superior
- SPADIES Sistema para la Prevención de la Deserción de la Educación Superior
- OLE Observatorio Laboral para la Educación

Sistemas de información internos:

Corresponden a los que soportan la operación de la universidad y que facilitan el funcionamiento de la estructura académico-administrativa; estos son:

- Sistema Académico (ACADEMUSOFT): El sistema académico permite administrar toda la información de estudiantes y docentes de la universidad, aquí se presentan los servicios, los anuncios, las aulas y la gestión del contenido académico: horarios, grupos, notas, hojas de vida etc.
- Sistema de Información Bibliográfica (SIBUPC): Los usuarios pueden hacer uso del catálogo, las bases de datos, las tesis digitales y el Repositorio Institucional a través de Internet.
- Sistema Financiero Administrativo (SYSMAN): Módulo financiero para manejo de información administrativa, presupuestal y contable. Sistema General de Almacén e Inventario (SYSMAN).
- Sistema de Gestión Humana (SYSMAN): Sistema de administración de información laboral de funcionarios (administrativos y docentes).

Para el caso de la investigación en curso el sistema de información prevalente de referencia será uno externo, el OLE Observatorio Laboral para la Educación, perteneciente al Ministerio de Educación Nacional. Por otra parte el análisis de riesgos en la información, no ha sido objeto de estudio, ni a nivel institucional, ni a nivel del proceso del programa de egresados.

2.4 Marco Teórico

De acuerdo a (De Pablos Heredero, 2006, Pág. 32) la información posee unas características que hacen posible su contextualización:

- La información es difícil dividirla en partes diferenciadas
- Una persona que disponga de información no la pierde cuando la trasmite a otra
- La información no se gasta con el uso, no se devalúa, sino que incluso mejora con el mismo
- Una información puede tener valor hoy y carecer del mismo mañana. La evolución en el tiempo del valor de la información es difícilmente previsible
- Una información puede ser inmenso valor para un sujeto y no tener relevancia para otro. Por tanto, la información tiene valor en función de quien la use.
- Para que una persona pueda apreciar el valor de una información, es decir, si esta satisface sus necesidades, debería poder conocerla. Por ello, resulta imposible facilitar una información para su evaluación sin entregar la propia información

Sobre esta teoría, podemos plantear el valor primario de la investigación en curso, considerando que toda gestión sobre la información produce un valor tangible o intangible, dicho

valor puede evolucionar en el tiempo y satisfacer o no necesidades para los procesos y/o las instituciones.

Una vez definido lo que es la información para el análisis, y sus características, podemos estructurar una base para considerar proteger, controlar, y evaluar dicha información por medio de la seguridad, según la norma ISO 27000, la seguridad de la información está asociada a la "preservación de la confidencialidad, la integridad y la disponibilidad de la información; además, puede involucrar otras propiedades tales como: autenticidad, trazabilidad (Accountability), no repudio y fiabilidad."

De acuerdo al (Ministerio de Tecnologías de Información y Comunicaciones MINTIC, 2016. Pág 6),

> Para la evaluación de riesgos en seguridad de la información, un insumo vital es la clasificación de activos de información ya que una buena práctica es realizar gestión de riesgos a los activos de información que se consideren con nivel de clasificación ALTA dependiendo de los criterios de clasificación; es decir que en los criterios de Confidencialidad, Integridad y Disponibilidad tengan la siguiente calificación:

Criterios de clasificación:

CONFIDENCIALIDAD:	INTEGRIDAD:	DISPONIBILIDAD:
INFORMACIÓN PÚBLICA RESERVADA	ALTA (A)	ALTA (A)
INFORMACIÓN PÚBLICA CLASIFICADA	MEDIA (M)	MEDIA (M)

INFORMACIÓN PÚBLICA	BAJA (B)	BAJA (B)
NO CLASIFICADA	NO CLASIFICADA (N)	NO CLASIFICADA (N)

Así mismo establece los niveles de clasificación:

ALTA: Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.

MEDIA: Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.

BAJA: Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Para realizar el proceso de administración del riesgo, la norma ISO 27005 establece 7 pasos definidos así:

1. ESTABLECIMIENTO DEL CONTEXTO
2. IDENTIFICACIÓN DEL RIESGO
3. ESTIMACIÓN DEL RIESGO
4. EVALUACIÓN DEL RIESGO
5. TRATAMIENTO DEL RIESGO
6. ACEPTACIÓN DEL RIESGO
7. COMUNICACIÓN DEL RIESGO

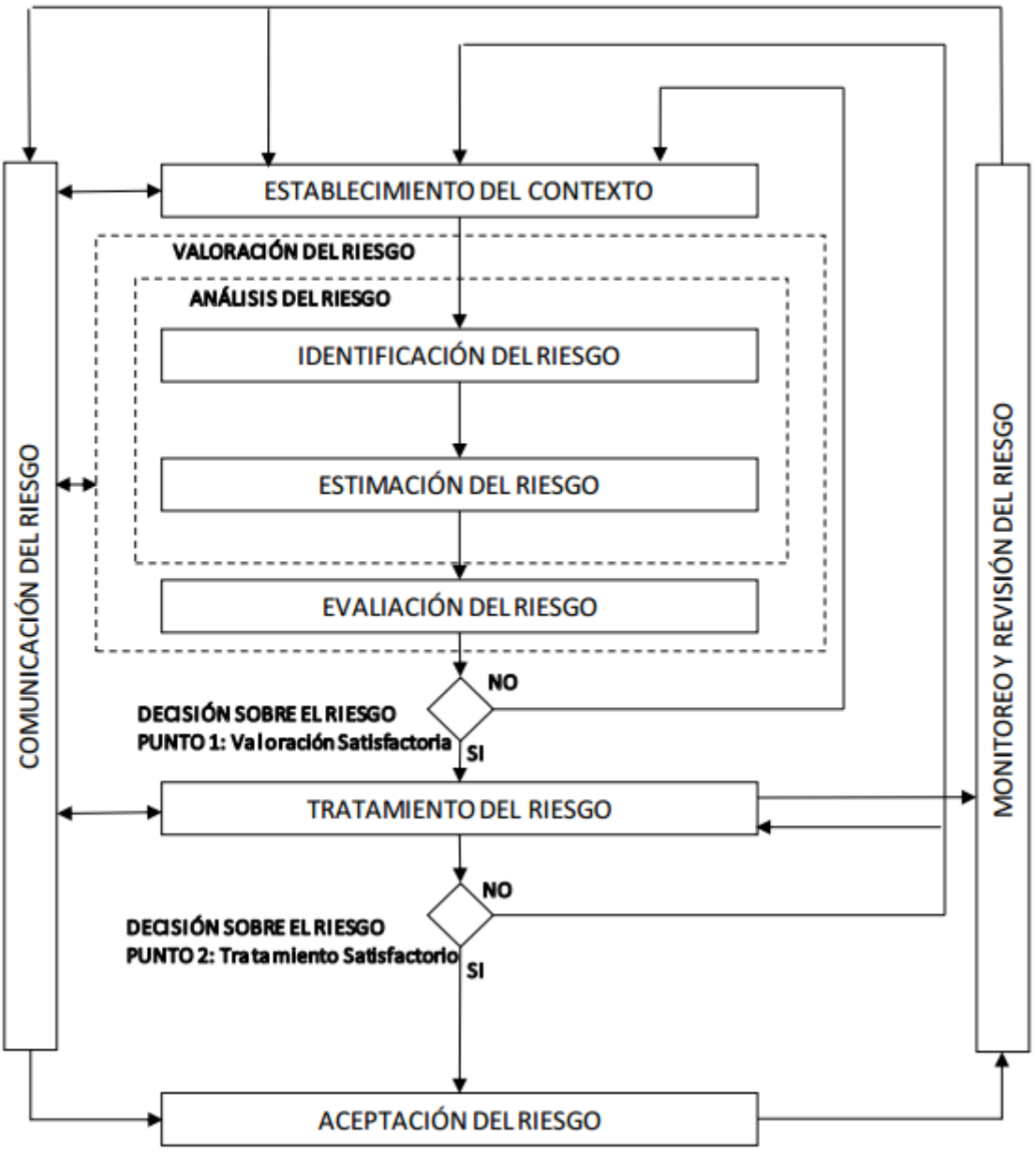


Figura 1. Proceso de administración del riesgo norma ISO 27005

El contexto se establece primero. Luego se realiza una valoración del riesgo. Si ésta suministra información suficiente para determinar de manera eficaz las acciones que se necesitan para modificar los riesgos hasta un nivel aceptable, entonces la labor está terminada y sigue el tratamiento del riesgo. Si la información no es suficiente, se llevará acabo otra iteración de la valoración del riesgo con un contexto revisado (por ejemplo, los

> Criterios de evaluación del riesgo, los criterios para aceptar el riesgo o los criterios de impacto), posiblemente en partes limitadas del alcance total (véase la Figura 1, Decisión sobre el riesgo-punto 1).
>
> La eficacia del tratamiento del riesgo depende de los resultados de la valoración del riesgo. Es posible que el tratamiento del riesgo no produzca inmediatamente un nivel aceptable de riesgo residual. En esta situación, si es necesaria, se puede requerir otra iteración de la valoración del riesgo con cambios en los parámetros del contexto (por ejemplo criterios para valoración del riesgo, de aceptación o de impacto del riesgo), seguida del tratamiento del riesgo (véase la Figura 1, Decisión sobre el riesgo-punto 2).La actividad de aceptación del riesgo debe asegurar que los riesgos residuales son aceptados explícitamente por los directores de la organización. Esto es especialmente importante en una situación en la que la implementación de los controles se omite o se pospone, por ejemplo debido al costo.

Así mismo la norma ISO 27005, define en su capítulo ANALISIS DE RIESGO lo asociado con el mismo:

Identificación del riesgo

Introducción a la identificación del riesgo

El propósito de la identificación del riesgo es determinar qué podría suceder que cause una pérdida potencial, y llegar a comprender el cómo, dónde y por qué podría ocurrir esta pérdida. Los pasos que se describen en los siguientes numerales de la sección 8.2.1deberían recolectar datos de entrada para la actividad de estimación del riesgo. ((Scribd ISO-27005 - español, 2017) Pág 19)

Identificación de los activos

Un activo es todo aquello que tiene valor para la organización y que, por lo tanto, requiere de protección. Para la identificación de los activos se recomienda tener en cuenta que el sistema de información consta de más elementos que sólo hardware y software. La identificación de los

activos se debería llevar a cabo con un nivel adecuado de detalle, que proporcione información suficiente para la valoración del riesgo. El nivel de detalle utilizado en la identificación de los activos tendrá influencia en la cantidad total de información recolectada durante la valoración del riesgo. Este nivel se puede mejorar en iteraciones posteriores de la valoración del riesgo. Se debería identificar al propietario de cada activo, para asignarle la responsabilidad y rendición de cuentas sobre éste. El propietario del activo puede no tener derechos de propiedad sobre el activo, pero tiene la responsabilidad de su producción, desarrollo, mantenimiento, uso y seguridad, según corresponda. El propietario del activo con frecuencia es la persona más idónea para determinar el valor que el activo tiene para la organización (véase el numeral 8.2.2.2 con relación a la valoración del activo).El límite de la revisión es el perímetro definido de los activos de la organización que debe ser gestionado por parte del proceso de gestión del riesgo en la seguridad de la información. ((Scribd ISO-27005 - español, 2017)Pág 20)

Identificación de las amenazas

Una amenaza tiene el potencial de causar daños a activos tales como información, procesos y sistemas y, por lo tanto, a las organizaciones. Las amenazas pueden ser de origen natural o humano y podrían ser accidentales o deliberadas. Es recomendable identificar tanto los orígenes de las amenazas accidentales como de las deliberadas. Una amenaza puede tener su origen dentro o fuera de la organización. Las amenazas se deberían identificar genéricamente y por tipo (por ejemplo, acciones no autorizadas, daño físico, fallas técnicas) y, cuando sea adecuado, las amenazas individuales dentro de la clase genérica identificada. Esto significa que ninguna amenaza se pasa por alto, incluidas las inesperadas, pero teniendo en cuenta que el volumen de trabajo requeridos limitado. Algunas amenazas pueden afectar a más de un activo. En tales casos

pueden causar diferentes impactos dependiendo de los activos que se vean afectados. La entrada para la identificación de las amenazas y la estimación de la probabilidad de ocurrencia (véase el numeral 8.2.2.3) se puede obtener de los propietarios o los usuarios del activo, del personal de recursos humanos, del administrador de las instalaciones y de especialistas en seguridad de la información, expertos en seguridad física, área jurídica y otras organizaciones que incluyen organismos legales, bien sea autoridades, compañías de seguros y autoridades del gobierno nacional. Los aspectos ambientales y culturales se deben tener en cuenta cuando se consideran las amenazas. La experiencia interna obtenida de los incidentes y las valoraciones anteriores de las amenazas, se deberían tomar en consideración en la valoración actual. Podría ser valioso consultar otros catálogos de amenazas (pueden ser específicas para una organización o un negocio) para completar la lista de amenazas genéricas, cuando sea pertinente. Los catálogos y las estadísticas sobre las amenazas están disponibles en organismos industriales, del gobierno nacional, organizaciones legales, compañías de seguros, etc. Cuando se utilizan catálogos de amenazas o los resultados de valoraciones anteriores delas amenazas, es conveniente ser consciente de que existe un cambio continuo de las amenazas importantes, en especial si cambia el ambiente del negocio o los sistemas de información. (Scribd ISO-27005 - español, 2017Pág 20)

Identificación de los controles existentes

Se debería realizar la identificación de los controles existentes para evitar trabajo o costos innecesarios, por ejemplo en la duplicación de los controles. Además, mientras se identifican los controles existentes es recomendable hacer una verificación para garantizar que los controles funcionan correctamente - una referencia a los reportes de auditoría desasí ya existente debería

limitar el tiempo que tarda esta labor. Si el control no funciona como se espera, puede causar vulnerabilidades. Es recomendable tomar en consideración la situación en la que el control seleccionado (o la estrategia) falla en su funcionamiento y, por lo tanto, se requieren controles complementarios para tratar de manera eficaz el riesgo identificado. En un SGSI, de acuerdo con ISO/IEC 27001, se tiene como soporte la revisión de la eficacia del control. Una forma de estimar el efecto del control es ver la manera en que reduce la probabilidad de ocurrencia de la amenaza y la facilidad de explotar la vulnerabilidad, o el impacto del incidente. Las revisiones por parte de la dirección y los reportes de auditoría también suministran información acerca de la eficacia de los controles existentes. Los controles que se planifican para implementar de acuerdo con los planes de implementación del tratamiento del riesgo, se deberían considerar en la misma forma que aquellos ya implementados. Un control existente o planificado se podría identificar como ineficaz, insuficiente injustificado. Si es injustificado o insuficiente, se debería revisar el control para determinar si se debe eliminar, reemplazar por otro más adecuado o si debería permanecer, por ejemplo, por razones de costos. (Scribd ISO-27005 - español, 2017Pág 21)

Identificación de las vulnerabilidades

Se pueden identificar vulnerabilidades en las siguientes áreas:- organización;- procesos y procedimientos;- rutinas de gestión;- personal;- ambiente físico;- configuración del sistema de información;- hardware, software o equipo de comunicaciones;- dependencia de partes externas. La sola presencia de una vulnerabilidad no causa daño por sí misma, dado que es necesario que haya una amenaza presente para explotarla. Una vulnerabilidad que no tiene una amenaza correspondiente puede no requerir de la implementación de un control, pero es recomendable reconocerla y monitorearla para determinar los cambios. Conviene anotar que un control

implementado de manera incorrecta o que funciona mal, o un control que se utiliza de modo incorrecto podrían por sí solo constituir una vulnerabilidad. Un control puede ser eficaz o ineficaz dependiendo del ambiente en el cual funciona. Por el contrario, una amenaza que no tiene una vulnerabilidad correspondiente puede no resultar en un riesgo. Las vulnerabilidades pueden estar relacionadas con las propiedades de los activos que se pueden usar de una manera, o para un propósito, diferente del previsto cuando se adquirió o se elaboró el activo. Las vulnerabilidades que se originan desde fuentes diferentes se deben considerar, por ejemplo, aquellas intrínsecas o extrínsecas al activo. (Scribd ISO-27005 - español, 2017 Pág 23)

Identificación de las consecuencias

Una consecuencia puede ser la pérdida de la eficacia, condiciones adversas de operación, pérdida del negocio, reputación, daño, etc. Esta actividad identifica los daños o las consecuencias para la organización que podrían ser causadas por un escenario de incidente. Un escenario de incidente es la descripción de una amenaza que explota una vulnerabilidad determinada o un conjunto de vulnerabilidades en un incidente de seguridad de la información (véase la norma ISO/IEC27002, sección 13). El impacto de los escenarios de incidente se determina tomando en consideración los criterios del impacto que se definen durante la actividad de establecimiento del contexto. Puede afectar a uno o más activos o a una parte de inactivo. De este modo, los activos pueden tener valores asignados tanto para su costo financiero como por las consecuencias en el negocio, si se deterioran o se ven comprometidos. Las consecuencias pueden ser de naturaleza temporal o permanente como es el caso de la destrucción de un activo. ((Scribd ISO-27005 - español, 2017) Pág 24)

Estimación del riesgo

Metodologías para la estimación del riesgo

Estimación cualitativa: La estimación cualitativa utiliza una escala de atributos calificativos para describirla magnitud de las consecuencias potenciales (por ejemplo, alta, intermedia y baja) y la probabilidad de que ocurran dichas consecuencias. Una ventaja de la estimación cualitativa es su facilidad de comprensión por parte de todo el personal pertinente, mientras que una desventaja es la dependencia en la selección subjetiva de la escala. Estas escalas se pueden adaptar o ajustar para satisfacer las circunstancias y se pueden utilizar descripciones diferentes para riesgos diferentes. La estimación cualitativa se puede utilizar:- como una actividad de tamizado inicial para identificar los riesgos que requieren un análisis más detallado;- cuando este tipo de análisis es adecuado para tomar decisiones;- cuando los datos numéricos o los recursos no son adecuados para una estimación cuantitativa. El análisis cualitativo debería utilizar información con base en hechos y datos, cuando estén disponibles. (Scribd ISO-27005 - español, 2017Pág 25)

Estimación cuantitativa

La estimación cuantitativa utiliza una escala con valores numéricos (a diferencia delas escalas descriptivas utilizadas en la estimación cualitativa) tanto para las consecuencias como para la probabilidad, utilizando datos provenientes de varias fuentes. La calidad del análisis depende de lo completos y exactos que sean los valores numéricos, y de la validez de los modelos utilizados. En la mayoría de los casos, la estimación cuantitativa utiliza datos históricos sobre los incidentes,

Dando como ventaja que ésta pueda relacionarse

Directamente con los objetivos de seguridad de la información y los intereses de la organización. Una desventaja Esla falta de tales datos sobre riesgos nuevos o debilidades en la seguridad de la información. Una desventaja del enfoque cuantitativo se puede presentar cuando no se dispone de datos basados en los hechos que se puedan auditar, creando así una ilusión del valor y la exactitud de la valoración del riesgo. La forma en la cual se expresan las consecuencias y la probabilidad, y las formasen las cuales se combinan para proveer el nivel del riesgo varían de acuerdo con el tipo de riesgo y el propósito para el cual se va a utilizar la salida de la valoración del riesgo. La incertidumbre y la variabilidad tanto de las consecuencias como de la probabilidad se deberían ser consideradas en el análisis y comunicarse de manera eficaz. (Scribd ISO-27005 - español, 2017Pág 25)

Evaluación de las consecuencias

Después de identificar todos los activos bajo revisión, se deberían tener en cuenta los valores asignados a estos activos en la evaluación de las consecuencias. El valor del impacto del negocio se puede expresar de manera cualitativa y cuantitativa, pero cualquier método para asignar valor monetario en general puede suministrar más información para la toma de decisiones y, por tanto, facilitar un proceso más eficiente detona de decisiones. La valoración de activos empieza con la clasificación de los activos de acuerdo con su criticidad, en términos de la importancia de los activos para cumplir los objetivos de negocio de la organización. La valoración se determina entonces utilizando dos medidas:- el valor de reemplazo del activo: el costo de la limpieza de recuperación y de reemplazo de la información (si es posible), las consecuencias para el negocio por la pérdida o compromiso de los activos, tales como consecuencias adversas potenciales para el negocio y/o consecuencias legales o reglamentarias

por la divulgación, modificación, no disponibilidad y/o destrucción de la información, y otros activos de información. (Scribd ISO-27005 - español, 2017Pág 26)

Evaluación de la probabilidad de incidentes:

Después de identificar los escenarios de incidentes, es necesario evaluar la probabilidad de cada escenario y el impacto de que ocurra, utilizando técnicas de estimación cualitativas o cuantitativas. Se deberían tomar en consideración la frecuencia con la que ocurren las amenazas y la facilidad con que las vulnerabilidades pueden ser explotadas, teniendo en cuenta:- la experiencia y las estadísticas aplicables para la probabilidad de la amenaza;- para fuentes de amenaza deliberada: la motivación y las capacidades, las cuales cambiarán con el tiempo, y los recursos disponibles para los posibles atacantes, así como la percepción de atracción y vulnerabilidad de los activos para un posible atacante;- para fuentes de amenaza accidental: factores geográficos como proximidad a plantas químicas o de petróleo, la probabilidad de condiciones climáticas extremas, y factores que pudieran tener influencia en los errores humanos y el malfuncionamiento del equipo;- vulnerabilidades, tanto individuales como en conjunto;- controles existentes y qué tan eficazmente reducen las vulnerabilidades. ((Scribd ISO-27005 - español, 2017) Pág. 27)

Nivel de estimación del riesgo

La estimación del riesgo asigna valores a la probabilidad y las consecuencias de un riesgo. Estos valores pueden ser cuantitativos o cualitativos. La estimación del riesgo sebosa en las consecuencias evaluadas y la probabilidad. Además, la estimación puede considerar el beneficio de los costos, los intereses de las partes involucradas y otras variables, según correspondan para

la evaluación del riesgo. El riesgo estimado es una combinación de la probabilidad de un escenario de incidente y sus consecuencias. ((Scribd ISO-27005 - español, 2017) Pág. 28)

Evaluación del riesgo

Los criterios de evaluación del riesgo utilizados para tomar decisiones deberían ser consistentes con el contexto definido para la gestión del riesgo en la seguridad de la información externa e interna y deberían tomar en consideración los objetivos de la organización, los puntos de vista de las partes interesadas, etc. Las decisiones, tal conoce toman en la actividad de evaluación del riesgo, se basan principalmente en el nivel aceptable de riesgo. Sin embargo, también es recomendable considerar las consecuencias, la probabilidad y el grado de confianza en la identificación y el análisis del riesgo. La agrupación de múltiples riesgos bajos o medios puede dar como resultado riesgos globales mucho más altos y es necesario tratarlos según corresponda. Las consideraciones deberían incluir:

- propiedades de la seguridad de la información

: Si un criterio no es pertinente párala organización (por ejemplo la pérdida de confidencialidad), entonces todos los riesgos que tienen impacto sobre este criterio pueden no ser pertinentes;

- la importancia de los procesos del negocio o de la actividad sustentada por un activo particular o un conjunto de activos

: Si se determina que el proceso tiene importancia baja, los riesgos asociados con él deberían tener una consideración más baja que los riesgos que tienen impacto en procesos o actividades más importantes.

A evaluación del riesgo utiliza la comprensión del riesgo que se obtiene mediante el análisis del riesgo para tomar decisiones sobre acciones futuras. Las decisiones deberían incluir:- si se debería realizar una actividad;- prioridades para el tratamiento de los riesgos considerando los valores estimados de ellos. ((Scribd ISO-27005 - español, 2017) Pág. 29)

2.5 Marco legal

El marco legal de la investigación en curso tiene alcance a la normatividad asociada a la seguridad de la información en Colombia y su manejo:

Ley Estatutaria 15 81 de 2012 y Reglamentada Parcialmente por el Decreto Nacional 1377 De 2013: Por la cual se dictan disposiciones generales para la protección de datos personales

Decreto 2693 de 2012: Lineamientos generales de la Estrategia de Gobierno en línea de la República de Colombia que lidera el Ministerio de las Tecnologías de Información y las Comunicaciones, se reglamentan parcialmente las Leyes 1341 de 2009 y 1450 de 2011, y se dictan otras disposiciones.

Decreto 2609 de 2012: Por medio del cual se reglamenta el Título V de la Ley General de Archivo del año 2000. Incluye aspectos que se deben considerar para la adecuada gestión de los documentos electrónicos

Ley 1273 DE 2009: Por medio de la cual se modifica el Código Penal, se crea un nuevo bien tutelado denominado “de la protección de la información y los datos” y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

Ley 1341 DE 2009: Por medio de la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y comunicaciones - TIC, se crea la Agencia Nacional de Espectro y se dictan otras disposiciones

Ley 962 DE 2005: Por la cual se dictan disposiciones sobre racionalización de trámites y procedimientos administrativos de los organismos y entidades del Estado y de los particulares que ejercen funciones públicas o prestan servicios públicos.

Ley 599 DE 2000: Por la cual se expide el Código Penal. Se crea el bien jurídico de los derechos de autor e incorpora algunas conductas relacionadas indirectamente con los delitos informáticos como el ofrecimiento, venta o compra de instrumento apto para interceptar la comunicación privada entre personas, y manifiesta que el acceso abusivo a un sistema informático protegido con medida de seguridad o contra la voluntad de quien tiene derecho a excluirlo, incurre en multa.

Capítulo 3. Diseño Metodológico

3.1 Tipo De Investigación

La investigación en curso presenta un tipo de investigación descriptiva,

> Con frecuencia, la meta del investigador consiste en describir fenómenos, situaciones, contextos y eventos; esto es, detallar como son y se manifiestan. Los estudios descriptivos buscan especificar las propiedades, las características y los perfiles de personas, grupos, comunidades, pro· casos, objetos 0 cualquier otro fenómeno que se someta a un análisis (Dañe, 1989). Es decir, miden, evalúan 0 recolectan datos sobre diversos conceptos (variables), aspectos, dimensiones 0 componentes del fenómeno a investigar. En un estudio descriptiva~ se selecciona una serie de cuestiones y se mide o recolecta información sobre cada una de ellas, para así (valga la redundancia) describir que se investiga. (Hernandez Sampieri, 2006, Pág 99)

Para el caso, se busca describir el objeto de estudio documental, que es la información del programa de egresados de la Universidad Popular del Cesar Seccional Aguachica y su comportamiento respecto al análisis de riesgos. De la misma manera, el fenómeno que surge del efecto de la aplicación de la seguridad de la información.

3.2 Método

Se utilizara un Enfoque Cuantitativo por medio de un Método descriptivo. Consiste, fundamentalmente, en caracterizar un fenómeno o situación concreta indicando sus rasgos más peculiares o diferenciadores. Los datos descriptivos cuantitativos se utilizan para la exposición de los datos que provienen de un cálculo o medición. Se pueden medir diferentes unidades, elementos o categorías identificables. (Web, 2017)

3.3 Población

(Hernandez Sampieri, 2006, Pág 238) retoma el concepto de (Celtic et al., 1980) sobre lo que es la delimitación de la población:

> Una vez que se ha definido cuál será la unidad de análisis, se procede a delimitar la población que va a ser estudiada y sobre la cual se pretende generalizar los resultados. Así, una población es el conjunto de todos los casos que concuerdan con una serie de especificaciones.

Para la investigación en curso, la población de la investigación se identifica como el 100% de la información que se produce, se gestiona, se administra y se controla en el Programa de Egresados de la Universidad Popular del Cesar Seccional Aguachica.

3.4 Muestra

De acuerdo con (Hernandez Sampieri, 2006 Pág 240) *"La muestra es, en esencia, un subgrupo de la población. Digamos que es un subconjunto de elementos que pertenecen a ese conjunto definido en sus características al que llamamos población."*

Para la investigación en curso la muestra de la investigación se tomará sobre la información producida por el Programa de Egresados de la Universidad Popular del Cesar Seccional Aguachica, los años 2012 a 2016.

3.5 Técnicas De Recolección De La Información

3.5.1 Fuentes primarias

La fuente primaria para la recolección de datos será la documentación del Programa de Egresados de la Universidad Popular del Cesar Seccional Aguachica, el análisis de riesgos se

realizará por medio de una lista de verificación y una matriz de riesgos, para lo cual se elaboraran formatos como instrumentos de recolección de información.

3.5.2 Fuentes secundarias

La fuente secundaria para la recolección de datos será la información del Observatorio Laboral para la Educación OLE del Programa de Egresados de la Universidad Popular del Cesar Seccional Aguachica.

3.6 Instrumentos de recolección de información

Se determina usar un método cualitativo y sociocritico, por medio del Análisis de Documentos, tomando como referencia las guías mencionadas en el marco referencial y realizando el diseño de formatos para la recolección de la información.

Para las etapas del desarrollo del proyecto se utilizaran los siguientes instrumentos de recolección de información:

Formato 1. Inventario Activos de Información

Inventario Activos de Información											
Programa de egresados Universidad Popular del Cesar Seccional Aguachica Confidencialidad: Solo fines educativos											
						Clasificación			**Criticidad**	**Propiedad**	
Código	**Proceso**	**Nombre del Activo**	**Observaciones**	**Tipo**	**Ubicación**	**Confidencialidad**	**Integridad**	**Disponibilidad**		**Propietario**	**Responsable**

Formato 2. Identificación y análisis de riesgos

Identificación y análisis de riesgos
Programa de egresados

Universidad Popular del Cesar Seccional Aguachica Confidencialidad: Solo fines educativos						
			Calificación			Evaluación
Código	Activo	RIESGO	Probabilidad	Impacto	Tipo	Zona de Riesgo

Formato 3. Identificación de controles y análisis de riesgos

Identificación de controles y análisis de riesgos													
Programa de egresados Universidad Popular del Cesar Seccional Aguachica Confidencialidad: Solo fines educativos													
			Calificación			Evaluación				Nueva Calificación		Evaluación	
Código	Activo	RIESGO	Probabilidad	Impacto	Tipo	Zona de Riesgo	Medida de Respuesta	CONTROLES	TIPO DE CONTROL	Probabilidad	Impacto	Zona de Riesgo	Medida de Respuesta

Capítulo 4. Resultados

4.1 Características generales del Programa de Egresados

4.1.1 Contexto Institucional

La Universidad Popular del Cesar en articulación con su misión y la construcción de nación ha definido un conjunto de políticas, estrategias y proyectos tendientes a la vinculación e interacción permanente de los egresados a la dinámica de la universidad, denominado Programa de Egresados, por medio del ACUERDO 067 de 27 de diciembre de 2005 del CSU.

> El Programa de Egresados planea, organiza y propone la ejecución de políticas, estrategias y proyectos acordes con los lineamientos del PEI, tendientes a la vinculación y comunicación en forma permanente entre los egresados de la universidad, lo cual es su Misión principal.
>
> A su vez el programa nace como un proyecto institucional de carácter permanente, el cual se establece como su Visión, que diseña y pone en práctica políticas, estrategias dirigidas a la vinculación interacción de los egresados a la dinámica de la universidad y su entorno social.
>
> La Universidad Popular del Cesar reconoce como egresado a la persona que haya terminado académicamente cualquiera de los programas de formación que se ofertan; y se distinguirán con incentivos especiales como: Designación en comités, grupos o equipos institucionales; Publicación y difusión de los aportes académicos e investigativos, así como apoyo a proyectos de investigación pertinentes a la misión social de la UPC. (UPC, 2005)

4.1.2 Estructura del Programa de Egresados

> De acuerdo con (UPC, 2005) La organización y administración del Programa de Egresados estará bajo la mirada académica de la institución en cabeza de la Vicerrectoría de Investigación a nivel institucional y de la Dirección Académica a nivel de la Seccional; para el desarrollo del programa se vinculará un egresado como director del mismo. De la misma manera el director se apoyara en un órgano de asesoría denominado Comité de Egresados quien está conformado además por el representante de los egresados ante el Consejo Superior, Académico y un representante de los consejos de Facultad.

4.1.3 Programas, Proyectos y Servicios

A nivel de Seccional se ha diseñado un portafolio de servicios de acuerdo con su egresado siguiendo la premisa del Enfoque diferencial; donde las características se hacen especiales por las condiciones socio-económicas del entorno, para esto se ofrece:

ADMINISTRACIÓN Y GESTIÓN DE LA INFORMACIÓN DE LOS PROFESIONALES

Mediante el aplicativo en línea del programa de Academusoft.

ACTUALIZACIÓN DE BASE DE DATOS

Permite determinar la ubicación, la evolución profesional y formación académica del egresado.

SEGUIMIENTO Y ACOMPAÑAMIENTO A EGRESADOS

Un mecanismo de gestión encargado de fortalecer el vínculo egresados y la universidad.

CARNETIZACIÓN

Cada profesional recibe su carné que lo acredita como egresado de la Institución.

ACTUALIZACIÓN PROFESIONAL

Constantemente la Universidad Popular del Cesar Seccional Aguachica, a través de la oficina de Egresados ofrece capacitaciones, conferencias, seminarios.

RED DE INFORMACIÓN VIRTUAL

A través de los correos electrónicos **egresados.aguachica@, s**e envía información de interés a los profesionales.

ESPACIOS DE INTEGRACIÓN

Realizan actividades lúdicas, deportivas y recreativas, que permiten fomentar la integración entre los egresados.

PERTENENCIA Y VINCULACIÓN DE EGRESADOS A LA UNIVERSIDAD

La Universidad Popular del Cesar respalda la vinculación de egresado profesional en los diferentes cuerpos colegiados, docentes y administrativos que contribuya en el proceso de mejoramiento y desarrollo continuo de la Institución; así mismo promueve la creación de agremiaciones como un canal para incrementar la integración de sus profesionales, con miras a estimular el sentido de pertenencia con la universidad.

4.2 Identificación de los activos de información del Programa de Egresados UPC Seccional Aguachica

Según (ISO 2007, 2013), *un activo es todo aquello que tiene valor para la entidad y que, por lo tanto, requiere de protección. La identificación de activos se debería llevar acabo con un nivel adecuado de detalle que proporcione información suficiente para la valoración del riesgo.*

Para la identificación de los activos del programa de egresados se toma como referencia la Guía para la Gestión y Clasificación de Activos de Información, del modelo de seguridad del fortalecimiento de la gestión TI en el estado, del Ministerio de Tecnologías de Información y Comunicación MINTIC.

De acuerdo a (MINTIC, 2017) El Ministerio de Tecnologías de la Información y las Comunicaciones - Min TIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, dando cumplimiento a sus funciones; publica El Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión.

El Modelo de Seguridad y Privacidad para estar acorde con las buenas prácticas de seguridad será actualizado periódicamente; reuniendo los cambios técnicos de la norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información. (MINTIC, 2017)

(MINTIC, 2017) pág. 4. Para el desarrollo de esa guía, se recogieron aspectos importantes de mejores prácticas y documentos de uso libre, tomando como base los lineamientos recomendados en Norma la ISO IEC 27005 – 2009, y la ley 1712 de 2014 por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.

Para iniciar el proceso de identificación de activos, se establece que la información generada por el programa de egresados se determina como parte de su proceso, el cual se especifica así:

	UNIVERSIDAD POPULAR DEL CESAR	CÓDIGO: : 102-180-MAN07
		VERSIÓN: 1
	PROCEDIMIENTOS	PÁG. 129 de 398
		FECHA: 13/11/2009

13.9 SEGUIMIENTO AL EGRESADO

SISTEMA DE CONTROL INTERNO SUBSISTEMA DE CONTROL DE GESTIÓN				
Componente: ACTIVIDADES DE CONTROL **Elemento:** PROCEDIMIENTOS **Formato:** DISEÑOS DE PROCEDIMIENTOS				
MACROPROCESO: MISIONAL				
PROCESO: DOCENCIA				
PROCEDIMIENTO : SEGUIMIENTO AL EGRESADO				
No.	**(1) ACTIVIDADES**	**(2) TAREAS**	**(3) MÉTODO**	**(4) CARGO RESPONSABLE**
1	Actualización banco de datos	Registrar los egresados graduados según fecha de grado registrada en el calendario académico.	Se le solicita a la Secretaría General la relación de graduados y a CARCA los datos generales de los graduados y se registran. Formato encuesta a egresados. Formato Encuesta a Egresados en Línea Código: 201-300-PRO09-FOR01.	Director Oficina de Egresado.
2	Evaluación del desempeño del egresado	Aplicar encuestas a egresados y a empleadores sobre el impacto del desempeño del egresado.	Por visitas directas y a través de la página Web, se aplican los instrumentos correspondientes	Director Oficina de Egresado.
3	Capacitación y actualización a los egresados.	Diseñar y ejecutar un plan de capacitación a los egresados.	Basado en el análisis del diagnóstico de evaluación, se diseña y ejecuta un plan de actualización y capacitación al egresado.	Proceso Gestión de extensión y Proyección Social.

ELABORADO POR: JESÚS VALENCIA BUSTAMANTE, SANDRA PADILLA	FECHA:
REVISADO POR: EQUIPO MECI – CALIDAD	FECHA:
APROBADO POR: COMITÉ DE COORDINACIÓN DE CONTROL INTERNO	FECHA:

Figura 2. Proceso seguimiento al egresado UPC

Es así que, como salida del programa, se cuenta con los siguientes procesos:

- Administración y gestión de la información de los profesionales
- Actualización de base de datos
- Seguimiento y acompañamiento a egresados
- Carnetización
- Actualización profesional
- Red de información virtual
- Espacios de integración
- Pertenencia y vinculación de egresados a la universidad

4.2.1Inventario de activos de información

El inventario de activos diseñado para el Proceso de Egresados UPC SA, cuenta con dos aspectos:

Información básica:

Hace referencia a las características del activo, se incluye código, proceso, nombre del activo, observaciones, tipo (información, software, hardware, recurso humano, servicio, otro), ubicación, clasificación y criticidad).

Código: Se estableció identificar los activos con las iniciales del programa de egresados, y darles una secuencia numérica de números enteros.

Así: PE-1, PE-2, ……PE-n

Proceso: El proceso al que está vinculado el activo será aquel del que haga parte la información, los procesos relacionados para el programa de egresados son:

- Administración y gestión de la información de los profesionales
- Actualización de base de datos
- Seguimiento y acompañamiento a egresados
- Carnetización
- Actualización profesional
- Red de información virtual
- Espacios de integración
- Pertenencia y vinculación de egresados a la universidad

Todos los procesos deben tener mínimo un activo de información

Nombre del Activo: El nombre del activo está asociado a su contenido o características, los nombres se asignaron de acuerdo a estas, o a su diaria mención.

Observaciones: Hace referencia a las particularidades de la información.

Tipo: La clasificación del tipo se tomó de (MINTIC, 2017), donde se proponen los siguientes:

Información

Software

Hardware

Recurso humano

Servicio

Otro

Ubicación: Espacio o lugar donde se encuentra el activo de información

Clasificación: La clasificación de los activos se tomó de (MINTIC, 2017)

> El sistema de clasificación definido se basa en la confidencialidad como principio rector en la selección e incluye el tratamiento de la información en cuanto a la Confidencialidad, la Integridad y la Disponibilidad de cada activo. Asimismo, contempla el impacto que causaría la pérdida de alguna de estas propiedades. Para cada propiedad se deben establecieron criterios específicos y lineamientos para el tratamiento adecuado del activo. Asimismo en esta guía se definieron tres (3) niveles que permiten determinar el valor general del activo en la entidad (es importante aclarar que los niveles pueden ser definidos a criterio de la entidad): Alta, Media y Baja, con el fin identificar qué activos deben ser tratados de manera prioritaria (MINTIC, 2017)

Tabla 1.

Principios rectores de la seguridad de la información

Confidencialidad	Integridad	Disponibilidad
INFORMACIÓN PUBLICA RESERVADA	INFORMACIÓN PUBLICA RESERVADA ALTA (A)	ALTA (1)
INFORMACIÓN PUBLICA CLASIFICADA	**MEDIA (M)**	**MEDIA (2)**
INFORMACIÓN PÚBLICA	**PÚBLICA BAJA (B)**	**BAJA (3)**
NO CLASIFICADA	**NO CLASIFICADA**	**NO CLASIFICADA**

Fuente: (MINTIC, 2017)

Criticidad: Se estableció de acuerdo a los resultados de la clasificación

Tabla 2.

Clasificación del valor general del activo

ALTA	**Activos de información en los cuales la clasificación de la información en dos (2) o todas las propiedades (confidencialidad, integridad, y disponibilidad) es alta.**
MEDIA	**Activos de información en los cuales la clasificación de la información es alta en una (1) de sus propiedades o al menos una de ellas es de nivel medio.**
BAJA	Activos de información en los cuales la clasificación de la información en todos sus niveles es baja.

Propiedad:

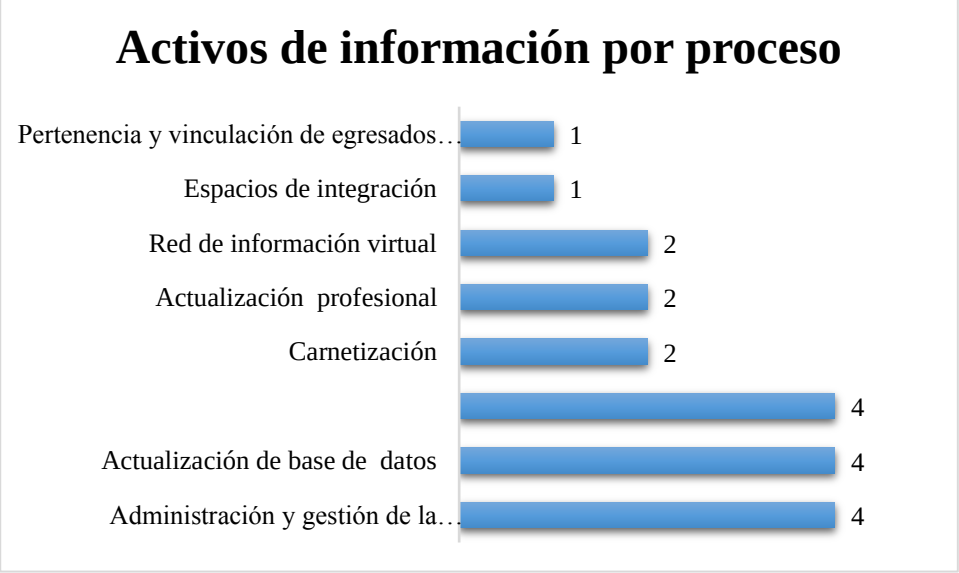
Hace referencia a identificar el propietario y responsable del activo

Propietario: Quien es dueño del activo de información

Responsable: Quine usa y custodia el activo de información

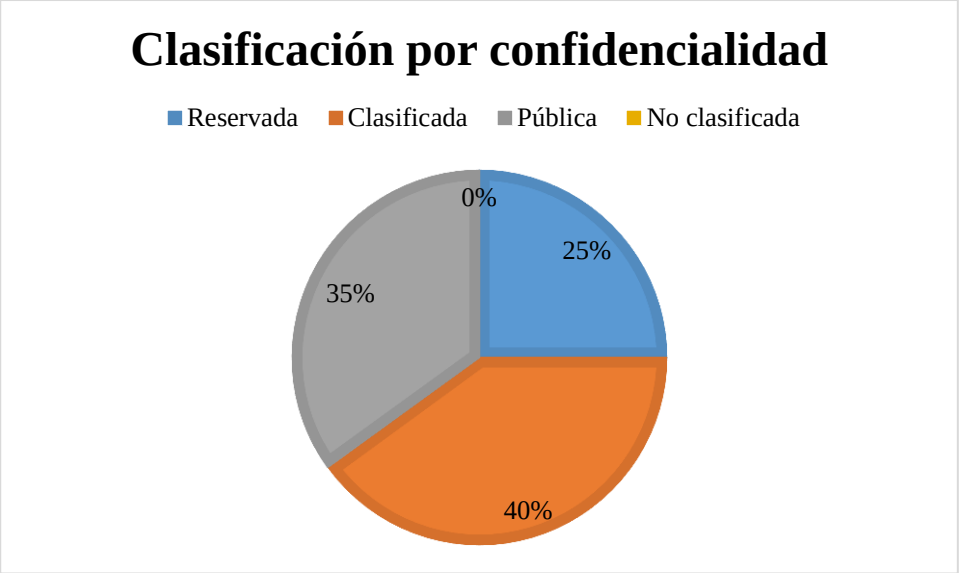
4.2.2 Resultados de la identificación de activos de información

En total se identificaron 19 activos de información, seguimiento y acompañamiento, actualización de base de datos y administración y gestión de la información fueron los procesos con más activos asociados (Grafica 1),



Gráfica 1. Activos de información por proceso

El 84% de los activos de información se clasificaron en una zona ALTA de criticidad, en cuanto a confidencialidad el 40% de los activos es clasificado, 35% pública, y 25% reservada. La integridad del 100% de los activos de información se clasifico como alta, esto por ser información personal de los egresados, y en cuanto a la disponibilidad el 89% se clasifico como alta y el 11% como media.



Gráfica 2. Clasificación de los activos por confidencialidad

Gráfica 3. Clasificación de los activos por disponibilidad

4.2.3 Matriz de activos de información.

Una vez identificados los activos de información la consolidación final fue dispuesta en la siguiente matriz:

Matriz 1. Inventario Activos de Información

Inventario Activos de Información											
Programa de egresados **Universidad Popular del Cesar Seccional Aguachica** **Confidencialidad: Solo fines educativos**											
						Clasificación			Criticidad	Propiedad	
Código	Proceso	Nombre del Activo	Observaciones	Tipo	Ubicación	Confidencialidad	Integridad	Disponibilidad		Propietario	Responsable
PE-1	Administración y gestión de la información de los profesionales	Hoja de vida Académica del egresado	Esta información es solo para consulta	Software	Software Academusoft	Reservada	A	1	ALTA	Egresado	Registro y Control
PE-2	Actualización de base de datos	Encuestas	Físicas, Digitales y Verbales	Información	Oficina Programa de Egresados	Reservada	A	1	ALTA	Egresado	Programa de Egresados
PE-3	Seguimiento y acompañamiento a egresados	Base de datos de egresados	Matriz de Excel	Información	Oficina Programa de Egresados	Reservada	A	1	ALTA	Programa de Egresados	Programa de Egresados
PE-4	Seguimiento y acompañamiento a egresados	Hoja de vida profesional del egresado	No se conserva permanentemente	Información	Oficina Programa de Egresados	Clasificada	A	1	ALTA	Egresado	Programa de Egresados

PE-5	Carnetización	Carné	Se entrega al egresado	Servicio		Pública	A	1	ALTA	Egresado	Programa de Egresados
PE-6	Carnetización	Registro de carnetización	Registro físico	Información		Clasificada	A	1	ALTA	Programa de Egresados	Programa de Egresados
PE-7	Actualización profesional	Registro de capacitaciones, conferencias, seminarios	Registro físico	Servicio	Oficina Programa de Egresados	Clasificada	A	1	ALTA	Programa de Egresados	Programa de Egresados
PE-8	Actualización profesional	Listas de asistencia a capacitaciones, conferencias, seminarios	Registro físico	Información	Oficina Programa de Egresados	Clasificada	A	1	ALTA	Programa de Egresados	Programa de Egresados
PE-9	Espacios de integración	Comunicaciones públicas	Físicas, Digitales y Verbales	Información	Oficina Programa de Egresados	Pública	A	1	ALTA	Programa de Egresados	Programa de Egresados
PE-10	Seguimiento y acompañamiento a egresados	Correo Electrónico	Herramienta	Otro	egresados.aguachica@	Reservada	A	1	ALTA	Programa de Egresados	Programa de Egresados
PE-11	Red de información virtual	Almacenamiento de archivos en la nube	Herramienta	Software	egresados.aguachica@	Clasificada	A	1	ALTA	Programa de Egresados	Programa de Egresados
PE-12	Red de información virtual	Redes Sociales	Herramienta	Otro	Facebook, Twitter	Pública	A	2	MEDIA	Programa de Egresados	Programa de Egresados
PE-13	Pertenencia y vinculación de egresados a la universidad	Portal de empleo	Herramienta	Software	http://trabajando.unicesar.edu.co/	Pública	A	1	ALTA	Programa de Egresados	Programa de Egresados
PE-14	Actualización de base de datos	Observatorio Laboral	Esta información es solo para consulta	Software	http://www.graduadoscolombia.edu.co/html/1732/w3-channel.html	Pública	A	2	MEDIA	MEN	Institucional
	Seguimiento y acompañamiento a egresados	Blog	Herramienta	Servicio	http://aguachicaegresadosupc.blogspot.com.co/	Pública	A	2	MEDIA	Programa de Egresados	Programa de Egresados

PE-15	Administración y gestión de la información de los profesionales	Informes de gestión	Registro físico	Información	Oficina Programa de Egresados	Clasificada	A	1	ALTA	Programa de Egresados	Programa de Egresados
PE-16	Actualización de base de datos	Informes de estadísticas	Registro físico	Información	Oficina Programa de Egresados	Clasificada	A	1	ALTA	Programa de Egresados	Programa de Egresados
PE-17	Actualización de base de datos	SNIES	Información externa para uso de consulta	Software	http://www.mineducacion.gov.co/sistemasdeinformacion/1735/w3-propertyname-2672.html	Clasificada	A	2	MEDIA	MEN	Institucional
PE-18	Administración y gestión de la información de los profesionales	Equipo de cómputo	Designado a programa de egresados	Hardware	Oficina Programa de Egresados	Reservada	A	1	ALTA	Programa de Egresados	Programa de Egresados
PE-19	Administración y gestión de la información de los profesionales	Profesional Universitario	Designado a programa de egresados	Recurso humano	Oficina Programa de Egresados	Pública	A	1	ALTA	Programa de Egresados	Programa de Egresados

4.3 Identificación de riesgos de los activos de información del programa de egresados de la UPC Seccional Aguachica

De acuerdo con (MINCTIC, 2016), pág. 19, *El propósito de la identificación del riesgo es determinar que podría suceder que cause una perdida potencial, y llegar a comprender el cómo, donde, y por qué podría ocurrir está perdida, las siguientes etapas deberían recolectar datos de entrada para esta actividad.*

Una vez identificados los activos se procedió asociar los riesgos a cada uno de ellos, de igual forma que en los activos.

Código: Se estableció identificar los riesgos con la inicial R y la inicial de egresados E, y darles una secuencia numérica de números enteros.

Así: RE-1, RE-2, …RE-n

Activo: Al cual está asociado el riesgo

Riesgo: Perdida potencial asociada al activo. La identificación de los riesgos se realizó por medio de la observación directa. Para esto se realizó una inspección al archivo físico y digital de la oficina de programa de egresados, de la misma forma se revisó las condiciones de red y seguridad del equipo de cómputo de la misma.

Observaciones encontradas:

Disposición del equipo de cómputo y archivo digital:

El equipo se encuentra en una oficina compartida con dos usuarios más, al ser una oficina para atención, se encuentra abierta al público, no se dispone de separadores ni cubículos.

Ilustración 1. Puesto de trabajo de la oficina Programa de Egresados

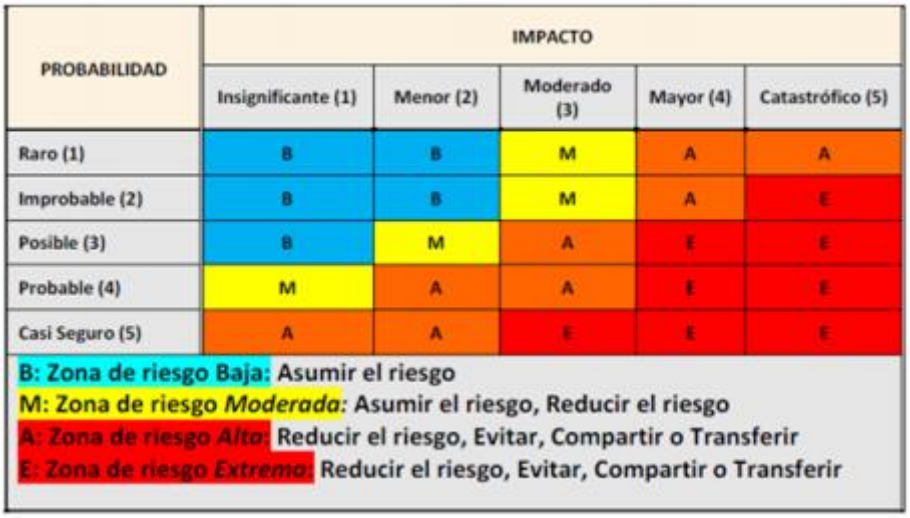
Disposición del archivo físico:

El archivo físico se encuentra dispuesto en una pequeña bodega, en la cual se guardan diferentes cosas y documentación. Por su parte las cajas para la disposición de los archivos finales del programa de egresados cuentan con las características técnicas, pero no se encuentran marcadas, por lo que carecen de identificación y no están archivados de acuerdo a la normatividad.

Ilustración 2. Archivo físico Programa de Egresados

Calificación y evaluación: Se hizo de manera cualitativa generando una comparación en la cual se presenta el análisis de la probabilidad de ocurrencia del riesgo versus el impacto del mismo.

Para esto se toma como referencia la Guía de Riesgos DAFP, presentada en (MINCTIC, 2016):



PROBABILIDAD	IMPACTO				
	Insignificante (1)	Menor (2)	Moderado (3)	Mayor (4)	Catastrófico (5)
Raro (1)	B	B	M	A	A
Improbable (2)	B	B	M	A	E
Posible (3)	B	M	A	E	E
Probable (4)	M	A	A	E	E
Casi Seguro (5)	A	A	E	E	E

B: Zona de riesgo Baja: Asumir el riesgo
M: Zona de riesgo *Moderada:* Asumir el riesgo, Reducir el riesgo
A: Zona de riesgo *Alta*: Reducir el riesgo, Evitar, Compartir o Transferir
E: Zona de riesgo *Extrema*: Reducir el riesgo, Evitar, Compartir o Transferir

Gráfica 4. Calificación y evaluación del riesgo

Fuente: Guía de Riesgos DAFP

Tipo:

Una vez identificado el activo y el riesgo, el tipo del riesgo se asoció a alguno de los pilares de la seguridad de la información:

- Disponibilidad
- Confidencialidad
- Integridad

4.3.1 Resultados de la identificación de riesgos de los activos de información

En total se identificaron 34 riesgos, 11 de los cuales se clasificaron el zona de riesgo E (Extrema), 12 en la zona de riesgos A (Alta), 9 en la zona de riesgo M (Media) y 2 en la zona de riesgo B (Baja). Se asociaron riesgos a todos los activos de información.

4.3.2 Matriz de identificación de riesgos de información

Matriz 2. Identificación y análisis de riesgos

Identificación y análisis de riesgos						
Programa de egresados						
Universidad Popular del Cesar Seccional Aguachica						
Confidencialidad: Solo fines educativos						
			Calificación			**Evaluación**
Código	**Activo**	**RIESGO**	**Probabilidad**	**Impacto**	**Tipo**	**Zona de Riesgo**
RE-1	Hoja de vida Académica del egresado	Conexiones de red pública sin protección	3	4	Confidencialidad	**E**
RE-2		Ausencia de "terminación de sesión" cuando se abandona la estación de trabajo	2	3	Confidencialidad	M
RE-3		Utilización de datos errados en los programas de aplicación	2	3	Integridad	M
RE-4		Ausencia de copias de respaldo	3	4	Disponibilidad	**E**
RE-5	Encuestas	Cambio en los datos de contacto de los usuarios	3	4	Integridad	**E**
RE-6		Datos provenientes de fuentes no confiables	3	4	Integridad	**E**
RE-7	Base de datos de egresados	Manipulación de terceros sobre la información	2	4	Confidencialidad	**A**

RE-8		Ausencia de copias de respaldo	2	3	Disponibilidad	M
RE-9		Corrupción de los datos	2	4	Integridad	A
RE-10	Hoja de vida profesional del egresado	Información desactualizada	3	3	Integridad	A
RE-11		Uso indebido de la información	2	3	Confidencialidad	M
RE-12		Perdida de la información	3	4	Disponibilidad	E
RE-13	Carné	Utilización de datos errados	2	3	Integridad	M
RE-14	Registro de Carnetización	Almacenamiento sin protección	3	2	Disponibilidad	M
RE-15	Registro de capacitaciones, conferencias, seminarios	Información desactualizada	1	4	Integridad	A
RE-16		Almacenamiento sin protección	3	4	Disponibilidad	E
RE-17	Listas de asistencia a capacitaciones, conferencias, seminarios	Ausencia de copias de respaldo	3	4	Disponibilidad	E
RE-18		Almacenamiento sin protección	3	4	Disponibilidad	E
RE-19	Comunicaciones públicas	Información desactualizada	1	1	Integridad	B
RE-20	Correo Electrónico	Ausencia de “terminación de sesión” cuando se abandona la estación de trabajo	2	4	Confidencialidad	A
RE-21	Almacenamiento de archivos en la nube	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	2	4	Disponibilidad	A
RE-22	Redes Sociales	Inseguridad de la arquitectura la red	2	4	Disponibilidad	A

RE-23	Portal de empleo	Inseguridad de la arquitectura la red	3	4	Disponibilidad	**E**
RE-24	Observatorio Laboral	Inseguridad de la arquitectura la red	2	4	Disponibilidad	**A**
RE-25	Blog	Inseguridad de la arquitectura la red	2	4	Disponibilidad	**A**
RE-26		Información desactualizada	3	4	Integridad	**E**
RE-27	Informes de gestión	Medios de almacenamiento o inexistentes	3	2	Disponibilidad	**M**
RE-28	Informes de estadísticas	Medios de almacenamiento o inexistentes	3	2	Disponibilidad	**M**
RE-29	SNIES	Inseguridad de la arquitectura la red	1	2	Disponibilidad	**B**
RE-30	Equipo de computo	Incumplimiento en el mantenimiento del equipo	3	4	Integridad	**E**
RE-31		Uso no autorizado del equipo	2	3	Confidencialidad	**M**
RE-32		Perdida de los servicios esenciales	4	3	Disponibilidad	**A**
RE-33	Profesional Universitario	Errores y omisiones no intencionales	2	4	Integridad	**A**
RE-34		Contratación provisional	1	4	Disponibilidad	**A**

4.4 Identificación de controles de riesgos asociados a los activos de información del programa de egresados de la UPC Seccional Aguachica

De acuerdo con (MINCTIC, 2016), pág. 34, *se busca escoger los controles que permitan disminuir los valores de exposición del riesgo, y luego se debe hacer un recalculo comparando nuevamente con los criterios establecidos y así buscar un nivel aceptable del riesgo en cada proceso para los temas de Seguridad.*

Una vez identificados los riesgos se procedió asociar posibles controles a cada uno de ellos, de igual forma que en los activos.

Código: Se estableció identificar los controles con la inicial C y la inicial de egresados E, y darles una secuencia numérica de números enteros.

Así: CE-1, CE-2, ……CE-n

Controles y tipo de control:

Para la asignación del control se tuvo en cuenta el tipo de control requerido, es decir de acuerdo a (MINCTIC, 2016) *Para hacer una clasificación y valoración de los controles, se debe tener en cuenta que en la guía, se presenta una clasificación entre dos tipos de Controles, Preventivos y Correctivos,*

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

4.4.1 Resultados de la identificación de controles de los riesgos de los activos de información

En total se identificaron 33 controles, 15 de los cuales se clasificaron correctivos y 18 preventivos. Después de esto, con la nueva clasificación de los riesgos se disminuyó la zona de riesgos y no se presenta ninguna extrema. La nueva clasificación presenta 9 riesgos en zona de riesgo Alta, 12 en zona Media y 12 en zona Baja.

4.4.2 Matriz de identificación de controles riesgos de información

Matriz 3. Identificación de controles y análisis de riesgos

Identificación de controles y análisis de riesgos													
Programa de egresados													
Universidad Popular del Cesar Seccional Aguachica													
Confidencialidad: Solo fines educativos													
			Calificación			**Evaluación**				**Nueva Calificación**		**Evaluación**	
Código	**Activo**	**RIESGO**	**Probabilidad**	**Impacto**	**Tipo**	**Zona de Riesgo**	Medida de Respuesta	**CONTROLES**	**TIPO DE CONTROL**	**Probabilidad**	**Impacto**	**Zona de Riesgo**	Medida de Respuesta
CE-1	Hoja de vida Académica del egresado	Conexiones de red pública sin protección	3	4	Confidencialidad	E	Reducir el Riesgo, Evitar, Compartir o Transferir	Procedimientos establecidos para la asignación de Roles y Perfiles dentro de la red	Preventivo	2	4	A	Reducir el Riesgo, Evitar, Compartir o Transferir
CE-2		Ausencia de "terminación de sesión" cuando se abandona la estación de trabajo	2	3	Confidencialidad	M	Asumir el riesgo, Reducir el Riesgo	Uso de parámetros de cierre de sesión automática por inactividad	Correctivo	1	2	B	Asumir el riesgo
CE-3		Utilización de datos errados en los programas de aplicación	2	3	Integridad	M	Asumir el riesgo, Reducir el Riesgo	Procedimiento de auditoria de datos	Preventivo	1	2	B	Asumir el riesgo
CE-4		Ausencia de copias de respaldo	3	4	Disponibilidad	E	Reducir el Riesgo, Evitar, Compartir o Transferir	Establecimiento de cronograma de backup	Preventivo	2	4	A	Reducir el Riesgo, Evitar, Compartir o Transferir

CE-5	Encuestas	Cambio en los datos de contacto de los usuarios	3	4	Integridad	E	Reducir el Riesgo, Evitar, Compartir o Transferir	Procedimiento establecido para implementar formato que pida varios datos de contacto	Preventivo	2	4	A	Reducir el Riesgo, Evitar, Compartir o Transferir
CE-6		Datos provenientes de fuentes no confiables	3	4	Integridad	E	Reducir el Riesgo, Evitar, Compartir o Transferir	Procedimiento de auditoria de validacion de datos	Preventivo	2	4	A	Reducir el Riesgo, Evitar, Compartir o Transferir
CE-7	Base de datos de egresados	Manipulación de terceros sobre la información	2	4	Confidencialidad	A	Reducir el Riesgo, Evitar, Compartir o Transferir	Establecimiento de contraseña de seguridad	Preventivo	1	3	M	Asumir el riesgo, Reducir el Riesgo
CE-8		Ausencia de copias de respaldo	2	3	Disponibilidad	M	Asumir el riesgo, Reducir el Riesgo	Establecimiento de cronograma de backup	Preventivo	1	2	B	Asumir el riesgo
CE-9		Corrupción de los datos	2	4	Integridad	A	Reducir el Riesgo, Evitar, Compartir o Transferir	Procedimiento de auditoria de validacion de datos	Preventivo	1	3	M	Asumir el riesgo, Reducir el Riesgo
CE-10	Hoja de vida profesional del egresado	Información desactualizada	3	3	Integridad	A	Reducir el Riesgo, Evitar, Compartir o Transferir	Protocolo de responsabilidad de la información por parte del egresado	Preventivo	2	3	M	Asumir el riesgo, Reducir el Riesgo
CE-11		Uso indebido de la información	2	3	Confidencialidad	M	Asumir el riesgo, Reducir el Riesgo	Protocolo de responsabilidad de uso por parte de la oficina de egresados	Preventivo	1	2	B	Asumir el riesgo
CE-12		Perdida de la información	3	4	Disponibilidad	E	Reducir el Riesgo, Evitar, Compartir o Transferir	Establecimiento de cronograma de backup	Preventivo	2	3	M	Asumir el riesgo, Reducir el Riesgo
CE-13	Carné	Utilización de datos errados	2	3	Integridad	M	Asumir el riesgo, Reducir el Riesgo	Procedimiento de auditoria de validacion de datos	Preventivo	1	2	B	Asumir el riesgo
CE-14	Registro de carnetización	Almacenamiento sin protección	1	4	Disponibilidad	A	Asumir el riesgo, Reducir el Riesgo	Fortalecer la infraestructura física	Correctivo	1	3	M	Asumir el riesgo, Reducir el Riesgo

CE-15	Registro de capacitaciones, conferencias, seminarios	Almacenamiento sin protección	1	4	Integridad	A	Reducir el Riesgo, Evitar, Compartir o Transferir	Fortalecer la infraestructura física	Correctivo	1	3	M	Asumir el riesgo, Reducir el Riesgo
CE-16	Listas de asistencia a capacitaciones, conferencias, seminarios	Ausencia de copias de respaldo	3	4	Disponibilidad	E	Reducir el Riesgo, Evitar, Compartir o Transferir	Establecimiento de cronograma de backup	Preventivo	2	4	A	Reducir el Riesgo, Evitar, Compartir o Transferir
CE-17		Almacenamiento sin protección	1	4	Disponibilidad	A	Reducir el Riesgo, Evitar, Compartir o Transferir	Establecimiento de cronograma de backup	Preventivo	1	3	M	Asumir el riesgo, Reducir el Riesgo
CE-18	Comunicaciones públicas	Información desactualizada	1	1	Integridad	B	Asumir el riesgo	Lista de chequeo para validación de información	Correctivo	1	1	B	Asumir el riesgo
CE-19	Correo Electrónico	Ausencia de "terminación de sesión" cuando se abandona la estación de trabajo	2	4	Confidencialidad	A	Reducir el Riesgo, Evitar, Compartir o Transferir	Uso de parámetros de cierre de sesión automática por inactividad	Preventivo	1	3	M	Asumir el riesgo, Reducir el Riesgo
CE-20	Almacenamiento de archivos en la nube	Disposición o reutilización de los medios de almacenamiento sin borrado adecuado	2	4	Disponibilidad	A	Reducir el Riesgo, Evitar, Compartir o Transferir	Lista de chequeo para validación de información	Correctivo	1	3	M	Asumir el riesgo, Reducir el Riesgo
CE-21	Redes Sociales	Inseguridad de la arquitectura la red	2	4	Disponibilidad	A	Reducir el Riesgo, Evitar, Compartir o Transferir	Implementación de mecanismos de seguridad	Correctivo	1	3	M	Asumir el riesgo, Reducir el Riesgo
CE-22	Portal de empleo	Inseguridad de la arquitectura la red	3	4	Disponibilidad	E	Reducir el Riesgo, Evitar, Compartir o Transferir	Implementación de mecanismos de seguridad	Correctivo	2	4	A	Reducir el Riesgo, Evitar, Compartir o Transferir
CE-23	Observatorio Laboral	Inseguridad de la arquitectura la red	1	2	Disponibilidad	B	Asumir el riesgo	Implementación de mecanismos de seguridad	Correctivo	1	2	B	Asumir el riesgo
CE-24	Blog	Inseguridad de la arquitectura la red	2	4	Disponibilidad	A	Reducir el Riesgo, Evitar, Compartir o Transferir	Implementación de mecanismos de seguridad	Correctivo	1	3	M	Asumir el riesgo, Reducir el

													Riesgo
CE-25		Información desactualizada	3	4	Integridad	E	Reducir el Riesgo, Evitar, Compartir o Transferir	Lista de chequeo para validación de información	Correctivo	2	4	A	Reducir el Riesgo, Evitar, Compartir o Transferir
CE-26	Informes de gestión	Medios de almacenamiento deteriorado o inexistentes	3	2	Disponibilidad	M	Asumir el riesgo, Reducir el Riesgo	Fortalecer la infraestructura física	Correctivo	2	2	B	Asumir el riesgo
CE-27	Informes de estadísticas	Medios de almacenamiento deteriorado o inexistentes	3	2	Disponibilidad	M	Asumir el riesgo, Reducir el Riesgo	Fortalecer la infraestructura física	Correctivo	2	2	B	Asumir el riesgo
CE-28	SNIES	Inseguridad de la arquitectura la red	1	2	Disponibilidad	B	Asumir el riesgo	Implementación de mecanismos de seguridad	Correctivo	1	2	B	Asumir el riesgo
CE-29		Incumplimiento en el mantenimiento del equipo	3	4	Integridad	E	Reducir el Riesgo, Evitar, Compartir o Transferir	Establecimiento de cronograma de mantenimiento de equipo	Preventivo	2	4	A	Reducir el Riesgo, Evitar, Compartir o Transferir
CE-30		Uso no autorizado del equipo	2	3	Confidencialidad	M	Asumir el riesgo, Reducir el Riesgo	Establecimiento de contraseña de seguridad	Preventivo	1	2	B	Asumir el riesgo
CE-31	Equipo de cómputo	Perdida de los servicios esenciales	4	3	Disponibilidad	A	Reducir el Riesgo, Evitar, Compartir o Transferir	Fortalecer la infraestructura física	Correctivo	3	2	A	Reducir el Riesgo, Evitar, Compartir o Transferir
CE-32		Errores y omisiones no intencionales	2	4	Integridad	A	Reducir el Riesgo, Evitar, Compartir o Transferir	Lista de chequeo para validación de información	Correctivo	1	3	M	Asumir el riesgo, Reducir el Riesgo
CE-33	Profesional Universitario	Contratación provisional	1	2	Disponibilidad	B	Asumir el riesgo	Capacitación al nuevo personal que se asigne	Preventivo	1	2	B	Asumir el riesgo

Conclusiones

Por medio del análisis de riesgos realizado en el programa de egresados de la Universidad Popular del Cesar Seccional Aguachica, se pudo identificar que el nivel de riesgo para la información es Alto. Este mismo análisis, permitió evaluar que se debe tomar medidas de reducción, eliminación o transferencia del riesgo.

En la identificación de los activos de información del programa de Egresados de la Universidad Popular del Cesar Seccional Aguachica, se pudieron encontrar 19 activos de información, asociados los siguientes procesos de seguimiento y acompañamiento, actualización de base de datos y administración y gestión de la información.

En la identificación de los riesgos de información del programa de Egresados de la Universidad Popular del Cesar Seccional Aguachica, se pudieron encontrar 34 riesgos, 11 de los cuales se clasificaron el zona de riesgo E (Extrema), 12 en la zona de riesgos A (Alta), 9 en la zona de riesgo M (Media) y 2 en la zona de riesgo B (Baja). Se asociaron riesgos a todos los activos de información.

En el análisis para la mitigación de los riesgos se identificaron 33 controles, 15 de los cuales se clasificaron como correctivos y 18 preventivos.

Con la nueva clasificación de los riesgos se disminuyó la zona de riesgos y no se presenta ninguna extrema. La nueva clasificación presenta 9 riesgos en zona de riesgo Alta, 12 en zona Media y 12 en zona Baja.

Finalmente se concluye, que este tipo de procesos está expuesto a un alto nivel de riesgos, por lo que es preciso que las IES articulen sus planes de desarrollo, con acciones para la seguridad de la información de los egresados.

Recomendaciones

Una vez concluido el Análisis De Riesgo De La Información Del Programa De Egresados De La Universidad Popular Del Cesar Seccional Aguachica, de acuerdo a la investigación se puede recomendar:

Socializar los resultados con la Alta Dirección para iniciar la implementación de los controles propuestos e iniciar con la gestión de los riesgos encontrados.

Una vez socializados los resultados, se recomienda escalar la investigación a los demás procesos institucionales, con el fin de iniciar la articulación de todos los activos de información de manera segura.

Articular al plan de desarrollo institucional y a los planes de acción anual, acciones de seguridad de la información de los egresados y los demás procesos de la institución.

Finalmente, teniendo en cuenta toda la exposición documental sobre la norma ISO-27005 realizada en el presente proyecto, se recomienda a la Institucion definir un Modelo de Seguridad y Privacidad de la Información con el fin de garantizar de forma adecuada los riesgos a los que se encuentra expuesto la información.

Referencias Bibliográficas

Abril, A., Pulido, J., & Bohada, J. (2013). *ANÁLISIS DE RIESGOS EN SEGURIDAD DE LA INFORMACIÓN.*

Areitio, J. (2008). *Seguridad de la información. Redes, informatica y sistemas de información.* Ediciones Paraninfo S.A.

De Freitas, V. (2009). *Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar.*

De Pablos Heredero, C. (2006). *Dirección y Gestión de los sistemas de informacion en la empresa.* ESIC EDITORIAL.

Del Carpio Gallego, J. (2006). *Análisis del riesgo en la administración de proyectos de tecnología de información.*

Guzmán, M. P. (2012). *Universidad Autonoma del Estado de Hidalgo*. Obtenido de https://www.uaeh.edu.mx/docencia/P_Presentaciones/prepa3/tipos_investigacion.pdf

Hernandez Sampieri, R. (2006). *Metodologia de la Investigación.* McGraw-Hili .

iso27000.es. (2005). Obtenido de **http://www.iso27000.es/iso27000.html**

López, M. I. (s.f.). *Analisis de Riesgos.* Gerente Network Security Team.

Merchán Paredes, L., & Gómez Mosquera, D. (2011). *Validación de un método ágil para el análisis de riesgos de la información digital.*

Ministerio de Tecnologías de Información y Comunicaciones MINTIC. (2016). *Guia 7. Guia para la gestion del riesgo.*

MINTIC. (2017). Guía para la Gestión y Clasificación de Activos de Información. *GUIA 5*, 4.

MINTIC. (07 de 2017). *http://www.mintic.gov.co*. Obtenido de http://www.mintic.gov.co/gestionti/615/w3-propertyvalue-7275.html

Ministerio de Educación Nacional. (Marzo de 2017). *Graduados Colombia. Observatorio Laboral para la Educación*. Obtenido de http://www.graduadoscolombia.edu.co/html/1732/w3-article-143157.html

Ministerio de Educación Nacional. (Marzo de 2017). *SACES Sistema de aseguramiento de la calidad en educación superior*. Obtenido de http://www.mineducacion.gov.co/sistemasdeinformacion/1735/article-221614.html

Ministerio de Educación Nacional. (Marzo de 2017). *SNIES Sistema Nacional de Información de la Educación Superior*. Obtenido de http://www.mineducacion.gov.co/sistemasdeinformacion/1735/w3-article-211868.html

Ministerio de Educación Nacional. (Marzo de 2017). *SPADIES Sistema para la Prevención de la Deserción en las Instituciones de Educación Superior*. Obtenido de http://www.mineducacion.gov.co/sistemasdeinformacion/1735/w3-article-254648.html

Ministerio de Educación Superior. (2013). *Lineamientos para solicitud, otorgamiento y renovación de registro calificado.*

Ministerio de Tecnologías de Información y Comunicaciones MINTIC. (2016). *Guia 7. Guia para la gestion del riesgo*

Namakforoosh, M. (2005). *Metodología de la investigación.* LIMUSA S.A.

Nepomuceno, A., Quesada, J. F., & Francisco, S. J. (2001). *Información: Tratamiento y Representación.* Sevilla: Universidad de Sevilla.

Scribd ISO-27005 - español. (Mayo de 2017). *Scribd ISO-27005 - español*. *seguridad27000*. (2013). Obtenido de **http://seguridad27000.blogspot.com.co/2013/10/historia-de-la-serie-27000.html**

UPC. (2005). ACUERDO 067 de 27 de diciembre de 2005 del CSU. Programa de Egresados.

Apéndices

Formato 4. Inventario Activos de Información

Inventario Activos de Información											
Programa de egresados Universidad Popular del Cesar Seccional Aguachica Confidencialidad: Solo fines educativos											
						Clasificación			**Criticidad**	**Propiedad**	
Código	**Proceso**	**Nombre del Activo**	**Observaciones**	**Tipo**	**Ubicación**	**Confidencialidad**	**Integridad**	**Disponibilidad**		**Propietario**	**Responsable**

Formato 5. Identificación y análisis de riesgos

Identificación y análisis de riesgos						
Programa de egresados **Universidad Popular del Cesar Seccional Aguachica** **Confidencialidad: Solo fines educativos**						
			Calificación			**Evaluación**
Código	**Activo**	**RIESGO**	**Probabilidad**	**Impacto**	**Tipo**	**Zona de Riesgo**

Formato 6. Identificación de controles y análisis de riesgos

Identificación de controles y análisis de riesgos

Programa de egresados
Universidad Popular del Cesar
Seccional Aguachica
Confidencialidad: Solo fines educativos

			Calificación			Evaluación				Nueva Calificación		Evaluación	
Código	Activo	RIESGO	Probabilidad	Impacto	Tipo	Zona de Riesgo	Medida de Respuesta	CONTROLES	TIPO DE CONTROL	Probabilidad	Impacto	Zona de Riesgo	Medida de Respuesta