UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGIAS
COORDINACION DE POSTGRADO

SISTEMATIZACION DE LA GESTION DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN EN LA RED DE LA UNIVERSIDAD CENTROCCIDENTAL "LISANDRO ALVARADO"

RAÚL JOSÉ GIL FERNÁNDEZ

Barquisimeto, Junio 2011

UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGIAS
COORDINACION DE POSTGRADO

SISTEMATIZACION DE LA GESTION DE RIESGOS DE LA SEGURIDAD DE LA INFORMACION EN LA RED DE LA UNIVERSIDAD CENTROCCIDENTAL "LISANDRO ALVARADO"

Trabajo de grado presentado para optar al grado de Técnico Superior
Especialista en Tecnologías de la Información y la Comunicación

Por: RAÚL JOSÉ GIL FERNÁNDEZ

Barquisimeto, Junio 2011

DEDICATORIA

A Dios por ser mi guía
A mis padres, hermanos y
demás familiares

AGRADECIMIENTO

A Dios, por ser mi guía en todo momento.

A mi madre por todo su apoyo.

A mis familiares por su ayuda.

A mi tutora Mailen Camacaro, por toda su ayuda, guía, sabiduría y orientación en el desarrollo de la investigación.

A los profesores Manuel Mujica, Euvis Piña y Carlos Primera por su disposición y colaboración.

Al personal de la Dirección de Telecomunicaciones, en especial a Junior Escalona por toda la información aportada

A mis compañeros de clases y amigos, Yliana, Jangely, Luis, Luisanny, Isis y Teresa.

Al personal de Postgrado, en especial a Elena, Carmela y Bethsay.

A Helen, Isabel, Yarilde, Glendy, Agustín, Francely, Karem, Niurka y Orlando por su ayuda.

A todos los profesores de Postgrado.

A todos aquellos que de alguna forma contribuyeron en el desarrollo de la investigación.

ÍNDICE GENERAL

ÍNDICE DE CUADROS

ÍNDICE DE GRÁFICOS

UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGIA
COORDINACION DE POSTGRADO

SISTEMATIZACIÓN DE LA GESTIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN EN LA RED DE LA UNIVERSIDAD CENTROCCIDENTAL "LISANDRO ALVARADO" (REDUCLA)

Autor: Ing. Raúl José Gil Fernández
Tutora: Dra. Mailen Camacaro
Fecha: Junio de 2011

RESUMEN

La presente investigación tuvo como propósito, presentar una propuesta para la Sistematización de la Gestión de Riesgos de la Seguridad de la información en la Red de la Universidad Centroccidental "Lisandro Alvarado", basada en la norma ISO/IEC 27001:2005. Esto motivado a la necesidad que tiene la Universidad de contar con una herramienta que le permita conocer los riesgos en su plataforma tecnológica y de esta forma aplicar controles de seguridad. Para este efecto, se desarrolló una investigación que se enmarca en una investigación de campo, de caráter no experimental, descriptiva, con el objetivo de Sistematizar la Gestión de Riesgos de seguridad de la información en la Universidad Centroccidental "Lisandro Alvarado" (RedUCLA). Para lograr el fin propuesto, se aplicó un (1) cuestionario con preguntas cerradas y dos (2) entrevistas con preguntas abiertas, con la finalidad de diagnosticar el proceso actual de la gestión de riesgos de seguridad de la información en la RedUCLA e identificar los componentes necesarios para diseñar el proceso para la sistematización de la gestión de riesgos. En los resultados obtenidos se encontró que las políticas de seguridad de seguridad no se encuentran actualizadas, la misma solo contempla la regulación de la gestión de riesgos a nivel lógico y un 86% de los usuarios la desconoce. Como resultado de la investigación, se hace necesario el diseño del proceso para la Sistematización de la Gestión de Riesgos de Seguridad de la Información en la Red de la Universidad Centroccidental "Lisandro Alvarado.

Palabras claves: Gestión de Riesgos, Seguridad de la Información, Norma ISO/IEC 27001:2005, Sistematización, Controles.

INTRODUCCIÓN

En la actualidad se están originando importantes cambios en nuestra sociedad relacionados con las tecnologías de la información que afectan a todos los ámbitos de la sociedad, como el económico, el educativo, el tecnológico y el normativo.

Estos cambios también han modificado la forma en que las organizaciones recogen, gestionan y trasmiten la información a través de diferentes medios como los son el Internet, la Intranet, la extranet y los sistemas de información. Todas estas acciones necesitan de protección.

Ante esta situación la Seguridad de la Información puede ser un excelente camino para mejorar aspectos relacionados con la actividad de una organización como su productividad, su competitividad, su capacidad de supervivencia ante desastres o la posibilidad de ofrecer garantías a sus clientes a modo de elemento diferenciador.

La seguridad de la información toma en cuenta leyes y normas que establecen criterios y medidas de seguridad no sólo desde un punto de vista lógicos y físicos, sino también organizativo y legal.

Dado este contexto, es necesario que las organizaciones conozcan los requerimientos de seguridad, que puedan comprometer la confidencialidad, disponibilidad o integridad de la información.

El propósito de esta investigación es la Sistematización de la Gestión de Riesgos de la Seguridad de la Información en la Red de la Universidad Centroccidental “Lisandro Alvarado”, basado en la norma ISO/IEC 27001:2005.

En este sentido, el trabajo de investigación consta de seis (6) capítulos:

El Capítulo I, Se plantea el problema que dio origen a la investigación, el objetivo general, los objetivos específicos, la justificación e importancia y por último el alcance.

El Capítulo II, denominado marco teórico, se presenta los antecedentes de la investigación, las bases teóricas, definición y operacionalización de las variables de la investigación.

El Capítulo III, se presenta el marco metodológico, contentivo del diseño y tipo de la investigación, la población y muestra, las técnicas e instrumentos de recolección de datos y finalmente las técnicas de procesamiento y análisis de los resultados.

El Capítulo IV, se refiere al análisis e interpretación de los resultados.

El Capítulo V, donde se exponen las conclusiones y recomendaciones de la investigación.

El Capítulo VI, representado por el Diseño del Proceso de Sistematización de la Gestión de Riesgos de la Seguridad de la Información en la Red de la Universidad Centroccidental "Lisandro Alvarado".

Por último, se presentan las referencias bibliografías y los anexos de la investigación.

CAPITULO I

EL PROBLEMA

Este capítulo expone el planteamiento del problema objeto de la investigación, del mismo modo se formulan el objetivo general y los objetivos específicos, además de la justificación del problema y el alcance.

PLANTEAMIENTO DEL PROBLEMA

En la actualidad, las organizaciones dependen cada día más de sus sistemas de información e infraestructuras tecnológicas, debido al auge producido por la implementación de tecnologías de información que facilitan la gestión adecuada y oportuna de la información generada por dichas organizaciones permitiendo así explorar mas allá de sus fronteras organizacionales.

Esto hace que las organizaciones y sus sistemas sean susceptibles a una serie de amenazas que pueden someter los activos críticos de información a diversas formas de fraude, sabotaje, delitos informáticos o destrucción de la plataforma tecnológica.

Los virus informáticos, los ataques de denegación de servicio son algunos ejemplos comunes y conocidos, pero también se deben considerar los riesgos de sufrir incidentes de seguridad causados voluntaria o involuntariamente desde dentro de la propia organización o aquellos provocados accidentalmente por catástrofes naturales y fallos técnicos. Todas las organizaciones, bien sean grandes, pequeñas, privadas o públicas, están expuestas a estos tipos de fenómenos, por lo que se hace necesario estar prevenidos ante cualquier tipo de inconveniente.

Cabe destacar un estudio realizado por Symantec (2010), donde se encuestaron 2.100 directores informáticos de empresas en 27 países. El estudio arrojó que el 42%

de las empresas para las cuales trabajan consideran la seguridad de información en sus organizaciones como un riesgo, mientras que un 75% indicaron que sus empresas han sufrido ataques cibernéticos en los últimos meses, causando grandes pérdidas de dinero. Dichos directivos informaron que la seguridad de información de la empresa es cada vez más difícil debido a factores como: la escasez de personal especializado en seguridad, la plataforma e infraestructura tecnológica como servicios y los problemas de cumplimiento de las normas de Tecnología de Información (TI) que intensifican los problemas de seguridad.

Por otra parte Ramio (2006), señala que la seguridad Informática es "un conjunto de métodos y herramientas destinadas a proteger la información y por ende los sistemas informáticos ante cualquier amenaza, un proceso en el cual además participan las personas" (p.50). De allí su importancia, la cual es necesaria para mantener la confidencialidad, integridad y disponibilidad de la información; así como para resguardar los activos tecnológicos de la organización.

Por lo tanto, la seguridad de la información constituye un proceso que ayuda a las organizaciones a tomar medidas para garantizar que la misma sea gestionada correctamente, haciendo uso de un proceso sistemático, documentado y conocido por toda la organización, desde un enfoque de riesgo organizacional; asegurando la evolución eficiente de la seguridad de los sistemas de Información y sus infraestructuras frente a todos los probables incidentes que pudiesen afectarla.

Resulta oportuno mencionar que a nivel internacional existen normas que permiten gestionar la seguridad de la información, entre ellas se encuentra la norma ISO/IEC 27001:2005, la cual evolucionó de la BS 7799-2.

La finalidad de la norma es permitir de forma sistemática minimizar el riesgo y proteger la información en las organizaciones, garantizando la selección de controles de seguridad adecuados y proporcionales; además, de adoptar un enfoque por procesos para establecer, implantar, operar, supervisar, revisar, mantener y mejorar un Sistemas de Gestión de Seguridad de la Información (SGSI). Esta norma responde a la necesidad de proporcionar una base común a las organizaciones desde la óptica técnica, organizativa y jurídica; cuyo cumplimiento implique que la organización

mantenga una infraestructura y un esquema de funcionamiento que le garanticen la seguridad de la información que manejan.

Se puede acotar, Países como España y Gran Bretaña han avanzado significativamente en la adopción de esta norma en sus organizaciones, ya que constituyen un medio que les permite gestionar la seguridad con el fin de disminuir el riesgo o vulnerabilidad de la información generada en todos los procesos de negocio (Serrera, 2010).

En el caso de las organizaciones venezolanas de acuerdo a un estudio realizado por Espiñeira, Sheldon y Asociados (2008), encontró que el 91% de las organizaciones manifestó conocer las mejores prácticas y estándares internacionales de seguridad y tecnología de información, pero al momento de indagar en el caso de adopción e implementación de estándares como parte de la gestión de seguridad, comentan que a Venezuela le falta un largo camino por recorrer, ya que se encontró que un 78% de las organizaciones no ha adoptado el estándar ISO/IEC 27001:2005 como medio que les permita gestionar la seguridad de la información.

En este orden de ideas, conviene que las organizaciones adopten normas que les permita gestionar la seguridad de la información que ellas manejan, frente a los riesgos que pudiesen afectarla. Indagando sobre esta materia en el sector educativo universitario en Venezuela, es obvio que las universidades manejan grandes volúmenes de información, razón por la cual con la incorporación de las tecnologías de información, han buscado de alguna manera no solo agilizar sus procesos, sino proporcionar la seguridad necesaria para el resguardo de sus activos de información.

Es oportuno mencionar que De Freitas (2009). Realizó un Análisis y evaluación del riesgo de la información donde 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, en donde concluyo 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 la norma ISO 27001:2005, para cada uno de dichos activos.

Es por ello que la Universidad Centroccidental “Lisandro Alvarado” (UCLA), institución de educación superior pública ha incorporado en sus procesos nuevas tecnologías de información que han contribuido a su cambio estructural como institución de educación superior, lo que constituye una condición imprescindible para que la universidad pueda continuar cumpliendo su función y compromiso fundamental en las sociedades presentes y futuras.

En efecto la UCLA desde el año 1996 inició su proceso de adecuación tecnológica en una moderna infraestructura llamada RedUCLA, donde se interconectó todas las dependencias de la institución a través de una red de fibra óptica, para la integración de los servicios de voz, dato y video. A su vez se desarrolló y estandarizó el uso de las redes LAN en cada una de las edificaciones, al implementarse el cableado estructurado, lo que permitió distribuir físicamente puntos de voz y datos en todas las áreas: docencia, laboratorios, bibliotecas, investigación y administrativo; toda esta infraestructura tecnológica es mantenida y gestionada por la Dirección de Telecomunicaciones.

Todos estos cambios han sido ventajosos en muchos aspectos como ha sido la masificación del uso de las tecnologías de información por parte de la comunidad universitaria de una forma accesible, eficiente y eficaz para minimizar las actividades administrativas y docentes de la institución.

Asimismo, el desarrollo, implementación y ejecución de sistemas académicos y administrativos ha generado la dependencia de los usuarios a la red a causa de todos los servicios que por ella transitan.

Sin embargo, estos cambios generan que la red se exponga a problemas propios de cualquier sistema en red, que pudieran afectar directamente su funcionamiento o actividades.

Siendo el interés de esta investigación abordar esta problemática que en parte ha sido indagada por el investigador a través de la técnica de observación directa, dado que realizo ayudantías de servicios en el departamento de redes de datos de la UCLA y además este proceso se evidencio aun más, a través de la aplicación de una entrevista no estructurada al Jefe del Departamento de Redes de Datos, observándose

que dicha problemática en cuanto a los Riesgos de Seguridad de la información, se encuentra el uso no adecuado de los recursos de la red, infecciones de virus que afectan los sistemas y/o aplicaciones; incidentes de seguridad que han sido ocasionados por los usuarios bien sea de manera voluntaria o involuntaria.

Asimismo, se encuentra la ausencia de políticas que permita controlar el uso o implementación de los sistemas y servicios apoyados en la red, la ausencia de mecanismos para la adecuada gestión de riesgos de seguridad de la información que permita detectar las amenazas y vulnerabilidades presentes y la adecuación de la misma a los nuevos cambios.

Dado este contexto, se evidencia la importancia de realizar una Sistematización de la Gestión de Riesgos de la Seguridad de la Información basado en la norma ISO/IEC 27001:2005, que permita conocer los riesgos a los que se encuentra expuesta la red; además de conocer la gestión actual de la misma y cuáles pueden ser las alternativas para poder mejorarlos.

Por lo antes expuesto, se propone Sistematizar la Gestión de Riesgos de la seguridad de la información en la Red de la Universidad Centroccidental "Lisandro Alvarado" (RedUCLA), tomando como referencia la norma ISO/IEC 27001:2005, para la cual se plantean las siguientes interrogantes:

¿Cuál es el proceso actual de la Gestión de Riesgos de la Seguridad de la Información en la Red de la Universidad Centroccidental "Lisandro Alvarado"?

¿Cuáles son los componentes necesarios para diseñar el proceso de Sistematización de la Gestión de Riesgos de la Seguridad de la Información en la Red de la Universidad Centroccidental "Lisandro Alvarado"?

¿Cómo será el diseño del proceso de sistematización?

Para responder a las interrogantes planteadas se formularon los siguientes objetivos.

OBJETIVOS DE LA INVESTIGACIÓN

Objetivo General

Sistematizar la Gestión de Riesgos de la seguridad de la información en la Red de la Universidad Centroccidental “Lisandro Alvarado”

Objetivos Específicos

1. Diagnosticar el proceso actual de la Gestión de Riesgos de la Seguridad de la Información en la Red de la Universidad Centroccidentral “Lisandro Alvarado”
2. Identificar los componentes para diseñar el proceso para la Sistematización de la Gestión de Riesgos de la Seguridad de la Información en la Red de la Universidad Centroccidental “Lisandro Alvarado”
3. Presentar el diseño del proceso para la Sistematización de la Gestión de Riesgos de la Seguridad de la Información en la Red de la Universidad Centroccidental “Lisandro Alvarado”

JUSTIFICACIÓN E IMPORTANCIA

Es evidente, el auge que ha obtenido la seguridad de la información en la últimas décadas en la organizaciones, con la incorporación del Internet y de las Tecnologías de Información y Comunicación (TIC) en sus procesos de negocios. Debido a que la seguridad de la información busca proteger a la información de una amplia gama de amenazas que puedan causarle daño, preservando la confidencialidad, integridad y disponibilidad de sus sistemas de información, así como los medios para su tratamiento dentro de una organización.

Es por ello, que se hace necesario que las organizaciones conozcan y afronten de una manera ordenada los riesgos a los que está sometida su información, a través de procedimientos adecuados que les permitan conocer las amenazas y vulnerabilidades a los que se enfrentan sus sistemas e infraestructura tecnológica y de esta forma aplicar controles de seguridad basados en una evaluación de los riesgos.

Dado este contexto, se hace oportuno proponer la Sistematización de Gestión de Riesgos de la Seguridad en la Red de la UCLA, en base a estándares internacionales, que permita la detección a tiempo de las amenazas y vulnerabilidades en su plataforma tecnológica, con el objetivo de garantizar la continuidad de la operatividad de la organización y minimizar el impacto si algunos de los riesgos se llegaran a materializar.

La sistematización de la gestión de riesgos de la Seguridad de la Información permitirá a través de un conjunto de normas y procedimientos administrar los incidentes de seguridad que se puedan presentar de acuerdo a los objetivos de la organización, para la toma de decisiones en un ambiente de incertidumbre sobre una acción que pueda suceder y las consecuencias que existirá si esta acción ocurre.

Por lo anteriormente señalado, la presente investigación es de una trascendencia social educativa, puesto que con la realización de dicho estudio se pretende dar un aporte al conocimiento en relación a la línea de investigación. Por cuanto constituye una contribución a los actores involucrados en el quehacer pedagógico, frente a la necesidad que tienen los administradores de la RedUCLA de conocer las amenazas y vulnerabilidades existentes, además de obtener un diagnóstico sobre el estado de seguridad de la información de la Red de la universidad.

Con este estudio se espera que la universidad defina políticas de seguridad, normas y procedimientos de trabajo que permita controlar los problemas detectados y disminuir de manera significativa el impacto de los riesgos. También servirá de ayuda y orientación para realizar investigaciones posteriores que tengan como finalidad la Sistematización de la Gestión de Riesgos de seguridad de la información.

Por último, se espera que esta investigación sirva de base a universidades con problemáticas de seguridad de información similares.

ALCANCE

El alcance de este trabajo de investigación está centrado en presentar el diseño de la Sistematización de la Gestión de Riesgos de la Seguridad de la Información en la Red de la Universidad “Lisandro Alvarado” tomando como referencia el estándar ISO/IEC 27001:2005, con la finalidad de analizar y gestionar los riesgos de seguridad a la que se expone la red de la Universidad.

CAPITULO II

MARCO TEÓRICO

Este capítulo incluyó la fundamentación teórica que sustentan a la investigación realizada. En éste se citaron investigaciones que han contribuido a generar antecedentes de la investigación; asimismo, se presentaron las bases teóricas, Luego se presentan las bases legales que tienen correspondencia con la investigación y por último la operacionalización de las variables.

ANTECEDENTES DE LA INVESTIGACION

En relación a la problemática planteada, se tomaron como referencia un conjunto de estudios previos relacionados con el tema objeto de estudio, que dan soporte bibliográfico y referencial en el desarrollo del estudio planteado.

Mendoza (2010), desarrollo un trabajo de grado titulado ***Sistema de Gestión para la Seguridad de la Información. Caso Centro de Tecnología de la Información y Comunicación del Decanato de Ciencias y Tecnología (CTIC) – UCLA***. La investigación consistió en evaluar las amenazas y riesgos a la que estaban sometidos los activos del CTIC, precedida por un diagnostico de la situación actual en materia de seguridad de la información; tomando como referencia el estándar internacional ISO/IEC 27001:2005 y los controles propuestos en la norma ISO/IEC 27002:2005.

La investigación permitió descubrir que las medidas actuales de control implementadas por el CTIC para satisfacer los requisitos mínimos de seguridad han sido efectivas solo parcialmente. El tipo de investigación empleada fue la de proyecto factible apoyado en la investigación monográfica documental y de campo.

Las conclusiones del trabajo describe la necesidad de adoptar una metodología solida para la gestión de riesgos que permite descubrir los puntos vulnerables de un sistema de información y tomar los correctivos necesarios.

La relación de este trabajo con la investigación objeto de estudio, se basa en la utilización del estándar ISO/IEC 27001:2005 como herramienta de apoyo para el análisis y gestión de riesgos de la información.

Matalobos (2009), elaboró una investigación titulada ***Análisis de Riesgos de la Seguridad de la Información***. El proyecto consistió en la realización de un análisis de riesgos de seguridad de la información que permitió cuantificar y comparar los requerimientos de seguridad de la información de la organización con los controles implantados para su cumplimiento. El método de trabajo implementado se basó en las principales metodologías de análisis y gestión de riesgos de uso habitual en el mercado de la seguridad de la información y en las necesidades de la organización.

El autor concluyó que identificando los principales activos de información de la organización en términos de los requerimientos de seguridad definidos, permite identificar las áreas que requieren mayor atención.

Este trabajo hace un aporte teórico importante para el análisis y gestión de riesgos basados en el estándar ISO/IEC 27001:2005, además de explicar distintas herramientas para el análisis de riesgos.

Tersek (2008), en su trabajo titulado ***Sistema de Gestión de Seguridad de la Información***, tiene como objetivo general establecer un sistema de gestión de seguridad de la información para un sistema de información tomando como caso de estudio el Sistema Administrativo (SAI) en la Universidad Nacional Experimental Politécnica "Antonio José de Sucre", Vicerrectorado de Puerto Ordaz. Toma como referencia la Norma ISO 27001:2005 y hace uso de una combinación de metodologías y herramientas para la evaluación de los riesgos que ayuda a la toma de decisión sobre las opciones de tratamiento de riesgos adecuados. La investigación se desarrolló bajo la modalidad de proyecto factible, con apoyo del estudio de campo y de investigación documental.

El autor concluyó que no se lleva una correcta administración y control de la red, es decir, no se implementan todas las medidas posibles para evitar amenazas y mantener la seguridad de los sistemas y aplicaciones que circulan por ella.

Este trabajo se relaciona con la investigación objeto de estudio debido a que presenta una guía metodológica para la gestión de riesgos de seguridad de la información, basados en el estándar ISO/IEC-27001:2005 y al aporte teórico en el área de seguridad de información, así como herramientas para el análisis y evaluación de riesgos.

Mujica (2007), en su trabajo titulado ***Diseño de un Plan de Seguridad Informática para la Universidad Nacional Experimental Politécnica Antonio José de Sucre, sede rectoral Barquisimeto***. El proyecto consistió en diseñar un plan de seguridad Informática para la Universidad Experimental Politécnica Antonio José de Sucre para dar respuesta a un conjunto de incidentes de seguridad en los servicios de información, así como la no existencia de un plan de seguridad que logre minimizar los riesgos ante las amenazas.

La investigación se concibió como un proyecto factible, desarrollada metodológicamente a través de las cuatro fases fundamentales en la formulación de un proyecto de este tipo como son: Fase I Diagnóstico; Fase II Factibilidad; Fase III Diseño del Plan de Seguridad Informática y Fase IV Evaluación del diseño del Plan de Seguridad Informática.

Dentro de las conclusiones obtenidas por el autor se puede considerar que no existen planes de sensibilidad en seguridad de la información dentro de la Universidad, debido al desconocimiento por parte del personal de las políticas de seguridad de información, del plan de continuidad del negocio y del plan de recuperación ante desastres. Por lo que el autor recomienda en primer lugar, aplicar el Plan de Seguridad Informática en todos los Vicerrectorados de la Universidad, además de difundir en la institución las políticas de seguridad de la información.

La relación de este estudio con la presente investigación es que el mismo se realizó en una institución de educación superior y se utilizó la norma ISO/IEC

27001:2005 para el control de los riesgos, sirviendo de base por presentar una problemática similar.

Villasmil (2007), en su trabajo titulado ***Análisis de Riesgos de Seguridad Informática para las Pequeñas y Medianas Empresas (PYMES) Usando el Estándar ISO 17799 para la Definición de Políticas de Seguridad que Protejan sus Sistemas de Información***. El proyecto consistió en Analizar los Riesgos en Seguridad Informática en las PYMES, usando el estándar ISO-17799 para la definición de políticas de seguridad, que permitan proteger sus Sistemas de Información, con la finalidad de apoyar y mejorar el desempeño de este grupo empresarial. Utilizando como metodología una investigación de campo no experimental descriptivo.

La autora encontró que la mayoría de las empresas encuestadas, tienen niveles de protección simple para sus sistemas de información, lo que conlleva que enfrenten riesgos para su información.

Este estudio se relaciona con la presente investigación debido a la metodología implementada, además de aporte teórico en el área de seguridad informática.

En conclusión, todos los trabajos citados anteriormente guardan relación entre sí y sirvieron de base para la presente investigación. Entre los aspectos que más se resaltan es que la seguridad de la información es un factor de gran importancia para las organizaciones ya que proporciona integridad, confidencialidad y disponibilidad de los datos y la utilización de normas internacionales para el logro de una adecuada evaluación y gestión de los riesgos.

BASES TEÓRICAS

Las bases teóricas, ubican el problema dentro de todos los fundamentos teóricos que permiten aclarar los conceptos relativos a Sistematización, Sistemas de Información, Seguridad de la Información, Riesgos, Análisis y Gestión de Riesgos de la Información; así como todo lo referente a controles y normas que permitan la disminución de riesgos en la REDUCLA. A continuación se exponen los conceptos fundamentales que soportan la investigación.

Sistematización

Según Alvarado (1998), la sistematización consiste en la aplicación de diferentes técnicas que permitan una mejor distribución del trabajo, el establecimiento de responsabilidades y visualizar la participación de los distintos niveles administrativos en un procedimiento específico.

En efecto, se puede decir que la sistematización consiste en un conjunto de procedimientos orientados a dar una secuencia lógica a los procesos para alcanzar un resultado, de esta forma obtener información oportuna y confiable para la toma de decisiones.

Para la presente investigación, la sistematización realizada se orientó en dar una secuencia lógica al proceso de gestión de riesgos de seguridad de la información, a través de un conjunto de normas y procedimientos que permita el análisis y gestión de los riesgos de la seguridad de la información en la Red de la Universidad.

Sistemas de Información

Según Oz (2001), en una organización un sistema de información está formado por varios componentes: datos, hardware, software, personas y procedimientos, todos con los puntos fuertes y débiles. Con el objetivo común de producir la mejor información a partir de los datos disponibles.

Por otra parte, O´Brien (2001) define sistemas de información como: "una combinación organizada de personas, hardware, software, redes de comunicaciones y recursos de datos que reúne, transforma y disemina información en una organización" (p.9)

En efecto, los sistemas de información son un conjunto de elementos organizados, relacionados y coordinados entre sí, que facilitan el funcionamiento general de una organización para el logro de sus objetivos, de allí la importancia de que las organizaciones, se aboquen a medidas de control que apoyen la seguridad de la información.

Seguridad de la Información

Según Maiwald (2003), la seguridad de la información se define como las "medidas adoptadas para evitar el uso no autorizado, el mal uso, la modificación o la denegación del uso de conocimientos, hechos, datos o capacidades".(p.4)

Por su parte Espiñeira y otros (2005), la definen como "la encargada de proteger los activos de información de una organización contra pérdidas o el uso indebido de la misma, además de permitir el acceso a los activos de la información, dando apoyo a los objetivos de la información."(p.1)

La Seguridad de la Información ayuda a identificar los riesgos y las amenazas a las que están expuestas las organizaciones, en qué medida las pueden afectar y cómo se pueden minimizar. Además permite establecer pautas y procedimientos en caso que se produzca algún desastre.

Al mismo tiempo, resulta oportuno mencionar que muchas veces los fallos de seguridad son ocasionados por la errónea percepción de que si la seguridad física está razonablemente asegurada, no tiene por qué haber problemas. O que protegiendo únicamente las aplicaciones y las bases de datos ya está garantizada la seguridad. Con esos supuestos se dejan desprotegidas muchas áreas de la organización, muchos activos de información que pueden ser fácilmente dañados o destruidos, ya que no se han tenido en cuenta todos los aspectos de la seguridad de la información: la seguridad física, la seguridad lógica y las medidas organizativas. (INTECO, 2010)

Es importante destacar, lo señalado por Interity (2010) en su portal web donde indica que la seguridad de la información no es sinónimo de seguridad informática. La seguridad de la información efectivamente incluye aspectos técnicos, pero se extiende también al ámbito de la organización y contempla aspectos jurídicos.

En este sentido, la seguridad de la información tiene que establecer las medidas necesarias que permitan proteger la confidencialidad, la integridad y la disponibilidad de la información.

Propiedades de la seguridad de la Información

Los sistemas de seguridad de la información se fundamentan en tres propiedades o principios básicos que debe cumplir todo sistema informático como lo son:

Confidencialidad: la información no se pone a disposición ni se revela a individuos, entidades o procesos no autorizados. (ISO/IEC 17799:2005)

Integridad: mantenimiento de la exactitud y completitud de la información y sus métodos de procesos. (ISO/IEC 17799:2005)

Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran. (ISO/IEC 17799:2005)

Además, la norma explica que también pueden estar involucradas otras propiedades como la autenticidad, responsabilidad, no-repudio y confiabilidad.

Por tanto, estas propiedades son elementos a proteger para el logro de sus objetivos.

Objetivos de la Seguridad de la Información

Oz (2001), expresa que el propósito de las medidas de seguridad y control es mantener la funcionalidad de los SI, la confidencialidad de la información, la integridad y disponibilidad de los datos y recurso de procesamiento de datos, además del cumplimiento de leyes de seguridad y privacia.

El autor explica que los principales objetivos de la seguridad en la información son:

- Reducir el riesgo de que los sistemas y las organizaciones cesen sus operaciones.
- Mantener la confidencialidad de la información.
- Asegurar la integridad y confidencialidad de los datos.
- Asegurar la disponibilidad de los datos o la información.

- Asegurar el cumplimiento de las leyes de seguridad nacionales de seguridad de la información y reglas de privacía.

Para planear medidas que ayuden a lograr estos objetivos, las organizaciones primero deben de estar conscientes de los riesgos potenciales a los que se enfrentan sus recursos de información (que incluye hardware, aplicaciones, datos, redes), entonces deben establecer medidas de seguridad para protegerse contra esos riesgos.

Asimismo, la Seguridad de la Información toma en cuenta la protección de la información desde tres puntos de vista: técnico (lógico y físico), organizativo y legal.

Tipos de seguridad

El estudio de la seguridad de la Información podría plantearse desde los siguientes enfoques o tipos:

Seguridad Física

Según Donado, Agreda y Carrascal (2002), son mecanismos que permiten asegurar el correcto funcionamiento de aquellos recursos físicos o equipos computacionales (servidores, estaciones de trabajo, router, switches, backbone, entre otros) que intervienen en el manejo y administración de los sistemas de información.

En tal sentido Ramio (2006), la asocia a la protección del sistema ante las amenazas físicas, incendios, inundaciones, edificios, cables, control de accesos de personas, entre otros.

Seguridad Lógica

La seguridad lógica pretende proteger el patrimonio informacional que se compone tanto de las aplicaciones informáticas como del contenido de las bases de datos y de los ficheros. La protección de este tipo se puede realizar a través de contraseñas, tanto lógicas como biométricas, conocimientos y hábitos del usuario, firmas digitales y principalmente la utilización de métodos criptográficos. (Camacaro, 2009)

Seguridad Organizacional Administrativa

Pretende cubrir el hueco dejado por las dos anteriores y viene en cierto modo a complementarlas. Es difícil, lograr de forma eficaz la seguridad de la información si no existen claramente definidas: las Políticas de seguridad, Políticas de personal, Políticas de contratación Análisis de riesgos y los Planes de Contingencia. (Camacaro, 2009)

Seguridad Jurídica o Legal

Su objetivo es lograr a través de la aprobación de normas legales, poder fijar el marco jurídico necesario para proteger los bienes informáticos y la información generada a través de estos. (Camacaro, 2009)

De acuerdo al tipo de seguridad de la información que se analice, es importante identificar los riesgos que se presentan en la misma.

Riesgos de seguridad de la información

Para toda organización es importante conocer los riesgos a los que se están sometidos sus procesos y actividades. Por medio de procedimientos de control, evaluar el desempeño de entorno de seguridad de la información.

En este sentido CSAE (2010), definen el riesgo como la estimación del grado de exposición a que una amenaza se materialice sobre uno o más activos causando daños o perjuicios a la Organización.

Por otro lado, Sena y Tenzer (2004), lo definen como “aquella eventualidad que imposibilita el cumplimiento de un objetivo.” (p. 2)

Sobre la base de las consideraciones anteriores, el riesgo en la seguridad de la información es definido por la ISO/IEC 27005 como el “potencial de que una amenaza determinada explote las vulnerabilidades de los activos causando así daño a la organización” (p.2)

En consecuencia, el riesgo se refiere grado de exposición a los que se encuentran sometidos los activos frente a una amenaza o a lo que le podría pasar si no se protegen adecuadamente.

Evaluaciones de Riesgos de Seguridad de la Información

De acuerdo a la norma ISO/IEC 27002, las evaluaciones de riesgo debieran identificar, cuantificar y priorizar los riesgos en comparación con el criterio para la aceptación del riesgo y los objetivos relevantes para la organización. Los resultados debieran guiar y determinar la acción de gestión apropiada y las prioridades para gestionar los riesgos de la seguridad de la información para implementar los controles seleccionados para protegerse contra los riesgos. Es posible que el proceso de evaluación de riesgos y la selección de controles se deba realizar un número de veces para abarcar las diferentes partes de la organización o sistemas de información individuales.

La evaluación del riesgo debiera incluir el enfoque sistemático de calcular la magnitud de los riesgos (análisis de riesgo) y el proceso de comparar los riesgos estimados con un criterio de riesgo para determinar la importancia de los riesgos (evaluación de los riesgos)

Las evaluaciones también debieran realizar periódicamente para tratar los cambios en sus requerimientos de seguridad y en la situación del riesgo; ejemplo, en los activos, amenazas, vulnerabilidades, impactos, evaluación del riesgo, y cuando ocurren cambios significativos. Estas evaluaciones se debieran de realizar de una manera metódica capaz de producir resultados comparables y reproducibles.

La evaluación del riesgo de seguridad de la información debiera tener un alcance claramente definido para ser efectiva y debiera incluir las relaciones con las evaluaciones de riesgo en otras áreas, si fuese apropiado.

En este orden de ideas, la evaluación de riesgos permitirá conocer las amenazas, vulnerabilidades y que características son de interés en cada activo, así saber en qué medida estas características están en peligro y de esta forma poder analizar el sistema.

El proceso de conocimiento de los riesgos incluye las siguientes etapas:

1. **Análisis de riesgos:** proceso sistemático para estimar la magnitud de los riesgos a que está expuesta una Organización.(Magerit,2006)
2. **Gestión de riesgos:** Selección e implantación de controles para conocer, prevenir, impedir, reducir o controlar los riesgos identificados. Una opción legítima es aceptar el riesgo. También se tiene que la seguridad absoluta no existe; en efecto, hay que aceptar un riesgo solo si se es conocido y ha sido evaluado de acuerdo a los requerimientos de seguridad. (Magerit,2006)

Estos procesos implican la decisión de aceptar un cierto nivel de riesgos, saber cuáles son las condiciones de trabajo. De esta forma poder aplicar los controles necesarios que permitan mitigar los riesgos y de una forma metódica tomar decisiones con fundamento y explicar racionalmente las decisiones tomadas.

Análisis y Gestión de Riesgos de la Seguridad de los Sistemas de Información

De acuerdo a Cao (2004), el proceso de análisis y gestión de riesgos ayuda a identificar todos los activos importantes para la seguridad de los sistemas de información, las amenazas que puedan afectarles, identificar la vulnerabilidad de cada uno de ellos frente a esas amenazas y calcular los riesgos existentes de un posible impacto sobre el activo.

CSAE (2010), explica que para una correcta definición e implantación de la seguridad, es necesario identificar y determinar los diferentes elementos significativos dentro del entorno de la seguridad de los sistemas de información. Es por ello que en todo proceso de análisis y gestión de riesgos se presentan elementos considerados significativos para el estudio de la seguridad de la información.

A continuación se presentan los elementos considerados significativos por MAGERIT y la norma ISO/IEC 27001:2005 para el estudio de la Seguridad en Sistemas de Información.

Activos: recursos del sistema de información o relacionados con éste, necesarios para que la organización funcione correctamente y alcance los objetivos propuestos por la dirección.

Amenazas: eventos que pueden desencadenar un incidente en la organización, produciendo daños materiales o pérdidas inmateriales en sus activos.

Vulnerabilidad de un activo: potencialidad o posibilidad de ocurrencia de la materialización de una amenaza sobre dicho activo.

Valoración de Activo: estimar qué valor tiene el activo para la organización, cual es su importancia para la misma.

Impacto en un activo: consecuencia sobre éste de la materialización de una amenaza.

Riesgo: probabilidad de que las amenazas exploten las vulnerabilidades y causen pérdidas o daños a los activos.

Riesgo = Vulnerabilidad + Amenazas

Análisis de riesgos: uso sistemático de la información para identificar fuentes y para estimar el riesgo.

Evaluación de riesgo: proceso de comparar el riesgo estimado con el criterio de riesgo dado para determinar la importancia del riesgo.

Gestión de riesgo: actividades coordinadas para dirigir y controlar una organización con relación al riesgo.

Tratamiento del riesgo: proceso de tratamiento e implementación de medidas para modificar el riesgo

Control: Medios para manejar el riesgo; incluyendo políticas, procedimientos, lineamientos, prácticas o estructuras organizacionales, las cuales pueden ser administrativas, técnicas, de gestión o de naturaleza legal.

Requerimientos de seguridad: procedimiento, dispositivo, físico o lógico, que reduce el riesgo.

En el gráfico 1 se ilustra el proceso de evaluación de riesgo.

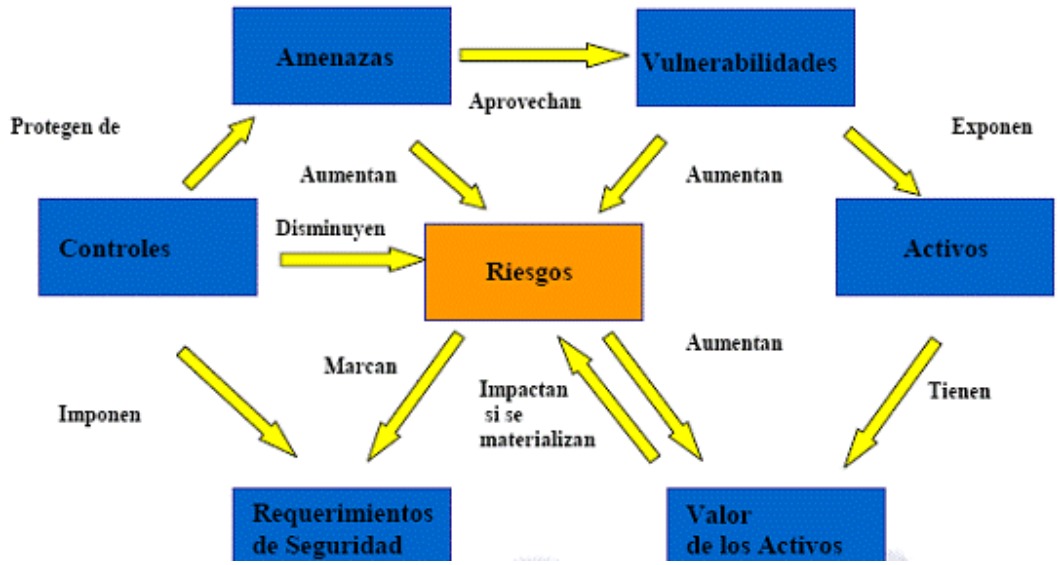

Gráfico 1. Proceso de evaluación del riesgo

Fuente: iso27001.es

Análisis de riesgos:

El análisis de riesgo tiene como propósito determinar los componentes de un sistema que requiere protección, las vulnerabilidades que lo debilitan y las amenazas que lo ponen en peligro, con el fin de valorar su grado de riesgo. (Erb, 2008)

En base a lo antes expuesto, se puede decir que el análisis de riesgos sirve para identificar las variadas formas en que los datos y otros activos informáticos se exponen a amenazas y cuáles son las consecuencias para la organización de dichas exposiciones.

Su importancia radica en que es una herramienta que nos va a permitir identificar las amenazas a los que se encuentran expuesto los activos organizacionales, además de estimar su frecuencia de materialización y valorar el impacto.

Para ello, la norma ISO/IEC 27001 establece una serie de paso para la realización de un análisis de riesgos enfocado a la implementación de un sistema de gestión de seguridad de la información (SGSI):

(a) Identificar los riesgos:

1. Identificar los activos que están dentro del alcance del SGSI y a sus responsables directos, denominados propietarios;
2. Identificar las amenazas en relación a los activos;
3. Identificar las vulnerabilidades que puedan ser aprovechadas por dichas amenazas;
4. Identificar los impactos en la confidencialidad, integridad y disponibilidad de los activos.

(b) Analizar y evaluar los riesgos:

1. Evaluar el impacto en el negocio de un fallo de seguridad que suponga la pérdida de confidencialidad, integridad o disponibilidad de un activo de información;
2. Evaluar de forma realista la probabilidad de ocurrencia de un fallo de seguridad en relación a las amenazas, vulnerabilidades, impactos en los activos y los controles que ya estén implementados;
3. Estimar los niveles de riesgo;
4. Determinar, según los criterios de aceptación de riesgo previamente establecidos, si el riesgo es aceptable o necesita ser tratado.

El análisis del riesgo es una parte importante de la Seguridad de la Información. No se puede proteger algo si no se sabe contra que hay que protegerlo, porque conociendo los riesgos se puedan plantear las políticas y técnicas que se necesiten reducir los mismo. Conocido todos los riesgos es necesario tomar decisiones y sobre la manera de gestionar esos riesgos.

Gestión de Riesgos de seguridad de la información:

La gestión de riesgos es el proceso de identificación y evaluación de riesgos, con el objetivo de tomar medidas que permitan reducir el riesgo a un nivel aceptable.

Según De Freitas (2009), la gestión de riesgos es una parte esencial de la gestión estratégica de cualquier organización. Es el proceso a través del cual las

organizaciones tratan los riesgos relacionados con sus actividades, con el fin de obtener un beneficio sostenido en cada una de ellas y en su conjunto.

Una gestión de riesgos eficaz se centra en la identificación y tratamiento de los riesgos. Su objetivo es añadir el máximo valor sostenible a todas las actividades de la organización.

Asimismo, la norma ISO/IEC 27005 explica que la gestión del riesgo en la seguridad de la información debería ser un proceso continuo. Tal proceso debería establecer el contexto, evaluar los riesgos, tratar los riesgos utilizando un plan de tratamiento para implementar las recomendaciones y decisiones. La gestión del riesgo analiza lo que se debería hacer y cuando hacerlo, con el fin de reducir el riesgo hasta un nivel aceptable.

Además, el proceso de gestión de riesgo en seguridad de la información se puede aplicar a la organización en su totalidad, a una parte separada de la organización (por ejemplo, un departamento, una ubicación física, un servicio), a cualquier sistema de información, existente o planificado, o a aspectos particulares del control (por ejemplo, la planificación de continuidad del negocio)

La gestión de riesgos debe estar integrada en la cultura de la organización con una política eficaz y un programa dirigido por la alta gerencia. Tiene que convertir la estrategia en objetivos tácticos y operacionales, asignando en toda la empresa responsabilidades, siendo cada gestor y cada empleado responsable de la gestión de riesgos como parte de la descripción de su trabajo. (De Freitas, 2009)

Por último, respalda la responsabilidad, la medida y la recompensa del rendimiento, promoviendo así la eficiencia operacional a todos los niveles.

Estas etapas ayudan a implementar controles de seguridad, basadas en la evaluación de los riesgos y en una medición de la eficacia de los mismos.

Sistema de gestión de seguridad de la información (SGSI)

INTECO (2010) , define SGSI como “la manera en la que una organización conoce los riesgos a los que está sometida su información y los gestiona mediante una

sistemática definida, documentada y conocida por todos, que se revisa y mejora constantemente".

Por otro lado, Colobran y otros (2008), explican que cualquier sistema de gestión de seguridad, tendrá que comprender la política, la estructura organizativa, los procedimientos, los procesos y los recursos necesarios para implantar la gestión de seguridad de la información dentro de una organización.

Los autores continúan detallando que básicamente, un sistema de gestión se caracteriza por:

- Cubrir los aspectos organizativos, lógicos, físicos y legales.
- Ser independiente de plataformas tecnológicas y mecanismos concretos.
- Ser aplicable a todo tipo de organizaciones, independientemente de la medida y actividad.
- Tener, como todo sistema de gestión, un fuerte contenido documental.

En los sistemas de gestión de seguridad de la información se definen:

Activo: recurso del sistema de información o relacionado con este, necesarios para que la organización funcione correctamente y logre los objetivos propuestos por la dirección.

Amenazas: suceso que puede desencadenar un incidente en la organización produciendo daños o pérdidas materiales o inmateriales en sus activos.

Riesgo: posibilidad que una amenaza se materialice.

Impacto: consecuencia sobre un activo de la materialización de una amenaza.

Control: práctica, procedimiento o mecanismo que reduce el nivel de riesgo.

Estándares de Gestión de Seguridad de la Información

ISO/IEC 27000 es un conjunto de estándares desarrollados ó en fase de desarrollo por ISO (International Organization for Standardization) e IEC (International Electrotechnical Commission), que proporcionan un marco de gestión

de la seguridad de la información utilizable por cualquier tipo de organización, pública o privada, grande o pequeña.

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

1. ISO/IEC27000 Sistemas de Gestión de Seguridad de la Información, Generalidades y vocabulario, publicada en Abril del 2009, en la que se recogen los términos y conceptos relacionados con la seguridad de la información, una visión general de la familia de estándares de esta área, una introducción a los SGSI, y una descripción del ciclo de mejora continua.
2. UNE-ISO/IEC 27001, Sistemas de Gestión de la Seguridad de la Información (SGSI). Requisitos. (ISO/IEC 27001:2005), publicada el 15 de octubre del 2005. Esta es la norma fundamental de la familia, ya que contiene los requerimientos del sistema de gestión de seguridad de la información y es la norma con arreglo a la cual serán certificados los SGSI de las organizaciones que lo deseen.
3. ISO/IEC27002, Tecnología de la Información. Código de buenas prácticas para la Gestión de la Seguridad de la Información, publicada en el año 2007. Esta guía de buenas prácticas describe los objetivos de control y controles recomendables en cuanto a seguridad de la información.
4. ISO/IEC27003. Guía de implementación de SGSI e información acerca del uso del modelo PHVA y de los requerimientos de sus diferentes fases
5. ISO27004: Estándar para la medición de la efectividad de la implantación de un SGSI y de los controles relacionados.
6. ISO/IEC27005:2008 Gestión del Riesgo en la Seguridad de la Información, Publicada el 4 de Junio de 2008. Esta norma al pertenecer a la familia de las Normas 27000, se ajusta a las necesidades de las organizaciones que pretende realizar su análisis de riesgos en este ámbito y cumplir con los requisitos de la Norma ISO 27001.
7. ISO/IEC27006. Requisitos para las entidades que suministran servicios de auditoría y certificación de sistemas de gestión de seguridad de la

información. Publicada en el año 2007. Recoge los criterios mediante los cuales una organización se puede acreditar para realizar esos servicios.

8. ISO/IEC27007. Guía para la realización de las auditorías de un SGSI.
9. ISO/IEC27011. Directrices para la seguridad de la información en organizaciones de telecomunicaciones utilizando la Norma ISO/IEC 27002. Contiene recomendaciones para empresas de este sector, facilitando el cumplimiento de la Norma ISO27001 y conseguir un nivel de seguridad aceptable.

Estándar internacional para la Seguridad de la Información ISO/IEC 27001:2005

Origen

En el año 1995 el British Standard Institute (BSI) publica la norma BS7799, un código de buenas prácticas para la gestión de la seguridad de la información.

A la vista de la gran aceptación de esta Norma, en 1998, el BSI pública la norma BS7799-2, Especificaciones para los sistemas de gestión de la seguridad de la información; se revisa en 2001. Tras una revisión de ambas Normas, la primera es adoptada como norma ISO en 2000 y denominada ISO/IEC 17799.

En 2002 la norma ISO se adopta como UNE sin apenas modificación (UNE 17799), y en 2004 se establece la norma UNE 71502, basada en BS7799-2, sin que haya un equivalente ISO.

A partir de julio de 2007 la ISO 17799:2005 adopta el nombre de ISO 27002 y en octubre de 2005 nace el estándar ISO/IEC 27001:2005, sustituyendo el BS 7799. Fue desarrollado por el comité técnico conjunto ISO/IEC (Organización Internacional de estándares/Comisión Electrónica Internacional) JTC 1, tecnología de la información, subcomité SC 27, técnicas de seguridad de TI. En el gráfica 2 se muestra la evolución histórica de la ISO/IEC 27001:2005.

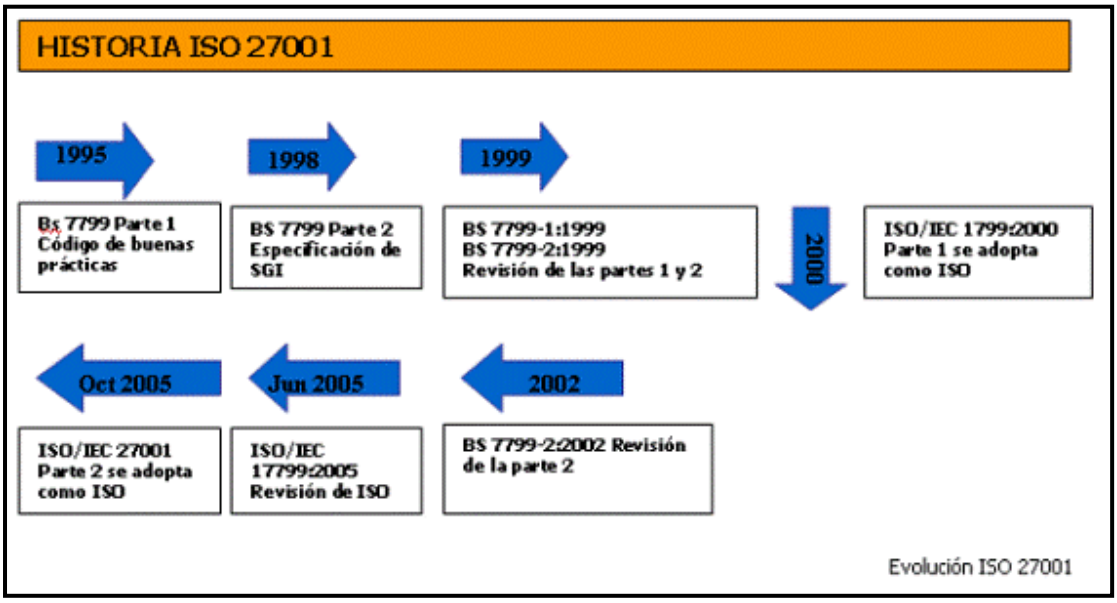

Gráfico 2. Evolución ISO 27001

Fuente: www.iso27001.es

Contenido de la norma

Según la Norma ISO/IEC 27001, el estándar internacional ha sido preparado con la finalidad de proporcionar un modelo para establecer, implementar, operar, monitorear, revisar, mantener y mejorar un Sistema de Gestión de Seguridad de la Información (SGSI). La adopción de un SGSI debe ser una decisión estratégica para una organización. El diseño e implementación del SGSI de una organización es influenciado por las necesidades y objetivos, requerimientos de seguridad, los procesos empleados, el tamaño y estructura de la organización. Se espera que estos y sus sistemas de apoyo cambien a lo largo del tiempo. Se espera que la implementación de un SGSI se extienda en concordancia con las necesidades de la organización; por ejemplo, una situación simple requiere una solución SGSI simple.

Este estándar internacional promueve la adopción de un enfoque del proceso para establecer, implementar, operar, monitorear, revisar, mantener y mejorar el SGSI de una organización. La organización necesita identificar y manejar muchas actividades para poder funcionar de manera efectiva. Cualquier actividad que usa recursos y es manejada para permitir la transformación de insumos en productos, se

puede considerar un proceso. Con frecuencia el producto de un proceso forma directamente el insumo del siguiente proceso.

La aplicación de un sistema de procesos dentro de una organización, junto con la identificación y las interacciones de estos procesos y su gestión, puede considerarse un "enfoque del proceso".

Un enfoque del proceso para la gestión de la seguridad de la información presentado en este estándar internacional fomenta que sus usuarios enfaticen la importancia de:

- Los requerimientos de seguridad de la información de una organización y la necesidad de establecer una política y objetivos para la seguridad de la información;
- Implementar y operar controles para manejar los riesgos de la seguridad de la información;
- Monitorear y revisar el desempeño y la efectividad del SGSI; y
- Mejoramiento continúo en base a la medición del objetivo.

El estándar internacional adopta el modelo del proceso planear-Hacer-Chequear-Actuar (PHVA), el cual se puede aplicar a todos los procesos SGSI. El Gráfico 3 muestra cómo un SGSI toma como insumo los requerimientos y expectativas de la seguridad de la información de las partes interesadas y a través de las acciones y procesos necesarios produce resultados de seguridad de la información que satisfacen aquellos requerimientos y expectativas. El Gráfico 3 y el cuadro 1 también muestran los vínculos en los procesos presentados en las Cláusulas 4, 5, 6, 7 y 8 de la norma y la descripción del modelo respectivamente.

La adopción del modelo PHVA también reflejará los principios tal como se establecen en los Lineamientos OECD (Lineamientos OECD para Sistemas y Redes de Seguridad de la Información – Hacia una Cultura de Seguridad. París, 2.002) que gobiernan los sistemas y redes de seguridad de la información. Este estándar internacional proporciona un modelo sólido para implementar los principios en aquellos lineamientos que gobiernan la evaluación del riesgo, diseño e implementación de seguridad, gestión y reevaluación de la seguridad.

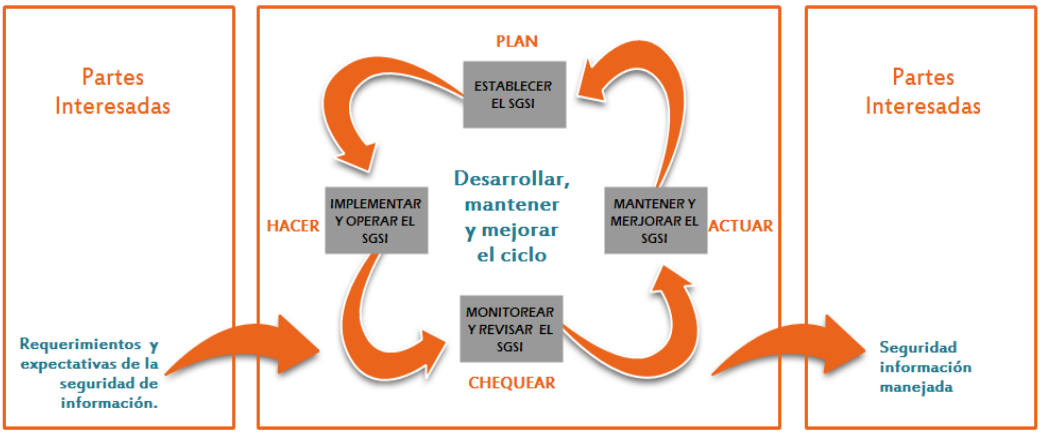

Gráfico 3. Modelo PHVA aplicados a los procesos SGSI

Fuente: norma ISO/IEC 27001:2005

Cuadro 1

Descripción del modelo PHVA aplicado a los procesos SGSI

Planear (Establecer SGSI)	Establecer política, objetivos, y procedimientos SGSI relevantes para manejar el riesgo y mejorar la seguridad de la información para entregar resultados en concordancia con las políticas y objetivos generales.
Hacer (Implementar y operar el SGSI)	Implementar y operar la política, controles, procesos y procedimientos SGSI
Chequear o Verificar (Monitorear y revisar el SGSI)	Evaluar y, donde sea aplicable, medir el desempeño del proceso en comparación con la política, objetivos y experiencias practicas SGSI y reportar los resultados a la gerencia para su revisión.
Actuar (Mantener y mejorar el SGSI)	Tomar acciones correctivas y preventivas, basadas en los resultados de la auditoría interna SGSI y la revisión gerencial u otra información relevante, para lograr el mejoramiento continuo del SGSI.

Fuente: norma ISO/IEC 27001:2005

La norma considera la organización como una totalidad y tiene en cuenta todos los posibles aspectos que se pueden ver afectados ante los posibles incidentes que se puedan producir. La mencionada norma en su anexo A (Ver Anexo H) muestra los

once dominios de control en lo que se encuentra estructurada, los mismos cubren completamente la gestión de la seguridad de la información, donde cada uno de ellos se refiere a un aspecto de la seguridad de la organización:

(1) Políticas de seguridad: proporcionar dirección gerencia y apoyo a la seguridad de la información en concordancia con los requerimientos comerciales y leyes y regulaciones relevantes.
(2) Organización de la seguridad de la información: manejar la seguridad de la información dentro de la organización.
(3) Gestión de activos: lograr y mantener la protección apropiada de los activos organizacionales.
(4) Seguridad de los recursos humanos: asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean adecuados para los roles para los cuales se les considera; y reducir el riesgo de robo, fraude o mal uso de los medios.
(5) Seguridad física y ambiental: evitar el acceso físico no autorizado, daño e interferencia al local y la información de la organización.
(6) Gestión de comunicaciones y operaciones: asegurar la operación correcta y segura de los medios de procesamiento de la información.
(7) Control de accesos: controlar acceso a la información.
(8) Adquisición desarrollo y mantenimiento de sistemas: asegurar que la seguridad sea una parte integral de los sistemas de información.
(9) Gestión de incidentes de seguridad de la información: asegurar que la información de los eventos y debilidades en la seguridad de la información asociados con los sistemas de información se comunicada de una manera que permita tomar una acción correctiva oportuna.
(10) Gestión de continuidad del negocio: contrarrestar las interrupciones de las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas o desastres importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.

(11) Conformidad legal: evitar violaciones de cualquier ley, obligación reguladora o contractual y de cualquier requerimiento de seguridad.

En el gráfico 4, se muestra los once dominios de control que estructura la norma y el tipo de seguridad.

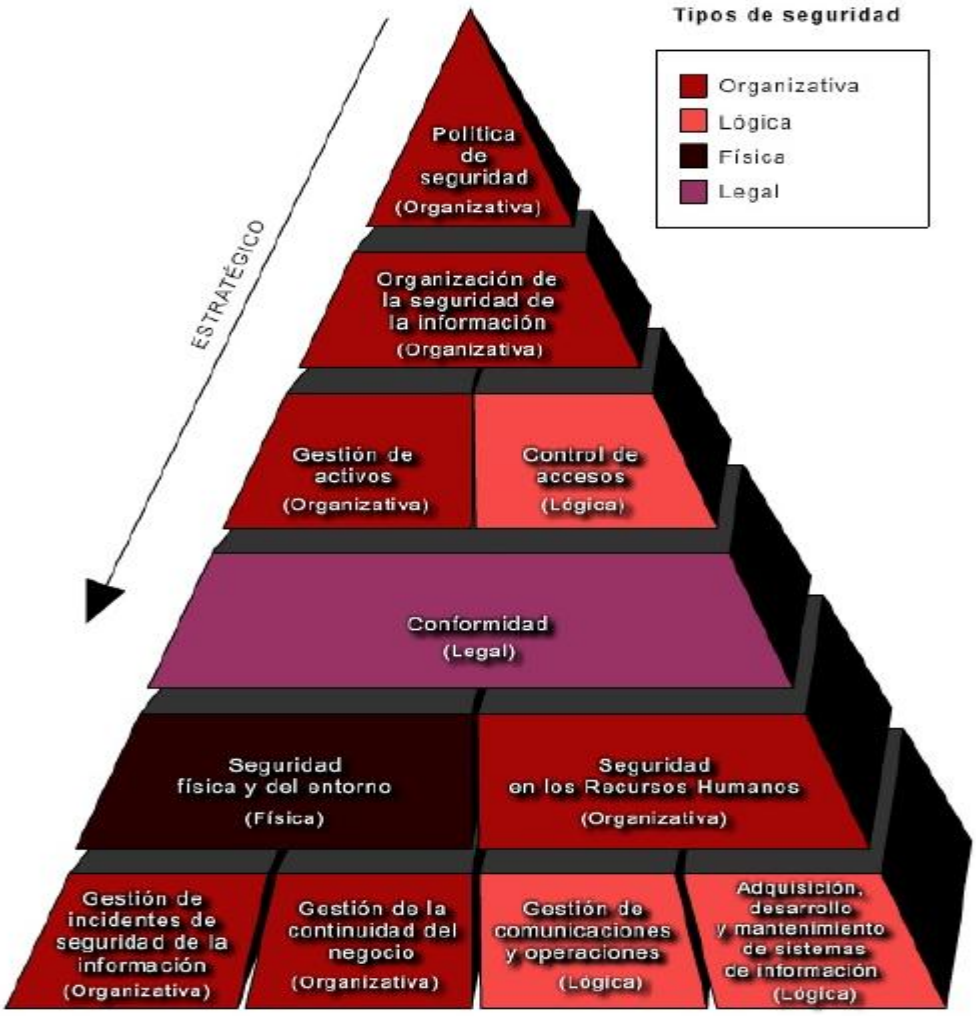

Gráfico 4. Dominios de control

Fuente: INTECO (2010)

Para verificar si los procesos de seguridad se están cumpliendo se puede realizar una auditoría de seguridad.

Auditoria de Seguridad

De acuerdo a lo expresado por Del peso (2003):

> "La auditoria de seguridad de la información es aquella que tiene por objeto verificar que se cumplan los controles estipulados. Esto puede hacerse bien en un documento de seguridad, en unas políticas de seguridad, en un plan de seguridad o en unos objetivos de control de carácter sectorial o general". (p.51)

Por otro lado Areito (2008), considera que la auditoria de seguridad consisten en seguir la pista de todas las acciones relacionadas con la seguridad que se puedan llevar a cabo en un sistema de información, de modo que se pueda detectar acciones no autorizadas por los usuarios y de esta forma poder mejorar las políticas de seguridad. La auditoria facilita el conocimiento de las personas o entidades que estén ejecutando operaciones en una determinada red o sistema de información y las acciones que se están realizando. Para ello, es necesario que se identifique a todos los sujetos (usuarios, procesos o agentes) y debe utilizarse la información de identidad para decidir si pueden acceder de forma legítima a la información y a los recursos contenidos en el sistema.

Dado este contexto, se puede decir que las auditorias de seguridad sirven como información de retroalimentación, para analizar en qué medida el sistema garantiza la seguridad, y detecta puntos de fallo concretos en cada activo.

Además, está estrechamente relacionada con la gestión de la seguridad, donde se establecen métricas de seguridad y se interactúan con cuadros de mando.

Asimismo, captura, registra, examina, revisa, y reconstruye las actividades relacionadas con la seguridad

En este sentido, la auditoria de seguridad nos permite la aplicación de controles de informáticos.

Control Interno Informático

Según Piattini y del Peso (1998), lo definen como los diferentes controles para la función informática, según el nivel de riesgos y diseñados de acuerdo a los objetivos del negocio y dentro del marco legal aplicable.

De igual manera, los autores indican que el Control Interno Informático permite controlar diariamente que todas las actividades de los sistemas de información sean realizadas cumpliendo los procedimientos, estándares y normas fijadas por la Dirección de la Organización y/o la Dirección Informática, así como los requerimientos legales.

Clasificación de Control Interno Informático

Controles preventivos: para tratar de evitar el hecho, como un software de seguridad que impida los accesos no autorizados al sistema. (Piattini y del Peso, 2001, p31)
Controles Detectivos: cuando fallan los preventivos para tratar de conocer cuanto antes el evento. Por ejemplo, el registro de intentos de accesos no autorizados, el registro de la actividad diaria para detectar errores u omisiones, entre otras. (Piattini y del Peso, 2001, p31)
Controles correctivos: facilitan la vuelta a la normalidad cuando se han producido incidencias. Por ejemplo, la recuperación de un fichero dañado a partir de las copias de seguridad. (Piattini y del Peso, 2001, p31)

Herramientas para el análisis de riesgos

MAGERIT

Desarrollado por el Ministerio de Administraciones Públicas de España, es una metodología de análisis de riesgos que describe los pasos para realizar un análisis del estado de riesgo y para gestionar su mitigación, detalla las tareas para llevarlo a cabo de manera que el proceso esté bajo control en todo momento y contempla aspectos prácticos para la realización de un análisis y una gestión realmente efectivos. Cuenta con detallados catálogos de amenazas, vulnerabilidades y salvaguardas. Cuenta con una herramienta, denominada PILAR para el análisis y la gestión de los riesgos de los sistemas de información que tiene dos versiones, una completa para grandes organizaciones y otra simplificada para las pequeñas.

SP800-30 NIST Risk Management Guide for Information Technology Systems:

Desarrollado por el NIST estadounidense, es una guía detallada de las consideraciones que deben hacerse para llevar a cabo una evaluación y una gestión de riesgos orientada a la seguridad de los sistemas de información.

CRAMM:

Es un método de análisis de riesgos desarrollado por el gobierno británico y cuenta con una herramienta, ya que es un método difícil de usar sin ella. Está basado en las mejores prácticas de la administración pública británica, por lo que es más adecuado para organizaciones grandes, tanto públicas como privadas.

EBIOS:

Es un compendio de guías, más que una herramienta de código libre gratuita, enfocada a gestores del riesgo de TI. Desarrollada en un principio por el gobierno francés, ha tenido una gran difusión y se usa tanto en el sector público como en el privado, no sólo de Francia, sino en otros países. La metodología EBIOS consta de un ciclo de cinco fases: Fase 1. Análisis del contexto, estudiando cuales son las

dependencias de los procesos del negocio respecto a los sistemas de información. Fases 2 y 3, Análisis de las necesidades de seguridad y de las amenazas, determinando los puntos de conflicto. Fases 4 y 5, Resolución del conflicto, estableciendo los objetivos de seguridad necesarios y suficientes, con pruebas de su cumplimiento y dejando claros cuales son los riesgos residuales.

OCTAVE: (Operationally Critical Threat, Asset, and Vulnerability EvaluationSM):

Desarrollado en EEUU por el SEI, es un una metodología para recoger y analizar información de manera que se pueda diseñar una estrategia de protección y planes de mitigación de riesgo basados en los riesgos operacionales de seguridad de la organización. Hay dos versiones, una para grandes organizaciones y otra para pequeñas, de menos de 100 empleados.

Norma ISO/IEC 27005:

La Norma habla de la gestión de los riesgos de la seguridad de la información de manera genérica, utilizando para ello el modelo PHVA, y en sus anexos se pueden encontrar enfoques para la realización de análisis de riesgos, así como un catálogo de amenazas, vulnerabilidades y técnicas para valorarlos.

BASES LEGALES

En la actualidad, existen diversas leyes y normativas relativas a la Seguridad de la Información y al uso de las tecnologías de la información (TI) que aplican a todo tipo de organizaciones. A continuación se presentan las normas internacionales, leyes nacionales y normativa interna de la universidad, que tienen correspondencia con la presente investigación.

Estándares Internacionales

ISO/IEC 27001:2005 Tecnología de la Información – Técnicas de Seguridad Sistemas de Gestión de Seguridad de la Información – Requerimientos. Aprobado y publicado como estándar internacional el 15 de octubre del 2005, por la Organización Internacional de Estándares y la Comisión Electrónica Internacional.

Leyes Nacionales

Ley Orgánica de Ciencia, Tecnología e Innovación

Promulgada en Gaceta Oficial N° 38.242 de fecha 03 de Agosto de 2005.

Título I. Disposiciones fundamentales
Artículo 1°. Objeto del Decreto-Ley
El presente Decreto-Ley tiene por objeto desarrollar los principios orientadores que en materia de ciencia, tecnología e innovación, establece la Constitución de la República Bolivariana de Venezuela, organizar el Sistema Nacional de Ciencia, Tecnología e Innovación, definir los lineamientos que orientarán las políticas y estrategias para la actividad científica, tecnológica y de innovación, con la implantación de mecanismos institucionales y operativos para la promoción, estímulo y fomento de la investigación científica, la apropiación social del conocimiento y la transferencia e innovación tecnológica, a fin de fomentar la capacidad para la generación, uso y circulación del conocimiento y de impulsar el desarrollo nacional.

Ley cuyo objetivo fundamental de estructurar el Sistema Nacional de Ciencia, Tecnología e Innovación (SNCTI). En este Sistema se integran las instituciones, organismos, entidades y organizaciones universitarias estadales del sector público y privado para que realicen actividades vinculadas al desarrollo científico, tecnológico e innovativo, y adelanten la formación del personal que hace vida en los diferentes entes que lo conforman.

Ley Orgánica de Telecomunicaciones

Ley Orgánica de Telecomunicaciones, promulgada en Gaceta Oficial N° 37.148 de fecha 28 de febrero de 2001 por Decreto N° 1.024 - 10 de febrero de 2001

> **Título I. Disposiciones Generales.**
> **Articulo 1.-**
> Esta Ley tiene por objeto establecer el marco legal de regulación general de las telecomunicaciones, a fin de garantizar el derecho humano de las personas a la comunicación y a la realización de las actividades económicas de telecomunicaciones necesarias para lograrlo, sin más limitaciones que las derivadas de la Constitución y las leyes.
> Se excluye del objeto de esta Ley la regulación del contenido de las transmisiones y comunicaciones cursadas a través de los distintos medios de telecomunicaciones, la cual se regirá por las disposiciones constitucionales, legales y reglamentarias correspondientes.

Ley que da soporte legal al área de las telecomunicaciones, regulando la transferencia de información entre los diferentes organismos, incluyendo las redes de datos.

Ley Especial Contra los Delitos Informáticos

Promulgada en Gaceta Oficial Nº 37.313 de fecha 30 de octubre de 2001 por la Asamblea Nacional.

> Título I. Disposiciones Generales.
> Artículo 1. Objeto de la ley. La presente ley tiene por objeto la protección integral de los sistemas que utilicen tecnologías de información, así como la prevención y sanción de los delitos cometidos contra tales sistemas o cualquiera de sus componentes o los cometidos mediante el uso de dichas tecnologías, en los términos previstos en esta ley.

Este instrumento legal concibe como bien jurídico la protección de los sistemas informáticos que contienen, procesan, resguardan y transmiten la información. Cuyo objetivo es proteger los sistemas que utilicen tecnologías de información, así como prevenir y sancionar los delitos cometidos contra o mediante el uso de tales tecnologías.

Ley Sobre Mensajes De Datos y Firmas Electrónicas

Promulgada en Gaceta Oficial N° 37.148 de fecha 28 de febrero de 2001, por Decreto N° 1.024 – 10 de febrero de 2001.

Capítulo I. Objeto y Aplicabilidad Del Decreto -Ley

> Artículo 1°: El presente Decreto-Ley tiene por objeto otorgar y reconocer eficacia y valor jurídico a la Firma Electrónica, al Mensaje de Datos y a toda información inteligible en formato electrónico, independientemente de su soporte material, atribuible a personas naturales o jurídicas, públicas o privadas, así como regular todo lo relativo a los Proveedores de Servicios de Certificación y los Certificados Electrónicos.
> El presente Decreto-Ley será aplicable a los Mensajes de Datos y Firmas Electrónicas independientemente de sus características tecnológicas o de los desarrollos tecnológicos que se produzcan en un futuro. A tal efecto, sus normas serán desarrolladas e interpretadas progresivamente, orientadas a reconocer la validez y eficacia probatoria de los Mensajes de Datos y Firmas Electrónicas. La certificación a que se refiere el presente Decreto-Ley no excluye el cumplimiento de las formalidades de registro público o autenticación que, de conformidad con la ley, requieran determinados actos o negocios jurídicos.

Esta ley sienta las bases para la regulación del comercio electrónico. Apoyando las transacciones a través de formatos digitales, la transferencias de datos entre organizaciones, el establecimiento de redes inter empresariales, así como la comunicación efectiva entre organismos públicos y privados.

Normativa Interna

Promulgada de acuerdo a la resolución de Consejo Universitario No. 1647. Normas de Seguridad Informática y de Telecomunicaciones de la Universidad Centroccidental “Lisandro Alvarado” aprobado el 21 de septiembre del 2.005. Barquisimeto Venezuela.

> Propósito. El propósito de estas normas es el proteger a los usuarios de la comunidad universitaria contra los virus, vandalismo, el uso informático no autorizado y cualquier otro ataques dirigido a sus datos, redes y los dispositivos conectados a la Infraestructura de telecomunicaciones de la UCLA (RedUCLA) a través de especificaciones tecnológicas,

> requerimientos administrativos y recomendaciones que serán gestionadas por la Dirección de Telecomunicaciones de la UCLA. Todo esto con el mejor interés de la Universidad en que los datos, redes y los dispositivos conectados en la RedUCLA sean íntegros, protegidos y disponibles para los usuarios, sistemas, servicios e información basados en estos. Estas normas y sus estándares asociados, por consiguiente, permitirán establecer configuraciones y administraciones de la red de forma segura para cualquier computadora provista con acceso a la RedUCLA.

SISTEMAS DE VARIABLES

De acuerdo a lo expresado por Balestrini (2006), una variable "es un aspecto o dimensión de un objeto, o una propiedad de estos aspectos o dimensiones que adquieren distintos valores y por lo tanto varia" (p.113).

Asimismo, Arias (1999) explica que un sistema de variables consiste en una serie de características de la variable a estudiar, definidas de manera operacional, en función de sus dimensiones e indicadores

En este orden de ideas, para el proceso de operacionalización de las variables se tomo como referencia lo formulado por Tamayo y Tamayo (2005); quienes exponen que es necesario determinar los parámetros de medición a partir de los cuales se establecerá la relación de variables enunciadas por hipótesis, para lo cual es necesario tener en cuenta: (a) el enunciado nominal que es simplemente el nombre de la variable que debe medirse; (b) la definición operacional, formado por las dimensiones e indicadores, donde la dimensión es un factor de rasgo de la variable que debe medirse y los indicadores señalan como medir cada uno de los factores o rasgos de la variable.

Para la investigación objeto de estudio, la definición nominal fue la Sistematización de la Gestión de Riesgos de Seguridad de la Información en la Red de la Universidad Centroccidental "Lisandro Alvarado".

La definición operacional, la componen las dimensiones gestión de riesgos y Seguridad de la Información. Los indicadores relacionados con la gestión de riesgos son: políticas de seguridad, gestión de activos, amenazas, vulnerabilidades y para la

seguridad de la información se encuentran: la integridad, confidencialidad y disponibilidad.

A continuación se presenta el cuadro Nro. 2, donde se puede apreciar la operacionalización de las variables para el trabajo de investigación.

Cuadro 2

Operacionalización de las variables.

Variable	Dimensión	Indicador	Instrumentos			Fuente
			A	B	C	
			Ítems			
Sistematización de la Gestión de Riesgos de la Seguridad de la Información en la Red de la Universidad Centroccidental "Lisandro Alvarado	**Gestión de Riesgos:** Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.	1. Políticas de Seguridad	1,2, 3,4	1,2, 8	1	Personal de la Dirección de Telecomunicaciones y Profesores expertos en el área de seguridad de la Información del Decanato de Ciencias y Tecnologías de la UCLA
		2. Gestión de Activos	5,6, 7, 8	4	2,3,4	
		3. Amenazas	9, 10 11, 12	5	5	
		4. Vulnerabilidades	13, 16 17	3,6, 7,9, 10	6,7	
	Seguridad de la Información: Protección de la confidencialidad, integridad y disponibilidad de los activos de información según sea necesario para alcanzar los objetivos de negocio de la organización.	5. Integridad	14,19			Personal de la Dirección de Telecomunicaciones
		6. Confidencialidad	15, 20			
		7. Disponibilidad	18, 21	3, 9		

Nota: Gil (2011)

CAPITULO III

MARCO METODOLÓGICO

El presente capítulo se refiere a los aspectos relacionados a la metodología de la investigación que incluye el diseño y tipo de la investigación, las técnicas y procedimientos necesarios para el logro de los objetivos propuestos.

Diseño y Tipo de la Investigación

De acuerdo a los objetivos que se pretendió alcanzar con la presente investigación: "Sistematizar la Gestión de Riesgos de Seguridad de la Información en la Red de la Universidad Centroccidental Lisandro Alvarado" y las características que presentan las variables, el diseño de la investigación fue no experimental, apoyada en un estudio de campo de tipo descriptivo.

Hernández, Fernández y Baptista (2003), define la investigación no experimental como "...la investigación que se realiza sin manipular deliberadamente variables." (p.267). En este tipo de investigación se observa el fenómeno tal y como se presentan en su contexto natural, para luego analizarlos.

En relación a la investigación de campo, según Arias (1999), "consiste en la recolección de datos directamente de la realidad donde ocurren los hechos, sin manipular o controlar variable alguna". (p. 48). Los datos recolectados fueron de fuentes primarias, directamente del personal que labora en la Dirección de Telecomunicaciones de la UCLA y de los especialistas en el área de seguridad de la información del Decanato de Ciencias y Tecnologías.

Finalmente, para el caso de la investigación de tipo descriptivo, Hernández y otros (2003) explican que este tipo de estudio buscar especificar las propiedades, características y rasgos importantes de cualquier fenómeno que se analice.

Población y Muestra

Población:

La población o universo es definida por Tamayo y Tamayo (2005) como: "la totalidad del fenómeno a estudiar, donde las unidades de población poseen una característica común, la cual se estudia y da origen a los datos de la investigación". (p. 114).

En la investigación objeto de estudio, la población estuvo representada por dos estratos: en primer lugar, el conjunto de todos los empleados de la Universidad que laboran en la Dirección de Telecomunicaciones (ver cuadro 3). En segundo lugar el conjunto de profesores expertos en el área de seguridad de la información adscrito al Decanato de Ciencias y Tecnología de la Universidad (ver cuadro 3).

Cuadro 3

Descripción de la población

ESTRATOS			
I. Personal Dirección de Telecomunicaciones		**II. Profesores expertos en el área de seguridad de la información**	
Descripción	Cantidad	Descripción	Cantidad
Director	1	Profesor	5
Jefes de Unidades	3		
Administradores de la Red	7		
Total	11	Total	5

Fuente: Gil (2011)

Muestra:

Una vez conocida la población se tomó una muestra representativa de la misma. Sabino (2002), define la muestra como "una parte del todo que llamamos universo y que sirve para representarlo". (p. 83).

Para los efectos de esta investigación se tomó en cuenta lo expresado por Ary (citado por Mujica, 2007) "...si la población posee pequeñas dimensiones, deben ser seleccionados en su totalidad, para así reducir el error en la muestra" (p.54); tomando como referencia esta definición para el caso de los empleados de la Universidad que laboran en la Dirección de Telecomunicaciones, se tomó la población en su totalidad; representada por once (11) empleados. De esta forma reducir el error en la muestra.

No obstante, para el conjunto de profesores expertos en el área de seguridad de la información adscritos al Decanato de Ciencias y Tecnología de la UCLA, la muestra siguió el criterio de expertos en área de seguridad de la información; razón por la cual la muestra representada por 5 profesores se realizó por el método de muestreo no probabilística intencional, el cual Cardona (2002) expresa lo siguiente para este tipo de muestreo: se basa en la selección de sujetos particulares de la población que son representativos o informativos. De acuerdo al juicio del investigador. Se seleccionan los casos que se piensa puedan aportar mayor información.

Para el caso de la presente investigación se tomó en consideración profesores expertos en el área de seguridad de la información, ya que aportarón información importante al estudio.

Técnicas de Recolección de Datos

Una vez seleccionado el diseño de la investigación y la muestra apropiada para la misma, se procedió a la recolección de los datos la cual consistió en la selección y construcción de los instrumentos, su validación y establecimiento de la confiabilidad para su posterior aplicación.

Entre las técnicas de recolección de los datos que se utilizaron en la presente investigación fueron las siguientes:

- **Entrevista:** de acuerdo a lo expresado por Sabino (2002), la entrevista "Consiste en una interacción entre dos personas, una de las cuales (el investigador) formula determinadas preguntas relativas al tema de investigación, mientras la otra (el investigado) proporciona verbalmente o por escrito la información que le es solicitada". (p. 106)
- **Cuestionario:** Según Hernández y otros (2003), "un cuestionario consiste en un conjunto de preguntas respecto a una o más variables a medir". (p. 391)

Para la recolección de los datos de la investigación, se elaboraron dos (2) entrevistas estructuradas (anexo B y C) que se aplicaron con el soporte de dos (2) cuestionarios, los cuales estaban conformados por preguntas abiertas en su totalidad. El primero constituido por diez (10) preguntas, fue aplicado al Director y los Jefes de Unidades de la Dirección de Telecomunicaciones, y el segundo constituido por siete (7) preguntas, fue aplicado a los Profesores expertos en el área de seguridad de la información.

También se elaboró un cuestionario (anexo D), el cual constó de veintiún (21) preguntas cerradas, siendo este aplicado a los administradores de la RedUCLA, conformado por preguntas de tipo dicotómicas, preguntas por escalas de Likert y finalmente preguntas de tipo selección, tanto múltiple como simple.

Validez y Confiabilidad

Validez

La validez de un instrumento, según Hernández y otros (2003), "se refiere al grado en que un instrumento refleja un dominio especifico de contenido de lo que se mide". (p. 347). Además, el autor señala que la validez se refiere al grado en que un instrumento realmente mide la variable que pretende medir.

Para determinar la validez de los instrumentos, se procedió a evaluar la validez de su contenido, para ello se utilizó la técnica del juicio de expertos; se sometió a esta prueba los instrumentos utilizados. Se seleccionaron tres (3) especialistas, uno (1) en el área de seguridad de la Información, uno (1) en metodología y otro en tecnologías de Información y comunicación; quienes a través de una matriz (Anexos E) validaron los ítems de los instrumentos, con la finalidad de recolectar sugerencias acerca de la redacción, claridad y pertinencia de los ítems.

Considerando las recomendaciones respectivas se procedió a realizar cambios en algunos ítems respecto a la forma de expresión y posteriormente se procedió a su aplicación a los sujetos de la muestra.

Confiabilidad:

La confiabilidad de un instrumento, de acuerdo a Hernández y otros (2003) "se refiere al grado en que su aplicación repetida al mismo sujeto u objeto produce resultados iguales". (p.346)

Los métodos utilizados para determinar la confiabilidad de consistencia interna de los instrumentos fueron los siguientes: (i) Alpha Cronbach y (ii) kuder Richardson (r20).

(i) Coeficiente de Alpha Cronbach: este método indica la capacidad que tiene el instrumento para arrojar resultados similares a repetidas ocasiones. Este método es aplicable en los casos que la medición de constructos se haga a través de escalas, donde no existen respuestas correctas ni incorrectas, sino que cada sujeto marca el valor de la escala que mejor representa su respuesta.

Para determinarlo se aplicó la siguiente fórmula:

$$r_{tt} = \frac{n}{n-1} * \frac{S_t^2 - \sum S_t^2}{S^2}$$

En donde:

r_{tt} = coeficiente de confiabilidad;
n = número de ítemes;
S_t^2 = varianza total de la prueba; y
$\sum S_t^2$ es la suma de las varianzas individuales de los ítemes.

Gráfico 5. Fórmula Coeficiente Alpha de Cronbach.

(ii) Formula de Kuder Richardson (kr20) (1937): La ecuación KR20 representa un coeficiente de consistencia interna del instrumento, que proporciona la medida de todos los coeficientes de división por mitades para todas las posibles divisiones del instrumento. Este modelo es aplicable en las pruebas de ítems de tipo dicotómicas.

$$r_{tt} = \frac{n}{n-1} * \frac{Vt - \sum pq}{Vt}$$

En donde:
r_{tt} =coeficiente de confiabilidad.
N =número de ítemes que contiene el instrumento.
V_t = varianza total de la prueba.
$\sum pq$ = sumatoria de la varianza individual de los ítemes.

Gráfico 6. Fórmula Kuder Richardson (kr20)

El índice de confiabilidad para ambos métodos debe ser menor o igual a uno (1) para que el valor indicativo del instrumento posea un alto grado de consistencia interna, lo que indica la exactitud y objetividad en los resultados.

Cuadro 4

Criterios de Confiabilidad.

Valores de Alpha	Criterio
De -1 a 0	No Confiable
De 0.01 a 0.49	Confiabilidad Baja
De 0.50 a 0.75	Confiabilidad Moderada
De 0.76 a 0.89	Confiabilidad Fuerte
De 0.90 a 1.00	Confiabilidad Alta

Fuente: Hernández y otros (2003).

En este sentido, la confiabilidad de instrumento (cuestionario) se realizó con una muestra piloto de 7 personas tomadas al azar. El coeficiente de la prueba para el caso de los ítem de tipo dicotómicas se obtuvo aplicando la formula de kuder Richardson (r20), obteniendo el siguiente resultado: r20=0.82 (anexo F); al mismo tiempo se aplico el Alpha Cronbach para los ítems representados en una escala de likert obteniendo α= 0.92 (anexo G). Como resultados de la aplicación de las formulas de confiabilidad, se concluye que el instrumento es de "Confiabilidad Fuerte" y "Confiabilidad Alta" de acuerdo a lo expresado en el cuadro 4.

Técnicas de Análisis de Datos

En esta fase se procedió a describir las distintas etapas a la que fueron sometidos los datos: clasificación, análisis e interpretación de la información que se recolectó. Balestrini (2003) explica que "esta es una etapa de carácter técnico, pero de reflexión, que involucra la introducción de técnicas adecuadas para la organización de la información". (p.169)

En lo referente al análisis e interpretación de los resultados, el cuestionario se analizó mediante el método de estadística descriptiva cuya finalidad es presentar y reducir los diferentes datos observados; a través de cálculos estadísticos de

frecuencias absolutas y porcentuadas, para obtener los resultados de la información recolectada.

Para el caso de las preguntas abiertas realizadas en las entrevistas, los resultados fueron presentados y analizados, mediante matrices de análisis de contenido.

Presentación de los Resultados

La representación de los resultados del estudio se realizó a través de gráficos estadísticos de barras y análisis de los mismos, que permitieron aclarar los alcances obtenidos.

CAPITULO IV

PRESENTACION Y ANALISIS DE RESULTADOS

En este capítulo se procedió al análisis e interpretación de la información recopilada mediante los instrumentos de recolección de datos aplicados a la población seleccionada para el estudio.

Resultados de la Entrevista

La entrevista (Anexo B) se aplicó al Director y Jefes de Unidades de la Dirección de Telecomunicaciones. Dicha entrevista se realizó con la finalidad de conocer aspectos puntuales sobre la Gestión de Riesgos de Seguridad de la Información en la RedUCLA. Los resultados de la aplicación del instrumento se muestran a continuación.

Cuadro 5

Matriz de Análisis de Contenido. Entrevista al Director y Jefes de Unidades de la Dirección de Telecomunicaciones.

Pregunta	Respuesta Obtenida	Análisis
1. ¿Cuáles políticas de seguridad se han definido para la red de la UCLA? ¿Las mismas están basada en estándares internacionales de seguridad de la información?	La dirección cuenta con las siguientes políticas: Reglamento de procedimientos de la Dirección de Telecomunicaciones. Normas de Seguridad Informática y de telecomunicaciones de la UCLA basada en la ISO/IEC 17799.	Al contar con políticas, se deben establecer parámetros para que las mismas se cumplan.

Pregunta	Respuesta Obtenida	Análisis
2. ¿El documento de políticas de seguridad contiene aspectos para la regulación de la gestión del riesgo de Seguridad de la Información? Explique su respuesta.	La norma contempla regulación de los riesgos a nivel lógico; sin embargo a nivel físico no se aplica.	Es necesario que el documento de políticas de seguridad cubra los aspectos lógicos, físicos, legales y organizativos. De esta manera, lograr el correcto funcionamiento de la gestión de riesgos de seguridad de la información.
3. ¿Qué controles han sido implementados en la red para mantener la seguridad de los sistemas y aplicaciones, incluyendo la información en tránsito?	En general la Dirección de Telecomunicaciones no se encarga de los controles en los sistemas y aplicaciones, no obstante se tiene mecanismos de respaldo de los datos. La red cuenta con un equipo principal, firewall, el cual controla la seguridad en la red, de igual forma se tienen controles a nivel de protocolo, a nivel de puertos y servicios. En la actualidad se está implementando planes de acción en cuanto a seguridad física y seguridad en los recursos humanos.	La norma establece que las redes deben ser manejadas y controladas adecuadamente para protegerlas de amenazas y mantener la seguridad de la información en tránsito.
4. ¿Existen planes de contingencia ante situaciones de desastres que puedan afectar los activos de la información?	En la actualidad no se cuenta con un documento que reúna todas las medidas técnicas necesarias para abordar las situaciones de contingencia presentadas en la Red. Sólo se basan en las experiencias de los administradores para atender las situaciones que puedan afectar los activos; y las mismas son propias de cada una de las Direcciones.	Es necesario que la universidad cuente con un plan de contingencia que reúna todas las acciones y gestiones que se deban realizar en caso de que se produzcan incidentes de seguridad que afecten los activos de información, así como la continuidad de los mismos.

Pregunta	Respuesta Obtenida	Análisis
5. ¿Qué tan concientizados están los usuarios en cuanto a los riesgos a los que están expuestos sus sistemas de información?	Se han realizado varias campañas de concientización a los usuarios, debido a problemas encontrados tales como virus, ataques informáticos los cuales afectan de una forma u otra forma a la Red. Se les dio a conocer la importancia de utilizar los antivirus al momento de utilizar dispositivos extraíbles, así como también, visitar sólo las páginas autorizadas; evitando de esta manera cualquier propagación de código maliciosos en la Red. Actualmente los usuarios no tienen el firme conocimiento de mantener la Red Operativa, sólo la utilizan para sus necesidades; igualmente se desconoce los riesgos que puedan implicar el uso inadecuado de los servicios.	Los usuarios deben entender los beneficios de contar con una infraestructura tecnológica como es la RedUCLA y de los riesgos que se corren por no hacer uso adecuado de los recursos o por desconocimiento de las políticas de seguridad.
6. ¿Cuáles son los riesgos a nivel de seguridad de la información si la Red fallara?	En caso de presentarse una falla en la Red, se verá afectado toda la Gestión Académica – Administrativo, debido a que todos los sistemas Administrativos y Académicos son gestionados sobre la Red. Las actividades estudiantiles no se afectan, sin embargo no se podrá hacer consultas, ni ningún tipo de gestión sobre la Red.	Se observa claramente la importancia que representan los sistemas de información y la red para el funcionamiento normal de la Universidad. De allí que se deba gestionar los riesgos adecuadamente, ya que permitirá a los gerentes y administradores de red tomar mejores decisiones en las áreas técnicas de acuerdo al diagnostico de los sistemas, y de esta manera seleccionar los mejores mecanismos de protección.

Pregunta	Respuesta Obtenida	Análisis
7. ¿Se han realizado evaluaciones de riesgos de seguridad de la información en la Red de la Universidad? En caso de ser afirmativo, indique los resultados obtenidos.	Se han realizado algunos Análisis apoyados en las ayudantías y tesistas. Los resultados reflejaron ciertos problemas en el ancho de banda de la Red, de igual forma se pudo observar que no todos los usuarios tienen el conocimiento o la capacitación para reconocer los problemas e incidentes de seguridad que puedan implicar hacer uso inadecuado de los servicios; en muchas oportunidades estas acciones pueden originar abrir puertas de acceso a un hacker. No obstante, se cuenta con un firewall el cual ha servido de gran ayuda en la Red. Las evaluaciones de riesgo que se han realizado han dado lugar a tomar acciones sobre la seguridad lógica de la Red.	La evaluación de riesgos consiste en elaborar un proceso de diagnóstico y detección. Permite identificar las relaciones funcionales entre los distintos activos de información, analiza todas las posibles contingencias que pueden presentarse. Dentro de este marco, establece un contexto de seguridad en el que se encuentra la infraestructura, permitiendo elegir herramientas de seguridad adecuadas para garantizar los requisitos de seguridad.
8. ¿Se han realizado auditorias informática a la Red de la Universidad? ¿Indique de qué tipo?	Se han realizado tres auditorias enfocadas a ciertos sectores de la Red. Todas señalaron que existen fallas de infraestructura, de igual forma vulnerabilidad de riesgo alta y muy alta. Se considera necesario realizar auditorías a los sistemas de información Administrativos y Académicos, los cuales son competencia de otras direcciones dentro de la Universidad.	La auditoria informática es un proceso de revisión e inventario, con el propósito de analizar en qué medida el sistema garantiza la Seguridad de la Información, y permite la detección de puntos de fallo concretos sobre cada activo, razón por la cual debe aplicarse.
9. ¿Se ejecutan pruebas a las aplicaciones o software desarrollados, a fin de verificar que estén cumpliendo con los requisitos de seguridad definidos por la dirección? ¿De qué tipo?	Sólo se realizan pruebas de los desarrollos Web de la dirección para verificar todos los puertos y lo posibles ataques. Sin embargo, a los sistemas de información desarrollados por otras direcciones no se tiene el pleno control de ello, debido a que no se cuenta con una política de seguridad de los sistemas de información en la data.	Se deben llevar a cabo pruebas de seguridad apropiada a los sistemas de información (caja negra, caja blanca) durante su desarrollo y antes de ser implementados en la red. La norma establece que la gerencia debe asegurar que los requerimientos y criterios de aceptación de los sistemas nuevos deben estar claramente definidos, aceptados, documentados y probados.

Pregunta	Respuesta Obtenida	Análisis
10. ¿Se realizan pruebas de intrusión a la infraestructura tecnológica para detectar posibles vulnerabilidades y accesos a sistemas por usuarios no autorizados? En caso afirmativo, indique cuáles.	Sólo se realizan pruebas de intrusión a la puerta de acceso a internet y al firewall, sin embargo en ciertos sectores puntales como la red académica no se realiza, debido a la ausencia de políticas de seguridad en los sistemas de información.	Las pruebas de intrusión se realizan para complementar la revisión de controles de seguridad y garantizar que la infraestructura tecnológica este asegurada. Es necesario que las mismas se realicen a todos los equipos principales de la red router, firewall, servidores, switch. Los resultados de estas pruebas de seguridad permitirán identificar las vulnerabilidades de los sistemas.

Fuente: Gil (2011)

Igualmente, se aplicó una entrevista (Anexo C) a los Profesores expertos en el área de seguridad de la información del Decanato de Ciencias y Tecnologías de la UCLA, con la finalidad de Identificar los componentes para diseñar el proceso de sistematización de la gestión de riesgos de Seguridad de la Información en la red de la Universidad Centroccidental "Lisandro Alvarado"

Cuadro 6

Matriz de Análisis de Contenido. Entrevista a los Profesores expertos en el área de seguridad de la información

Pregunta	Respuesta Obtenida	Análisis
1. ¿Conoce usted el estándar ISO 27001:2005 Sistemas de Gestión de Seguridad de la Información?	En resumen, todos afirmaron conocer la norma ISO 27001:2005.	Los profesores expertos conocen la norma para identificar todos los componentes de la gestión de riesgos en base a la norma ISO 27001, elemento fundamental en el desarrollo de la investigación.

Pregunta	Respuesta Obtenida	Análisis
2. ¿Qué aspectos se deben contemplar al efectuar el proceso de análisis riesgos de seguridad de la información?	Se deben evaluar los procesos, medios de transmisión y almacenamiento que puedan comprometer la seguridad de la información respecto a su disponibilidad, integridad y confidencialidad. También se deben considerar la identificación y valoración de los activos, vulnerabilidades, amenazas, impacto, salvaguardas y control.	La norma establece las siguientes actividades para la realización del análisis de riesgos: identificación y tasación de los activos, calcular el impacto que podría resultar de la perdida de la confidencialidad, integridad y disponibilidad para los activos identificados, identificar y calcular las amenazas y vulnerabilidades; por ultimo calcular los niveles de riesgos.
3. ¿Qué metodología considera apropiada para el análisis de riesgos de seguridad de la información? Indique por qué.	Existen diversas metodologías de análisis de riesgos, entre la más conocidas Magerit, Cramm, ISO 27005, Octave, entre otras. Se deben considerar metodologías probadas y comprobadas por la comunidad científica y que arrojen resultados repetitivos. Asimismo, se deben escoger aquella que sean sencillas, de manera que simplifique todo el proceso. Se sugiere Magerit, debido a que una metodología abierta de análisis y gestión para los sistemas de información, la misma recomienda las medidas apropiadas que deberían adoptarse para conocer, prevenir, impedir, reducir o controlar los riesgos investigados.	Existen numerosas metodologías estandarizadas para el análisis de riesgos. Se debe tomar aquella que se ajuste a las necesidades de la organización, tomando en cuenta que el análisis de riesgos se debe revisar periódicamente. Aunque es perfectamente aceptable definir una propia. Lo primordial de la metodología, es que los resultados obtenidos sean comparables y repetibles.
4. ¿Qué estrategias se pueden considerar para el tratamiento o reducción de los riesgos?	Se pueden implementar modelos de seguridad probados y comprobados, reconocidos por la comunidad científica, tal como el propuesto por la norma ISO/IEC 27001. Asimismo, se deben considerar las evaluaciones de riesgos y de estar forma aplicar medidas para el tratamiento o aceptación de los riesgos. Además, debe considerarse la comunicación, monitoreo y revisión de los riesgos.	La norma establece que una vez efectuado el análisis y evaluación de riesgos, se debe decidir cuáles son las acciones que se deben tomar con los activos que estén sujetos a riesgos. Se pueden manejar los riesgos con controles de detección o prevención y aplicando tácticas para Transferirlo, Eliminarlo, Mitigarlo o Asumirlo.

Pregunta	Respuesta Obtenida	Análisis
5. Según su opinión, ¿cuáles considera son las principales amenazas que presenta en la RedUCLA?	La principal amenazas tiene que ver con la disponibilidad de los servicios y de la información que contienen, la difusión masiva de virus informáticos y el acceso a internet. Por ende, se deberían implementar estrategias que garanticen tanto la disponibilidad de los servicios (correo, internet, intranet) como su aceptable prestación (que no estén degradados). Los planes deben considerar el crecimiento normal de la demanda.	Es necesario identificar las amenazas que pueden afectar a estos activos y evaluar su posibilidad de ocurrencia.
6. Según su opinión, ¿cuáles considera son las principales vulnerabilidades que presenta en la RedUCLA?	La obsolescencia de la infraestructura de red y de los equipos servidores, la Interrupción de servicio eléctrico. También se puede considerar la deficiencia de la red WiFi en puntos estratégicos.	Las vulnerabilidades son debilidades, que permite que una amenaza cause daño a la organización. De allí la importancia de evaluar las posibles amenazas que puedan afectar un activo de información.
7. ¿Cómo experto en el área indique como se puede mejorar su seguridad con un enfoque para la gestión de riesgos de seguridad de la información?	Implementando con rigurosidad la norma ISO/IEC 27001. Al mismo tiempo, se puede considerar el diseño de una nueva metodología para el análisis de riesgos en los SGSI para la UCLA.	Es necesario conocer los riesgos que corren los activos de información y de esta forma evitarlos, aplicando controles para disminuir o eliminar su posibilidad de ocurrencia. La norma ISO/IEC 27001 especifica los requisitos para establecer, implantar, documentar y evaluar un Sistema de Gestión de seguridad de la información (SGSI) dentro del contexto de los riesgos identificados por la Organización.

Fuente: Gil (2011)

Resultados del Cuestionario

El cuestionario (Anexo D) se aplicó a los administradores de la RedUCLA. Dicha entrevista se realizó con la finalidad de conocer aspectos sobre la Gestión de Riesgos de Seguridad de la Información en la RedUCLA. Los resultados de la aplicación del instrumento se muestran a continuación.

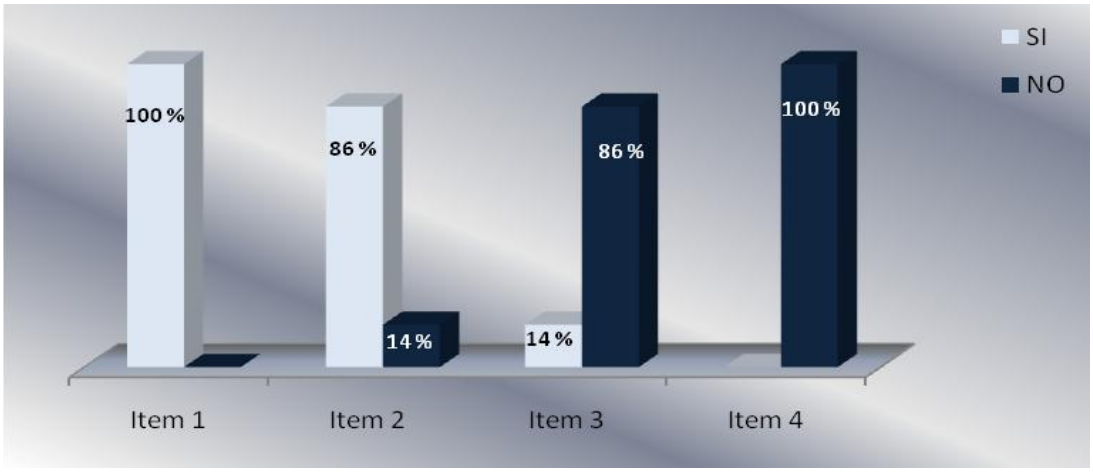

Gráfico 7. Medición de la Variable Gestión de Riesgos. Indicador: Políticas de Seguridad.
Nota: Resultado obtenido de la aplicación de cuestionario.

En el gráfico 7 se presenta la información del indicador políticas de seguridad, y en él se observa lo siguiente:

En el ítem 1, referido a la existencia de políticas de seguridad de la información, se encontró que el 100% de los encuestados manifestaron que la Universidad cuenta con políticas de seguridades de la información formalmente documentadas y aprobadas por el consejo universitario. La documentación y divulgación de las políticas de seguridad de la información, son elementos fundamentales en la gestión de seguridad de la información.

En lo que se refiere al ítem 2 aspectos de regulación de la gestión de riesgos de seguridad de la información, se puede observar que el que 86% de la muestra considera que las políticas de seguridad contienen aspectos para la regulación de la gestión de los riesgos en seguridad, sin embargo se encontró que un 14% de los

encuestados no conocen los aspectos de regulación que contienen las políticas de seguridad.

Asimismo, en el ítem 3 referido al conocimiento de las políticas de seguridad por parte de los usuarios, se observa que el 86% de los encuestados considera que las políticas de seguridad no son del conocimiento de los usuarios de la red. Se presume que a causa del desconocimiento de las políticas, los usuarios no hagan buen uso de los servicios de la red. Es fundamental que los usuarios perciban la importancia de las políticas de seguridad y sean conscientes de que no es una comunicación más dentro de la organización, sino que debe ser asumida y puesta en práctica.

Por último, en el ítem 4 diseños de las políticas de seguridad, se observa que 100% de los encuestados considera que las políticas de seguridad no han sido elaboradas en base a la norma ISO 27001:2005, por lo que se infiere, que la misma no se encuentra actualizada. Las políticas de seguridad de la información deben ser revisadas periódicamente, a intervalos planificados; y en los casos puntuales en que se produzcan cambios que afecten la infraestructura tecnológica de la Universidad.

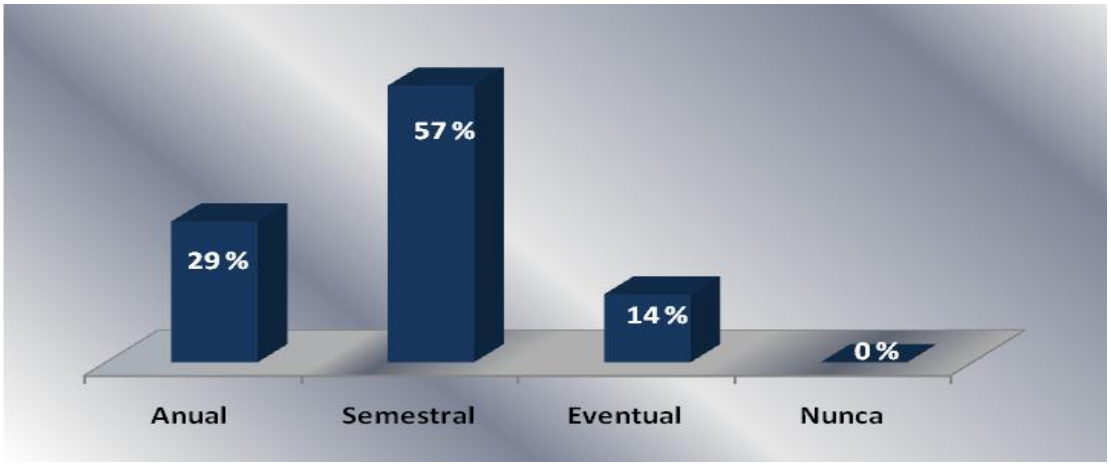

Gráfico 8. Medición de la Variable Gestión de riesgos. Indicador: Frecuencia de realización de inventarios

Nota: Resultado obtenido de la aplicación de cuestionario.

En ítem 5 indicada en el gráfico 8 referido a la frecuencia de realización de inventario, se observa que el 57% de los encuestados considera que se realizan inventarios semestrales de los equipos asociados en la red, mientras que el 29% dijo

que se realizan anualmente y por ultimo un 14% considera que se realizan de forma eventual. Es importante que se cuente con inventarios de los activos importantes de la red para de esta forma se pueda realizar un protección efectiva de los mismos. También es un elemento significativo en la gestión de riesgos.

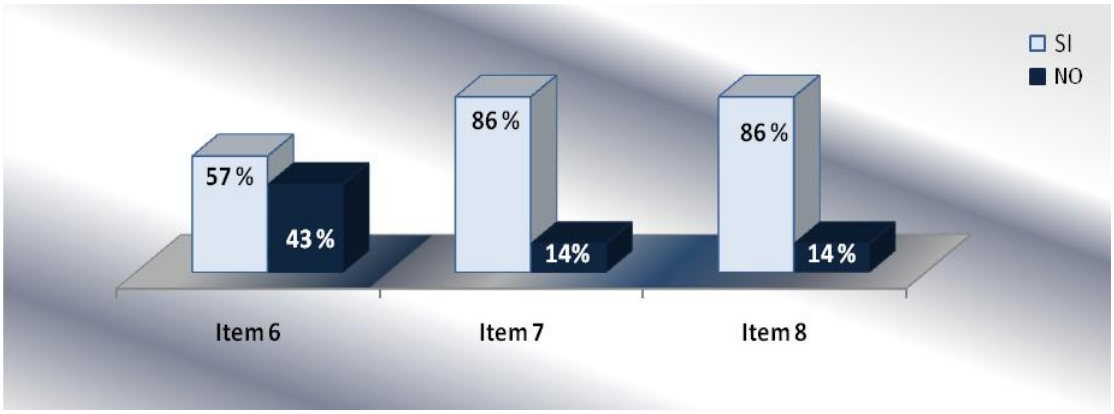

Gráfico 9. Medición de la Variable Gestión de Riesgos. Indicador: Activos de Información
Nota: Resultado obtenido de la aplicación de cuestionario.

En el gráfico 9, se observa en el ítem 6 referido a los planes de contingencia, que un 57% de los encuestados considera que si Existen planes de contingencia ante situaciones de desastres que puedan afectar los activos de la información, el otro 43% considera que no. De este ítem puede inferir que no se cuenta con los planes de contingencia formalmente documentados o que los mismos no son del conocimiento de todos los empleados. Es importante que el personal conozca las acciones a realizar en casos de que se produzcan incidentes de seguridad que afecten los activos de la información, garantizando la confidencialidad, integridad y disponibilidad de ésta en el menor tiempo posible.

Asimismo, se observa en el ítem 7 reglas para el control de uso de la información. Se observa que el 86% considera que la universidad cuenta con reglas para el control de uso aceptable de los activos de información. Por lo que se puede deducir que los usuarios deberían conocer los límites existentes para el uso de la

información y los activos asociados con los medios y recursos de procesamiento de la información por lo cual estos son los responsables por el uso que le den a los mismos.

En ítem 8 correspondiente a los controles para mitigar los riesgos, se observa que el 86% de los encuestado considera que en la RedUCLA existen controles para mitigar los riesgos, mientras un 14% considera que no. Es importante la aplicación de controles para de esta forma se pueda asegurar la seguridad de la información.

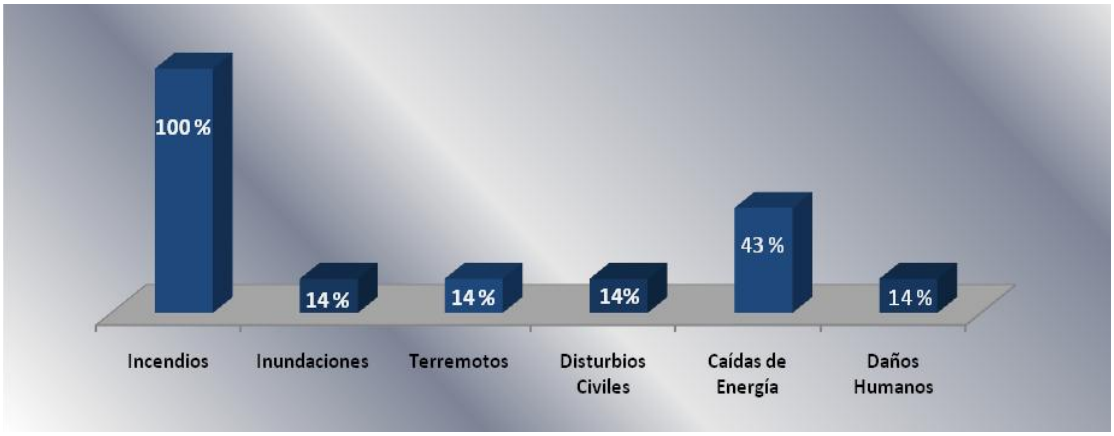

Gráfico 10. Gestión de riesgos. Indicador: Mecanismos de Protección Contra Riesgos.
Nota: Resultado obtenido de la aplicación de cuestionario.

El gráfico 10, muestra el comportamiento de ítem 9 mecanismos de protección contra riesgos, donde se observa que los principales mecanismos de protección contra amenazas en el área de comunicaciones de la RedUCLA son: los controles contra incendio y contra caídas de energía. Es necesario prestar atención a cualquier amenaza física o ambiental que pueda afectar el área de comunicaciones.

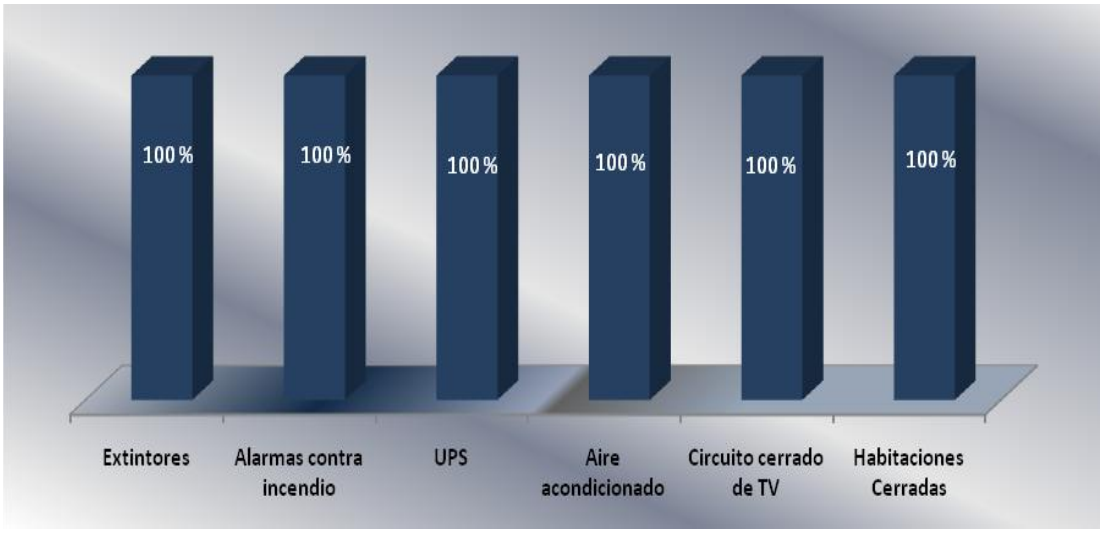

Gráfico 11. Medición de la variable Gestión de riesgos. Indicador: Mecanismos de Protección Contra Amenazas Implantados.

Nota: Resultado obtenido de la aplicación de cuestionario.

Del resultado del ítem 10 mecanismos de protección contra amenazas implantados, mostrado en el gráfico 11, se puede inferir que se están aplicando controles para la protección de los equipos contra amenazas físicas externas y se salvaguardan los equipos de comunicaciones contra fallas de suministros eléctricos, incendio, robos; además de contar con mecanismo de control adecuados para mantener en buenas condiciones ambientales los equipos de comunicaciones.

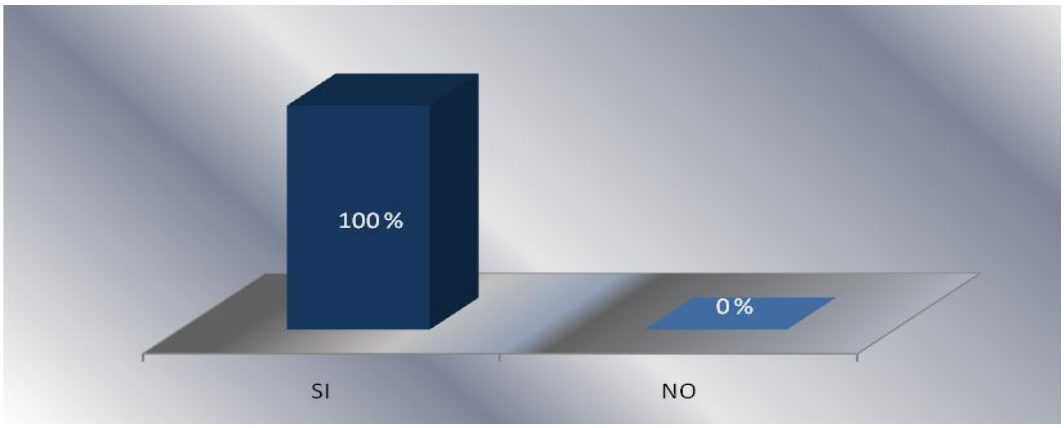

Gráfico 12. Medición de la variable Gestión de Riesgos. Indicador: Documentación y notificación de las situaciones de contingencia.

Nota: Resultado obtenido de la aplicación de cuestionario.

En el gráfico 12, referido al ítem 11 documentación y notificación de las situaciones de contingencia, se observa que el 100% de los encuestados considera que las situaciones de contingencia si son documentadas y notificadas oportunamente. Se presume que se cuentan con procedimientos para el registro de los eventos de contingencia ocurridos en la red.

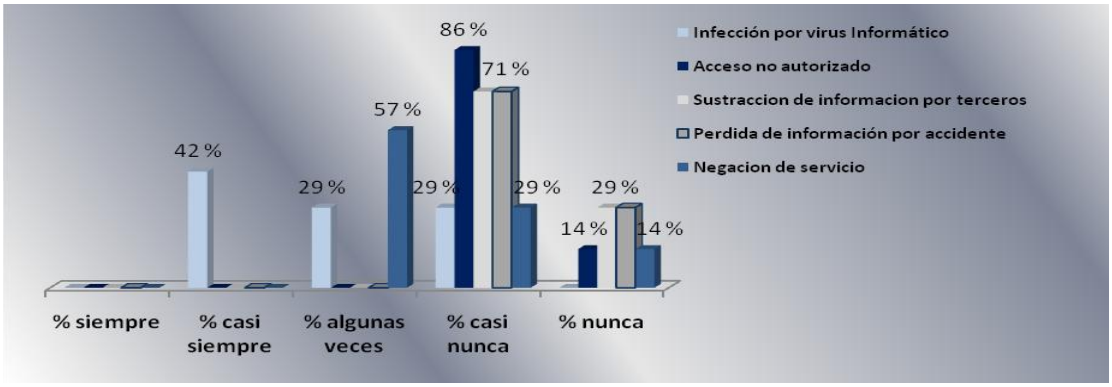

Gráfico 13. Medición de la variable Gestión de riesgos. Indicador: Incidentes de Seguridad.

Nota: Resultado obtenido de la aplicación de cuestionario.

El gráfico 13, donde se observa el comportamiento del ítem 12 incidentes de seguridad en la RedUCLA, muestra que el principal incidente de seguridad que ha ocurrido en la red de la universidad ha sido la infección de virus informático, dado en

un 42% y la denegación de servicio tuvo una proporción del 57 %. Por lo que se puede inferir que a pesar de los controles que se han implementado en la red para reducir su posibilidad de ocurrencia, los mismos no se han podido mitigar en su totalidad.

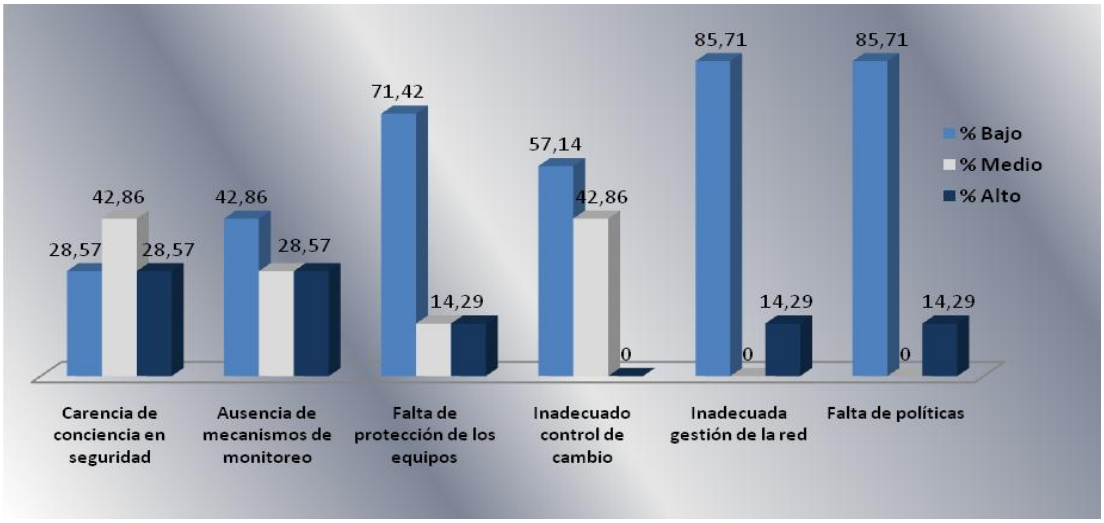

Gráfico 14. Medición de la variable Gestión de riesgos. Indicador: Vulnerabilidades

Nota: Resultado obtenido de la aplicación de cuestionario.

Se observa en el gráfico 14, referido al ítem 13 Vulnerabilidades en la RedUCLA, se observa que la carencia de conciencia de seguridad de la información por parte de los usuarios fue considerada por lo encuestados con una vulnerabilidad media 42,86, mientras que el resto de las vulnerabilidades fueron consideradas de bajo riesgo para la red. Sin embargo, se deber evaluar la posibilidad de que amenazas puede aprovechar esas vulnerabilidades y causar un incidente de seguridad que afecte los servicios de la red.

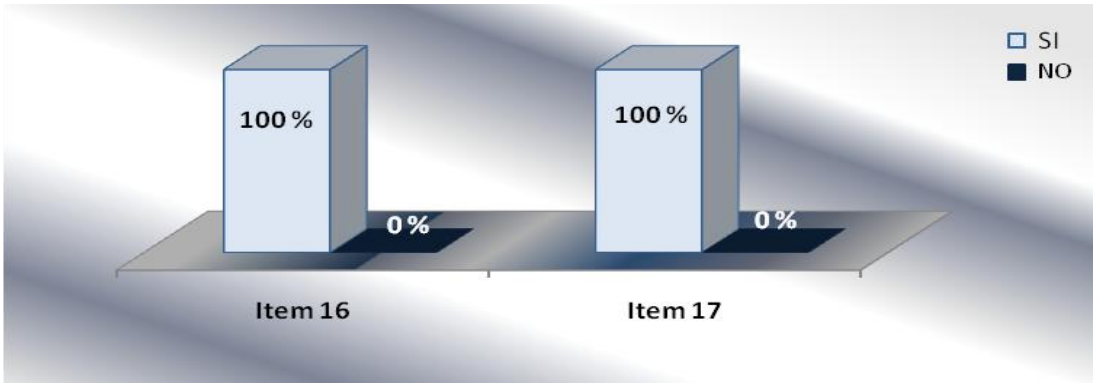

Gráfico 15. Medición de la variable Gestión de Riesgos. Indicador: Mantenimiento Preventivo.

Nota: Resultado obtenido de la aplicación de cuestionario.

El gráfico 15, correspondiente a los ítems 16 y 17 mantenimiento preventivo, indica que el 100% de los encuestados considera que la infraestructura de hardware y software asociados a la RedUCLA cuentan con planes de mantenimiento preventivo. El mantenimiento de los equipos afecta directamente a la seguridad de la infraestructura tecnológica y se debe llevar un control del mantenimiento de la misma, por lo que se infiere que la RedUCLA cuenta con un plan de mantenimiento adecuado de la infraestructura de hardware y software; asegurando la continua disponibilidad e integridad de la información.

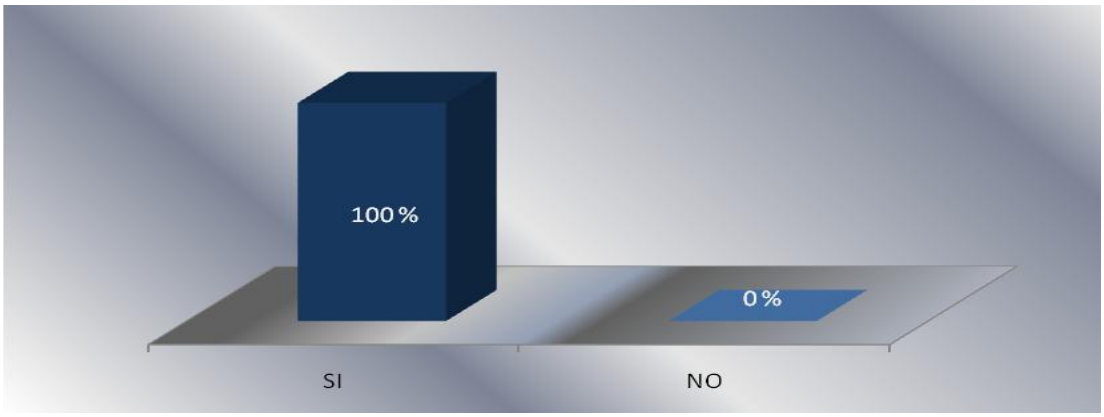

Gráfico 16. Medición de la variable Seguridad de la Información. Indicador: Mecanismos para la protección de la red contra códigos maliciosos.

Nota: Resultado obtenido de la aplicación de cuestionario.

En el gráfico 16, correspondiente al ítem 14 Mecanismos para la protección de la red contra códigos maliciosos, se observa que la totalidad de los encuestados manifestaron que la red cuenta con mecanismos de protección contra códigos maliciosos. De este resultado se deduce que la red posee mecanismos para la prevención contra amenazas como lo son los virus informáticos.

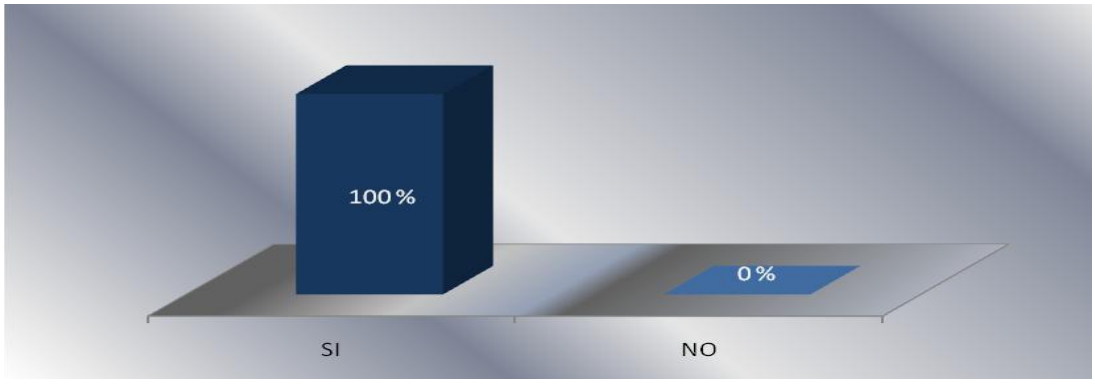

Gráfico 17. Medición de la variable Seguridad de la Información. Indicador: Accesos de los usuarios a los Servicios autorizados de la Red.

Nota: Resultado obtenido de la aplicación de cuestionario.

El gráfico 17, referido al ítem 15 acceso de los usuarios a los servicios de la red, indica que el 100% de los encuestados considera que los usuarios de la red sólo tienen acceso a los servicios para los cuales han sido autorizados, por lo que se infiere

que el acceso de los usuarios a la red y sus servicios se encuentran controlados. Es importante destacar que las conexiones no autorizadas e inseguras a los servicios de la red pueden afectar a toda la organización.

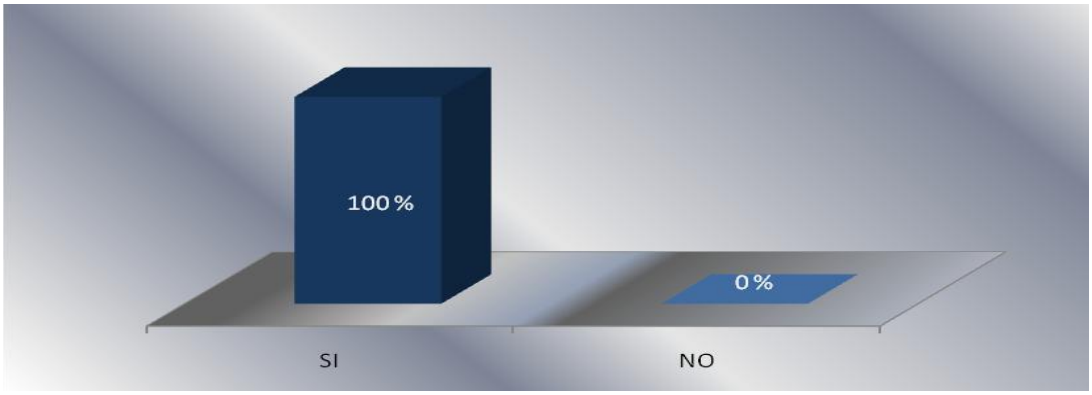

Gráfico 18. Medición de la variable Seguridad de la Información. Indicador: Proyecciones de los requerimientos de los sistemas a ser implementados dentro de la RedUCLA.

Nota: Resultado obtenido de la aplicación de cuestionario.

En el gráfico 18, correspodiente al item 18 proyecciones de los requerimientos de los sistemas, se observa que el 100% de los encuestados considera que se realizan proyecciones de los requerimientos de los sistemas a ser implementados dentro de la RedUCLA, por lo que se infiere que se evalúan los requerimientos mínimos de capacidad y seguridad de los sistemas a ser implementados. De esta forma se reduce el riesgo de sobrecarga y se asegura la disponibilidad del sistema de acuerdo al desempeño requerido.

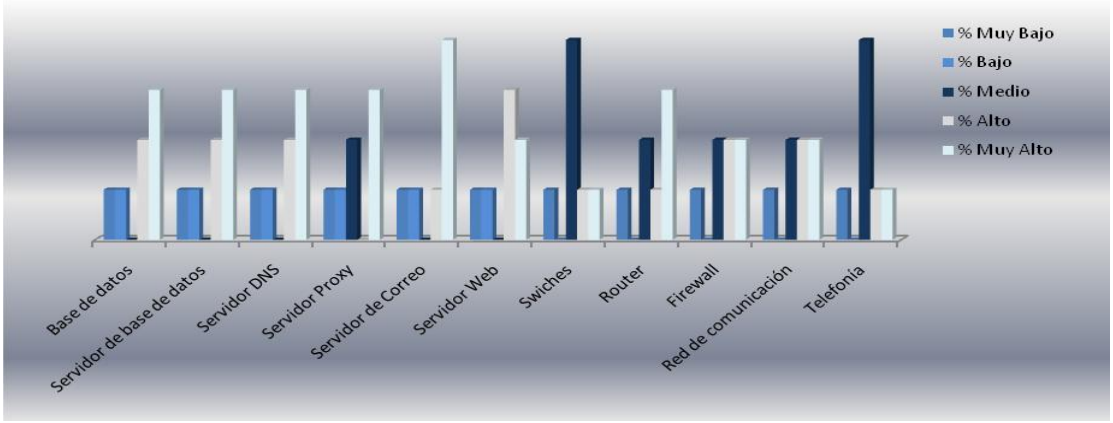

Gráfico 19. Medición de la variable Seguridad de la Información. Indicador: Integridad.
Nota: Resultado obtenido de la aplicación de cuestionario.

El gráfico 19, referido al ítem 19 niveles de afectación de la integridad, muestra que un 80% de los encuestados manifiesta que el nivel de afectación por la pérdida de integridad de los activos de información es alto o muy alto para la red. Es importante la aplicación de controles que protejan la integridad de los activos.

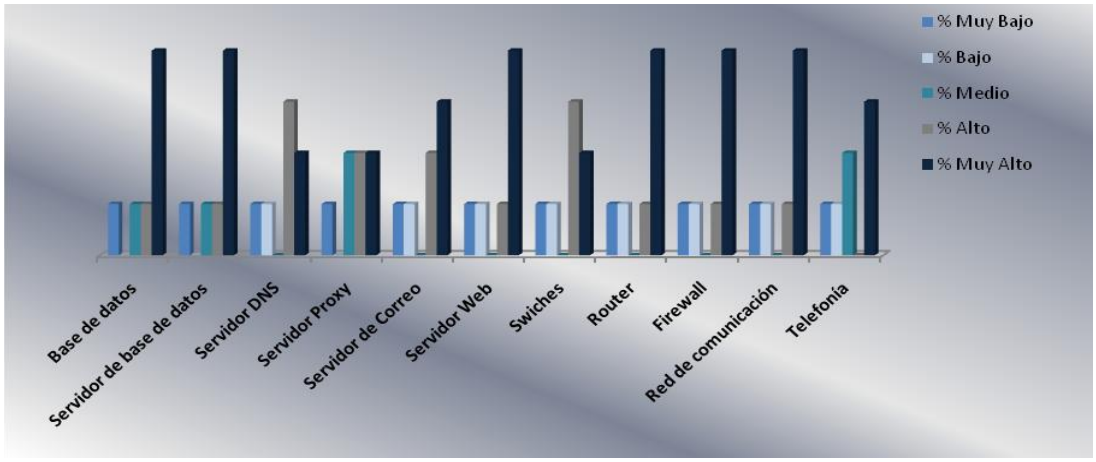

Gráfico 20. Medición de la variable Seguridad de la Información. Indicador: Confidencialidad.
Nota: Resultado obtenido de la aplicación de cuestionario.

Se puedo observar en el gráfico 20, correspondiente al ítem 20 niveles de afectación de la confidencialidad, que el 80% de los encuestados considera alto o muy alto el nivel de afectación por la pérdida de confidencialidad en todos los activos de información. De allí la importación de preservar la confidencialidad de los activos.

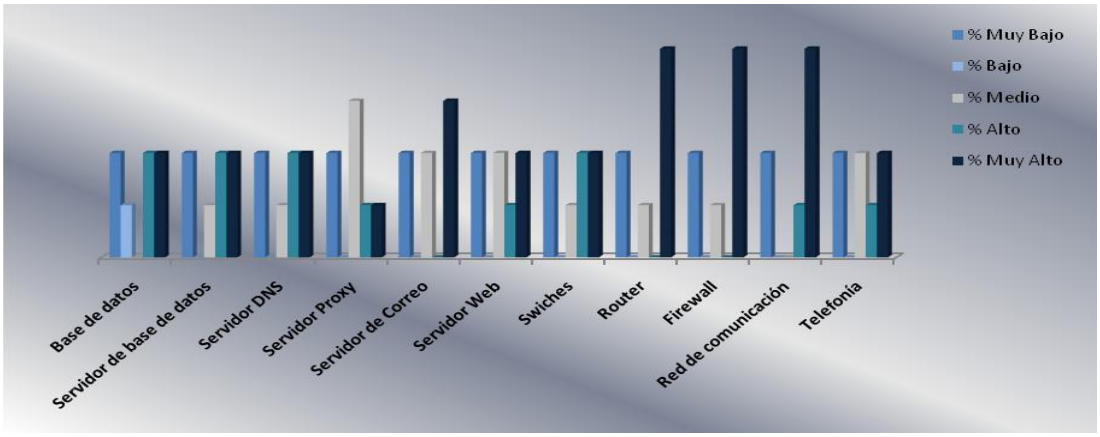

Gráfico 21. Medición de la variable Seguridad de la Información. Indicador: Disponibilidad.

Nota: Resultado obtenido de la aplicación de cuestionario.

En el gráfico 21, se puede observar en el ítem 21 niveles de afectación de la disponibilidad, que el 80% de los encuestados consideraron alto o muy alto el nivel de afectación por la pérdida de disponibilidad en todos los activos de información, a excepción de servidor proxy, que tuvo una valoración de afectación medio. De allí la importancia de aplicar controles que permitan la disponibilidad de los activos.

De los resultados obtenidos a través del cuestionario aplicado se pudo observar lo siguiente:

Políticas de Seguridad:

- ✓ La universidad cuenta con políticas de seguridad de la información formalmente documentada y aprobada por el consejo universitario.
- ✓ Un ochenta y seis por ciento de los encuestados (86%) considera que las políticas contienen aspectos para la regulación de los riesgos de seguridad de la información y que los usuarios desconocen las políticas de seguridad de seguridad.
- ✓ Un cien por ciento (100%) considera que las políticas no han sido desarrolladas en base a la Norma ISO 27001.

Gestión de Activos:

- ✓ Un cincuenta y siete por ciento (57%) considera que la frecuencia de la realización de inventarios de los quipos de comunicación asociados a la RedUCLA, se realiza de manera semestral y que la Universidad cuenta con planes de contingencia ante situaciones de desastres que puedan afectar a los activos de información.
- ✓ Un ochenta y seis por ciento de los encuestados (86%), manifestó que existen reglas para el control de uso aceptable de los activos de información y que además existen reglas para mitigar los riesgos

Amenazas:

- ✓ Se observo que el mecanismo de protección más utilizado para minimizar los riegos de amenazas en el área de comunicaciones ha sido los controles contra incendio en un cien por ciento (100%).
- ✓ Un cien por ciento (100%) de los encuestados considera que las situaciones de contingencia son documentadas y notificadas oportunamente, además se han aplicados mecanismos contra amenazas físicas y externas.
- ✓ Un cuarenta y dos por ciento (42%) de los encuestados considera que el principal incidente de seguridad en la RedUCLA ha sido la infección por virus.

Vulnerabilidades:

- ✓ Un cuarenta y tres por ciento (43%) de los encuestados considera una vulnerabilidad media la carencia de seguridad de la información por parte de los usuarios.
- ✓ Un ciento por ciento (100%) considera que la RedUCLA cuenta con planes de mantenimiento preventivo de la infraestructura de hardware y software asociados a la RedUCLA.

Integridad:

- ✓ Un ciento por ciento (100%) considera que existen mecanismos para la protección en la red contra códigos maliciosos.
- ✓ Un ochenta por ciento (80%) considera alta el nivel de afectación de la pérdida de integridad en los principales activos de información.

Confidencialidad:

- ✓ Un ciento por ciento (100%) considera que los usuarios tienen acceso solo a los servicios que han sido autorizados.
- ✓ Un ochenta por ciento (80%) considera alta el nivel de afectación de la pérdida de confidencialidad en los principales activos de información.

Disponibilidad:

- ✓ Un ciento por ciento (100%) considera que se realizan proyecciones de los sistemas a ser implementados dentro de la RedUCLA.
- ✓ Un ochenta por ciento (80%) considera alta el nivel de afectación de la pérdida de Disponibilidad en los principales activos de información.

CAPITULO V

CONCLUSIONES Y RECOMENDACIONES

A continuación se presentan las conclusiones y recomendaciones como resultados de la investigación:

Conclusiones

- Las entrevistas y cuestionario aplicados permitieron conocer la situación actual de la gestión de riesgos de seguridad de la información en la RedUCLA, donde se encontró que las políticas de seguridad de seguridad no se encuentran actualizadas, la misma solo contempla la regulación de la gestión de riesgos a nivel lógico y un 86% de los usuarios la desconoce.
- Las políticas de seguridad de la información son de vital importancia para el funcionamiento de la estructura de seguridad de las Organizaciones, debido a que ayudan a dirigir y dar soporte al proceso de gestión de riesgos de seguridad de la información, asimismo permiten establecer todos los lineamientos necesarios para determinar qué se quiere proteger dentro de las organizaciones y porqué; además deben estar alineadas a los objetivos de la organización, aprobada por la dirección y comunicada a todos los empleados y terceras partes.
- El análisis y gestión de riesgos proporciona a los gerentes de las organizaciones, información de donde residen los problemas actuales o potenciales de seguridad de la información y por tanto tomar mejores decisiones para alcanzar el nivel de seguridad deseado.

- La seguridad de la información protege a la información desde tres aspectos importantes la confidencialidad, la integridad y la disponibilidad, además es un proceso que debe ser revisado y evaluado continuamente.
- Las metodologías para el análisis de riesgos conllevan de una manera sistemática y estructurada, aplicar técnicas, métodos adecuados y homogéneos.
- Las valoraciones de riesgo permite identificar las amenazas que pueden comprometer los activos, su vulnerabilidad e impacto en la organización, determinando el nivel del riesgo.
- El proceso de gestión de riesgos aplicado a cualquier actividad consta de las siguientes etapas: Establecimiento del contexto, Identificación, Análisis, Evaluación, Tratamiento, Monitoreo y revisión, por último comunicar y consultar los riesgos.
- Las medidas de seguridad necesarios para proteger la información deben ser lógicas, físicas, legales, organizativas y fundamentalmente trabajar de manera integrada.

Recomendaciones:

- Es necesario la actualización del documento de políticas de seguridad de la Universidad de acuerdo al estándar ISO 27001 y en él se incluyan todas las medidas para la protección de la información desde el punto de vista lógico, físico, legal y organizativo.
- Para el cumplimento de las políticas de seguridad se debe diseñar un plan de concientización, para lograr que el personal perciba la importancia de contar con políticas de seguridad y cuáles son sus responsabilidades, de esta forma lograr una cultura de seguridad en la organización; además este proceso puede ser apoyado con un plan de formación para determinar cuáles son las necesidades de formación en el personal y sus posibles carencia.
- Diseñar y ejecutar un plan de contingencia que cubra todos los aspectos que se van a adoptar en caso de incidentes relacionados con la pérdida de información

a través de estrategias de recuperación y políticas de respaldo, que permitan la recuperación de los activos de información en respuesta a los desastres de seguridad.

- Analizar los principales activos de información de la infraestructura y determinar su valor.
- Es necesario que la Gerencia de Telecomunicaciones oriente a los usuarios sobre la importancia de gestionar los riesgos de seguridad de la información.
- Para reducir las vulnerabilidades y amenazas presentes se debe promover el establecimiento de la normas ISO 27001:2007 Sistema de Gestión de Seguridad de la información, ya que misma establece once dominios de control clasificados en seguridad lógica, física, organizativa y legal
- Poner en práctica la propuesta del proceso de Gestión de Riesgos de Seguridad de la Información.

CAPITULO VI

DISEÑO DE LA PROPUESTA

En este capítulo se presenta el diseño del proceso para la sistematización de la gestión de riesgos de seguridad de la información en la red de la Universidad Centroccidental “Lisandro Alvarado”

Presentación de la propuesta

Se hace necesario en toda institución u organización contar con una herramienta que les garantice, una forma adecuada de evaluación de los riesgos de seguridad de la información a las que están expuestos sus procesos y actividades de información.

Viendo la necesidad en el entorno de la Universidad de este tipo de herramientas y teniendo en cuenta que una de las principales causas de los problemas dentro del entorno informático, es la inadecuada gestión de los riesgos por lo tanto se deben realizar actividades coordinadas para dirigir y controlar una organización con respecto a estos, ya que le va a permitir analizar lo que se debería hacer y cuando hacerlo, con el fin de reducir el riesgo a un nivel aceptable. Por su parte, el análisis de riesgos implica: determinar qué se necesita proteger, de qué hay que proteger y cómo hacerlo.

Es por ello que con esta propuesta del proceso de Sistematización de la Gestión de Riesgos de Seguridad de la Información, permitirá a los administradores de la RedUCLA de una forma organizada administrar los incidentes de seguridad que se puedan presentar, alineados a los objetivos de la institución; asimismo permite la toma de decisiones sobre los riesgos que puedan impactar en el funcionamiento de la infraestructura tecnológica.

El proceso de gestión de riesgos de seguridad de la información se fundamenta en los siguientes principios:

- Confidencialidad: Solo quienes estén autorizados pueden acceder a la información.
- Integridad: La información y sus métodos de proceso son exactos y completos en todo momento
- Disponibilidad: Los usuarios autorizados tienen acceso a la información y a sus activos asociados cuando lo requieran.

En consecuencia, el análisis y gestión de los riesgos permite conocer donde residen los problemas actuales o potenciales que se debe solucionar para alcanzar el nivel de seguridad deseado.

La siguiente propuesta quedo estructurada de la siguiente manera:

1. Fundamentación teórica

Para el diseño del proceso de gestión de riesgos de Seguridad de la Información en la Red de la Universidad Centroccidental "Lisandro Alvarado" (RedUCLA), se utilizó la norma ISO/IEC 27001:2005, este estándar adopta el modelo del proceso Planificar-Hacer-Verificar-Actuar (PHVA), el mismo se puede aplicar a todos los procesos del Sistema de Gestión de Seguridad de la Información (SGSI). Su propósito es garantizar que los riesgos de seguridad de la información sean conocidos, asumidos, gestionados y minimizados por la organización. Se tomó como guía la primera fase del modelo "Planificar" que explica los procedimientos adecuados para la realización de un análisis y gestión de riesgos.

También se apoyó el diseño en la norma ISO/IEC 27002:2005, la cual es una guía de buenas prácticas que describe los objetivos de control y controles recomendados en cuanto a seguridad de la información. Igualmente, se utilizó la ISO/IEC 27005:2007, esta norma proporciona una guía para la gestión del riesgo en un sistema de seguridad de la información. La misma soporta los conceptos definidos en la ISO/IEC 27001 y está diseñado para ayudar a la implementación de un sistema de seguridad de la información basado en la gestión del riesgo.

Para efectos del diseño del diseño de proceso de gestión de riesgo de seguridad de la información se utilizó la metodología de la cadena de valor de Potter (1985), la misma está constituida por una serie de procesos que describen como se desarrolla determinada actividad en una organización. Constituido por actividades primarias, las mismas estarán relacionadas con la producción de servicios y actividades secundarias o actividades de apoyo, que hacen posible la realización de las actividades primarias. Asimismo puede decirse que, la gestión de riegos presentada en la propuesta, refleja las actividades principales, secundarias y de apoyo a seguir para la gestión de riesgos de la seguridad de la información de la RedUCLA.

2. Objetivo de la propuesta

General:

Diseñar el proceso para la sistematización de la gestión de riesgos de seguridad de la información en la red de la Universidad Centroccidental “Lisandro Alvarado”

Específicos:

1. Definir el proceso de gestión de riesgos de seguridad de la información
2. Describir las fases para el proceso de gestión de riesgos de seguridad de la información
3. Presentar la Sistematización de la gestión de riesgos de seguridad de la información en la red de la Universidad Centroccidental “Lisandro Alvarado.

3. Desarrollo de la Propuesta

En lo que respecta al proceso de gestión de riesgos de la seguridad de la información, puede decirse que en el mismo se debe definir la metodología a seguir para determinar, analizar, valorar y clasificar el riesgo, para posteriormente implementar mecanismos que permitan controlarlo. (Ver gráfico 22)

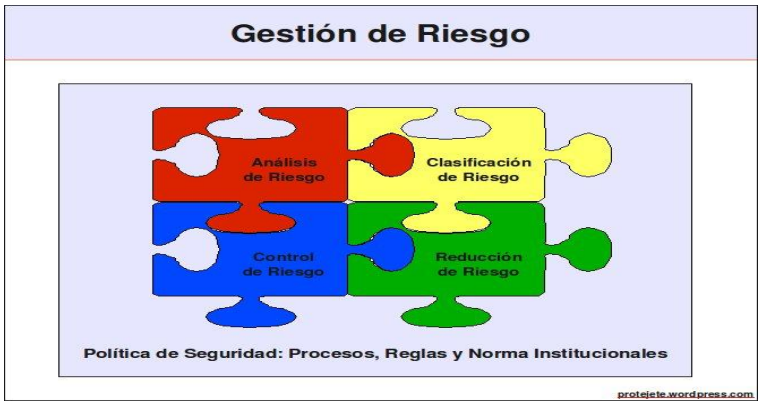

Gráfico 22. Proceso de Gestión de Riesgo
Fuente: Erb (2008)

En este sentido dicho proceso sistemático y lógico de la gestión de riesgos de seguridad de la información, puede incluir las siguientes etapas:

Cuadro 7

Descripción del proceso de gestión de riesgos de seguridad de la información.

Fase	Descripción
1. Determinación del Contexto	Se deberían establecer los criterios básicos necesarios contra los cuales se evaluaran los riesgos, definir la estructura del análisis de riesgos y aceptación de los riesgos.
2. Identificación de los riesgos	Identificar los activos, amenazas y vulnerabilidades.
3. Análisis de los riesgos	Se deben determinar los controles existentes y analizar riesgos en términos de consecuencias y probabilidades en el contexto de esos controles.
4. Evaluación de los riesgos	Compara niveles estimados de riesgos contra los criterios preestablecidos. Esto posibilita que los riesgos sean ordenados como para identificar las prioridades de administración.
5. Tratamiento de los riesgos	Aceptar, monitorear e implantar un plan de tratamiento de los riesgos.
6. Monitoreo y Revisión	Toda la información de riesgos obtenida en el proceso de gestión.
7. Comunicación y consulta	Toda la información de riesgos obtenida en el proceso de gestión.

Fuente: Gil (2011)

Dichas etapas pudieran operacionalizarse de la siguiente forma:

Fases del proceso de gestión de riesgos de seguridad de la información

Las principales fases del proceso de la gestión de riesgos que se define son:

Fase I: Determinar el contexto de la Gestión de Riesgos.

La primera acción a realizar consiste en definir el alcance, objetivos, límites y responsabilidades para establecer una organización adecuada donde opere la gestión del riesgo de seguridad de la información. Asimismo, se deben definir los niveles aceptables de riesgos y la metodología a utilizar.

El alcance del proceso de gestión debe detallar si se aplicara a toda la universidad o parte de ella, un proceso, un departamento o un servicio. Además debe alinearse a las políticas de seguridad de la información existente.

Fase II: Identificación de los Riesgos.

Una vez definido el alcance se deben identificar y clasificar los activos de información, así como también las amenazas y las vulnerabilidades que estén dentro del contexto de gestión de riesgos definidas en la fase I.

(a) Identificación de activos: la primera actividad de esta fase consiste en identificar los activos de información. En efecto, un Activo es todo aquello que tiene valor para la organización y por lo tanto debe protegerse. Asimismo, un activo de información es aquel elemento que contiene o manipula la información. (INTECO, 2010).

De esta forma, para el proceso la identificación de los activos se puede utilizar la siguiente clasificación (ISO 27002:2005):

- ✓Activos de Información: bases de datos y archivos de datos, documentación del sistema, manuales de usuario, materiales de entrenamiento, procedimientos operativos de apoyo, planes de continuidad, entre otros.
- ✓Documentos impresos: contratos, lineamientos, documentos de la institución, documentos que contienen resultados importantes del negocio, entre otros.

- ✓ Activos de Software: software de aplicación, software de sistemas, herramientas de desarrollo y utilidades, entre otros.
- ✓ Activos físicos: servidores, PCs, teléfonos, impresoras, routers, cableado, entre otros.
- ✓ Personas: estudiantes, empleados, profesores, entre otros.
- ✓ Servicios: Servicios de computación y comunicación, entre otros servicios técnicos.
- ✓ Intangible: imagen y reputación de la institución, entre otros.

El cuadro 8, muestra el formato para la realización del inventario de los activos de información.

Cuadro 8

Formato para el Inventario de los activos de Información.

Nro.	Nombre del activo	Tipo de activo	Descripción	Propiedad del Activo	Localización

En efecto, Los activos de información están sujetos a diversas amenazas que aprovechando cualquier vulnerabilidad pueden causar un incidente en la organización.

(b) Identificación de amenazas: Una identificados los activos de información, se efectúa la identificación de amenazas. Una amenaza es un evento o incidente provocado por una entidad natural, humana o artificial que aprovechando una o varias vulnerabilidades de un activo, ponen en peligro la confiabilidad, la integridad o disponibilidad de ese activo, es decir, una amenaza explota la vulnerabilidad del activo(INTECO, 2010). Además, los activos de información se encuentran expuestos a diversas amenazas que pueden afectar su funcionamiento.

Es evidente entonces, que la condición que permite que una amenaza se materialice se debe a la ausencia o debilidad de un control, que puede impactar de forma negativa la organización.

Para el proceso de identificación de amenazas, es necesario identificar el origen de las mismas. Las amenazas pueden ser: deliberados, accidentales o naturales.

Para efecto de la identificación de amenazas, se puede tomar como referencia los tipos de amenazas que lista la ISO 27005:2008 en su anexo C (ver Anexo I)

(c) Identificación de vulnerabilidades: El siguiente paso consiste en identificar las vulnerabilidades. Las vulnerabilidades se refieren a las debilidades que puedan presentar un activo de información. Una vulnerabilidad es una debilidad de seguridad asociada a los activos de información, es decir, es una condición que permite que una amenaza afecte a un activo (De Freitas, 2009).

Para efecto de la identificación de las vulnerabilidades, se puede tomar como referencia los ejemplos correspondiente a vulnerabilidades en diversas aéreas de seguridad que presenta la norma ISO 27005:2008 en su anexo D. (ver Anexo J)

Fase III: Análisis de los Riesgos.

Una vez identificados los activos dentro de alcance, se deben clasificar y valorar los activos de información, así como también la probabilidad de ocurrencia de las amenazas, la posibilidad de explotación de las vulnerabilidades de los riesgos identificados en la fase II.

(a) Valoración de los activos: ya identificado los activos de información, se procede a valorar los mismos en términos del daño que podría suponer la pérdida de un activo que afecte su disponibilidad, integridad y confidencialidad. Esta etapa permite asignar valores a los activos en términos de la importancia que representan para la universidad. Para efectos de la valoración se puede utilizar una escala de likert donde el valor 1 significa Muy Bajo, 2: Bajo, 3: Medio, 4: Alto y 5: Muy Alto; y la pregunta que debe efectuarse para utilizar la escala es: ¿Cómo la pérdida o falla en un

determinado activo puede afectar la disponibilidad, la integridad y la confidencialidad? (Alexander, 2007).

(b) Valoración o probabilidad de ocurrencias de las amenazas: una vez identificadas las amenazas se debe valorar la probabilidad y el impacto que ocasionaría que alguna de las amenaza ocurriera. Para ello se puede utilizar una escala de likert donde el valor 1 significa Muy Bajo, 2: Bajo, 3: Medio, 4: Alto y 5: Muy Alto.

(c) Valoración o posible explotación de las vulnerabilidades: Una vez identificadas las vulnerabilidades, se debe evaluar para cada una de ellas, la posibilidad de ser explotadas por una amenaza (Alexander, 2007). Para ello también se puede utilizar una escala de likert donde el valor 1 significa Muy Bajo, 2: Bajo, 3: Medio, 4: Alto y 5: Muy Alto.

Fase IV: Evaluación de riesgos

Efectuado el cálculo del riesgo de todos los activos pertenecientes a la organización, área, o departamento (de acuerdo al alcance definido), se debe determinar cuáles son las amenazas cuyos riesgos son más significativos (Alexander, 2007). Para esta fase se debe utilizar una escala de likert para evaluar los criterios para la importancia del riesgo. Esta etapa contempla tres elementos básicos: estimado del valor de los activos de riesgo, probabilidad de ocurrencia del riesgo y valoración de los riesgos de los activos (Vidalina, 2009).

(a) Estimado del valor de los activos de riesgos: este punto es fundamental para evaluar el riesgo. El objetivo es determinar el daño económico que el riesgo pudiera causar a los activos evaluados. Esto puede llevar a cabo dándole un valor monetario a cada activo de acuerdo al valor de referencia en el mercado y de su importancia para la Universidad.

(b) Probabilidad de ocurrencia del riesgo: se debe representar por cada activo sus impactos, amenazas y posibilidad de ocurrencia, así como las vulnerabilidades y su posibilidad de ser explotadas, determinándose la posibilidad de ocurrencia del riesgo por cada activo de información.

(c) Valoración del riesgo de los activos: por último, se debe llevar a cabo la valoración del riesgo de los activos.

Fase V: Tratamiento.

Ya realizado el análisis y evaluación de los riegos, se debe iniciar el proceso de toma de decisión, donde se debe decidir qué acciones se tomarán en los activos que están sujetos a riesgos.

> La gestión de esos riesgos implica seleccionar e implantar las medidas técnicas y organizativas necesarias para impedir, reducir o controlar los riesgos identificados, de forma que los perjuicios que puedan causar se eliminen o, si esto no es posible, se reduzcan lo máximo posible (INTECO, 2010, p.63).

La norma ISO/IEC 27002:2005, establece que las posibles opciones de tratamiento del riesgo incluye:

- Aplicar controles apropiados para reducir los riesgos.
- Aceptar los riesgos consciente y objetivamente, siempre que cumplan claramente con la política y el criterio de aceptación de la organización.
- Evitar los riesgos no permitiendo acciones que podrían causar que el riesgo ocurra
- Transferir los riesgos asociados a otros grupos; por ejemplo aseguradoras.

En este proceso de toma de decisiones para los activos que se decidan mitigar (o reducir), se debe escoger los controles de acuerdo a la norma ISO/IEC 27001:2005, Anexo A (ver Anexo H).

Fase VI: Monitoreo y Revisión:

Esta fase consiste en monitorear y revisar el desempeño del proceso de gestión de riesgo y los procesos que pueden afectarlos.

Esta etapa se encuentra involucrada en todo el proceso de gestión, ya que consiste en revisar continuamente y en cada etapa si los criterios utilizados para valorar y tratar los riesgos son pertinentes y adecuados para el contexto establecido durante el proceso de gestión del riesgo de seguridad de la información.

Fase VII: Comunicar y Consultar

Esta fase consiste en intercambiar y compartir la información obtenida del proceso de gestión de riesgos entre todas las partes involucradas en el proceso de gestión. Es importante que los administradores de la red comuniquen la información de los riesgos obtenidos, al personal gerencial de la dirección de telecomunicaciones y a todas las otras partes que pudiesen estar involucradas en el proceso de gestión. De acuerdo a la norma ISO 27005:

> "la comunicación del riesgo es una actividad para lograr acuerdo sobre la manera de gestionar los riesgos al intercambiar y compartir los riesgos entre quienes toman decisiones y las otras partes involucradas. La información incluye, pero no se limita a la existencia, naturaleza, forma, probabilidad, gravedad, tratamiento y aceptabilidad de los riesgos" (p.27).

En consecuencia, se deben desarrollar planes de comunicación de los riesgos para las operaciones normales de la RedUCLA así como para las situaciones de emergencia que se pudiesen presentar.

Para el cumplimiento de las etapas se propone el siguiente cronograma:

Cuadro 9

Cronograma a seguir en las etapas de gestión de riesgos de seguridad de la información.

Fases	Descripción	Actividad	Trimestre					Responsables
			1	2	3	4	5	
I	Determinación del Contexto	Definir: Alcance Objetivos Metodologías						Director de telecomunicaciones y jefes de unidades
II	Identificación de los riesgos	Identificar: Activos Amenazas Vulnerabilidades						Jefes de unidades y administradores de la red
III	Análisis de los riesgos	Valorar: Activos Amenazas Vulnerabilidades						Jefes de unidades y administradores de la red
IV	Evaluación de los riesgos	Calculo del riesgo Decidir tratamiento						Jefes de unidades y administradores de la red
V	Tratamiento de los riesgos	Tratar: Mitigar Asumir Transferir Eliminar						Jefes de unidades y administradores de la red
VI	Monitoreo y Evaluación	Monitorear y evaluar el proceso						Director de telecomunicaciones y jefes de unidades.
VII	Comunicación y consulta	Comunicar la información de los riesgos						Director de telecomunicaciones y jefes de unidades.

Fuente: Gil (2011)

Las fases anteriormente detalladas representan la Sistematización de la Gestión de Riesgos de Seguridad de la Información en la Red de la Universidad Centroccidental “Lisandro Alvarado, las cuales puede visualizarse en el gráfico No. 23, que a continuación se presenta:

Gráfico 23. Proceso de Gestión de riesgos de seguridad de la información
Fuente: Gil (2011)

BIBLIOGRAFÍA

Arias, F. (1999). El proyecto de Investigación. Guía para su elaboración. Caracas: Episteme.

Alexander, A. (2007). Diseño de un Sistema de Seguridad de la Información. Óptica ISO 27001:2005. Alfaomega Colombia S.A. Bogotá Colombia.

Alvarado, H. (1999). Sistemas y procedimientos en las organizaciones. Universidad Centroccidental "Lisandro Alvarado. [En línea]. URL: http://bibcyt.ucla.edu.ve/edocs_bciucla/hernan_alvarado/SYPORG.pdf (Consulta: Noviembre 2010)

Balestrini, M. (2006). Cómo se elabora el Proyecto de Investigación en Venezuela. BL Consultores Asociados, Servicio Editorial. Caracas Venezuela.

Camacaro, M. (2009). Seguridad Informática. Guía de Estudio. Cátedra Auditoria Informática. Universidad Centroccidental "Lisandro Alvarado.

Cao, J (2004). Análisis y gestión de riesgos de la seguridad de los sistemas de la información. [En línea]. URL: http://www.cii-murcia.es/informas/abr05/articulos/Analisis_gestion_riesgos_seguridad_sistemas_informacion.pdf (Consulta: Enero 2010)

Coordinación de Emergencias en Redes Teleinformáticas de la Administración Pública Argentina (ArCERT). (2009). Manual de Seguridad en redes [En línea]. URL: http://www.arcert.gov.ar/ncursos/ssi-2009.html. (Consulta: Enero 2010)

Colobran M., Arqués M. y Galindo E. (2008). Administración de Sistemas Operativos en Red, Editorial UOC. Barcelona España.

Consejo Superior de Administración Electrónica (CSAE) (2010). Gobierno de España URL: http://www.csi.map.es/csi/pg5m20.htm (Consulta: Marzo 2010)

De Freitas, V. (2009). Análisis y evaluación del riesgo de la información: caso de estudio Universidad Simón Bolívar. Revista Venezolana de Información, Tecnología y Conocimiento, 6 (1), 43-55. URL: http://www.revistaespacios.com/a10v31n01/10310151.html (Consulta: Enero 2011)

De Freitas, V. (2010). Propuesta de Metodología de Gestión de Seguridad de las TIC's para el Sector Universitario Venezolano. Revista Espacios [Revista en Línea]. Vol. 31 URL: http://www.revistaespacios.com/a10v31n01/10310151.html (Consulta: Abril 2010)

Del Peso E. (2003). Manual de Outsourcing infroamatico. 2da ed. Ediciones Diaz del Santo. [Libro en Línea] URL: http://books.google.com/bkshp?hl=es&tab=pp. (Consulta: Abril 2010)

Donado, S., Agredo, G., Carrascal, C. (2002) Políticas de seguridad Computacional. Facultad de Ingeniería Electrónica y Telecomunicaciones. Universidad de Cauca – Colombia. URL: http://www.criptored.upm.es/guiateoria/gt_m124c.htm. (Consulta: mayo 2010)

Erb, M. (2008). Gestión de Riesgo en la Seguridad Informática. [Blog en Línea]. URL: http://protejete.wordpress.com/about/ (Consulta: Diciembre 2010)

Espineira, Sheldon y Asociados. (2005). Seguridad de la información: un nuevo enfoque para el control de riesgos de negocio. Articulo. [En línea]. URL: www.pc-news.com/detalles.asp?sid=&id=11&lda=1926. (Consulta: Octubre 2009)

Espineira, Sheldon y Asociados. (2008). Practicas de seguridad Informática de las Empresas en Venezuela. Encuesta Nacional 2007-2008. Articulo. [En línea]. URL: http://www.pwc.com/es_VE/ve/encuestas/assets/si-2008.pdf. (Consulta: Diciembre 2009)

Hernández, R., Fernández, C. y Baptista, P. (2003). Metodología de la Investigación. 3ra. Edic. McGraw-Hill/Interamericana Editores. México.

Instituto Nacional de Tecnologías de la Comunicación (INTECO). (2010). Manual Curso de Sistemas de gestión de la seguridad de la información según la norma UNE ISO IEC 27001 [En línea]. URL: https://formacion-online.inteco.es/index.php. (Consulta: Mayo 2010)

Integrity IT (2011). Servicios de Consultoría y Auditoria TIC de Abstrac System. Auditoría de Seguridad basada en las Normas ISO27001 e ISO27002 [En Línea]. URL: http://integrity.abast.es/iso27001_iso27002.shtml (consulta: Abril 2001)

ISO/IEC 17799:2005 – Tecnología de la Información – Técnicas de seguridad – Código para la práctica de la gestión de la seguridad de la información Organización Internacional de Estándares (ISO).

ISO/IEC 27001:2005 – Tecnología de la Información – Técnicas de seguridad – Sistemas de gestión de seguridad de la información – Requerimientos. Organización Internacional de Estándares (ISO).

ISO/IEC 27002:2007 - Tecnología de la información - Técnicas de Seguridad - Código de práctica para la gestión de la seguridad de la información

ISO/IEC 27005:2008 – Tecnología de la Información – Técnicas de seguridad – Gestión del riesgo en la seguridad de la información – Requerimientos. Organización Internacional de Estándares (ISO).

Ley Especial Contra Delitos Informáticos promulgada en Gaceta Oficial Nº 37.313 de fecha 30 de octubre de 2.001 por la Asamblea Nacional, Caracas Venezuela.

Ley Orgánica de Telecomunicaciones, promulgada 12 de junio de 2000 y publicada en Gaceta Oficial No.36.970. Caracas Venezuela.

Ley Orgánica de Ciencia, Tecnología e Innovación, Promulgada en Gaceta Oficial N° 38.242 de fecha 03 de Agosto de 2005. Caracas Venezuela.

Ley Sobre Mensajes de Datos y Firmas Electrónicas promulgada en Gaceta Oficial N° 37.148 de fecha 28 de febrero de 2.001, por Decreto N° 1.024 – 10 de febrero de 2001, Caracas Venezuela.

Maiwald, E. (2003) Fundamentos de Seguridad de Redes. 2da. Edición. Mc.Graw Hill. México D.F. México.

Matalobos, J. (2009). "Análisis de Riesgos de Seguridad de la Información". [En línea]. URL: http://oa.upm.es/1646/1/PFC_JUAN_MANUEL_MATALOBOS_VEIGAa.pdf. Trabajo de Grado. Universidad Politécnica de Madrid, facultad de Informática. Madrid – España. (Consulta: Diciembre de 2009)

Mendoza, R. (2010). Sistema de Gestión para la Seguridad de la Información. Caso Centro de Tecnología de la Información y Comunicación del Decanato de Ciencias y Tecnología (CTIC) – UCLA. Trabajo de Grado. Universidad Centroccidental "Lisandro Alvarado". Barquisimeto.

Mujica, M. (2007). Diseño de un Plan de Seguridad Informática para la Universidad Nacional Experimental "Antonio José de Sucre" Sede Rectoral. Trabajo de Grado. Universidad Centroccidental "Lisandro Alvarado". Barquisimeto.

Oz. E. (2001). Administración de sistemas de Información, 2da ed. Editorial Thomson Learning DF. México.

O'Brien. J. (2001). Sistemas de Información Gerencial, 4ta ed. Editorial Mc-Graw Hill. Colombia.

Piattini M y Del Peso E. (2001). Auditoria Informática. Un enfoque práctico, 2da ed. Editorial Alfaomega. México.

Ramio, J. (2006). Libro Electrónico de Seguridad Informática. Versión 4.1. Universidad Politécnica de Madrid. [En línea] URL: http://www.criptored.upm.es/guiateoria/gt_m001a.htm. (Consulta: Abril 2010)

Resolución de Consejo Universitario No. 1647. Normas de Seguridad Informática y de Telecomunicaciones de la Universidad Centroccidental "Lisandro Alvarado" aprobado el 21 de septiembre del 2.005. Barquisimeto.

Sabino, C. (2002). El proceso de Investigación. Editorial Panapo de Venezuela. Caracas.

Sena, L., Tenzer, S. (2004). Introducción a los Riesgos Informáticos. Cátedra de Introducción a la Computación. Faculta de Ciencias Económicas y de Administración Universidad de la Republica, Uruguay. URL: http://www.ccee.edu.uy/ensenian/catcomp/material/Inform_%20II/riesgoinf8.pdf. (Consulta Enero 2010)

Serrera, P. (2010). Seguridad LOPD a través de un SGSI. Madrid: "Opinión de los expertos" Revista digital Datospersonales.org. Madrid: APDCM, 27 de Enero de 2011, Número 49.http://www.madrid.org/comun/datospersonales/0,3126,457237_0_127535941_12151300_12145900,00.html>. (Consulta Febrero de 2011).

SYMANTEC (2010). Estudio de Symantec sobre el estado de la seguridad empresarial 2010. [Articulo en Línea] URL: http://www.symantec.com/es/mx/about/news/release/article.jsp?prid=20100224_01 (Consulta febrero 2010)

Tamayo y Tamayo, M. (2005). El proceso de la Investigación Científica, 4ta ed. Editorial Limusa. México.

Tersek, Y. (2008). "Sistema de Gestión de Seguridad de la Información para un Sistema de Información (Caso Sistema Administrativo Integrado S.A.I) en la Red de datos de la UNEXPO-Puerto Ordaz)". Trabajo de grado. Universidad Centroccidental "Lisandro Alvarado. Barquisimeto.

Universidad Metropolitana de Caracas (UNIMET). (s.f). Guía de estudio: Seguridad Informática. [En línea] URL: ares.unimet.edu.ve/programacion/fgpr01/material/seguridadinformatica.ppt. (Consulta enero 2010)

Universidad Centroccidental "Lisandro Alvarado" (UCLA). (2002). Manual para la Elaboración del Trabajo Conducente a Grado Académico de Especialización, Maestría y Doctorado. Barquisimeto.

Universidad Centroccidental "Lisandro Alvarado" (UCLA). (2009). Revista 47 aniversario. Barquisimeto. [En línea] URL: http://issuu.com/ucla/docs/ucla_47anos. (Consulta febrero 2010)

Villasmil, F (2007). "Análisis de los Riesgos de Seguridad Informática para la Pequeñas y Medianas Empresas (PYMES), Usando el Estándar ISO-17799. Para la definición de políticas de seguridad que protejan sus sistemas de información. Trabajo de grado. Universidad Centroccidental "Lisandro Alvarado". Barquisimeto.

ANEXOS

[Anexo A]

RESUMEN CURRICULAR

Raúl José Gil Fernández
INGENIERO EN INFORMÁTICA

FORMACIÓN ACADÉMICA:

T.S.U. Especialista en Tecnología de Información y Comunicaciones
(Actualmente pendiente aprobación y defensa de Trabajo Especial de Grado)
Universidad Centroccidental Lisandro Alvarado (2008 - Actualidad)
Barquisimeto, Edo. Lara.

Ingeniero en Informática
Universidad Centroccidental Lisandro Alvarado (2009)
Decanato de Ciencias y Tecnología
Barquisimeto, Edo. Lara.

Analista de Sistemas
Universidad Centroccidental Lisandro Alvarado (2003)
Decanato de Ciencias y Tecnología
Barquisimeto, Edo. Lara.

CURSOS, TALLERES Y SEMINARIOS

Programa Cisco CCNA (Aprobado 4 Módulos), Cedei, Colégio Universitário "Fermín Toro" (320h). Barquisimeto – Edo. Lara (2008)

Taller instalación Avanzada y Entonación Servidores en Debían GNU/LINUX, Academia de Software Libre, FUNDACITE Lara (20h). (2008)

Taller Básico de Desarrollo de Aplicaciones Web con PHP y mySQL, Colegio Universitario "Fermín Toro. (18h.). Barquisimeto – Edo. Lara (2007)

Curso Básico de Ingles Fundación Universidad de Carabobo. (340h.). Barquisimeto – Edo. Lara (2006)

Curso Básico de Gerencia, Instituto de Formación Gerencial. (60h.). Barquisimeto – Edo. Lara (2005)

Administración de Redes, UCLA. (24h.) Barquisimeto Edo. Lara (2004)

EXPERIENCIA PROFESIONAL

Ingeniero de Operaciones
Corporación Telemic, C.A. (INTER) (Desde Julio 2009)
Barquisimeto, Edo. Lara.

Ayudantías de Servicio
Dirección de Telecomunicaciones, Universidad Centroccidental Lisandro Alvarado (Desde Octubre 2008 - Junio 2009)
Barquisimeto, Edo. Lara.

Proyeccionista
Inversiones Maydar, C.A. (CINEX) (Desde Noviembre 2004 – Marzo 2007)
Barquisimeto, Edo. Lara.
Soporte Técnico
Simecca, C.A. (Desde Octubre 2003 – Octubre 2004)
Guanare, Edo. Portuguesa.
Pasante
Policía Municipal de Barinas. (Desde Julio 2003 – Agosto 2003)
Barinas, Edo. Barinas.

[Anexo B]

Instrumento "A" (Entrevista para el Director y Jefes de Unidades de la Dirección de Telecomunicaciones)

UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGIAS
COORDINACION DE POSTGRADO

Estimado(a):

_____

La presente tiene como finalidad conocer su opinión sobre la Gestión de Riesgos de Seguridad Informática en la Red de la Universidad Centroccidental "Lisandro Alvarado" como parte de un estudio para la realización del trabajo de grado titulado **SISTEMATIZACIÓN DE LA GESTIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN EN LA RED DE LA UNIVERSIDAD CENTROCCIDENTAL "LISANDRO ALVARADO"**

La información que usted aporte será de estricta confidencialidad para el investigador del presente estudio y solo será utilizada para los objetivos que en él se proponen, por ello no es necesario su identificación y firma.

Se agradece de antemano su colaboración.

Preguntas

1. ¿Cuáles políticas de seguridad se han definido para la red de la UCLA? ¿Las mismas están basada en estándares internacionales de seguridad de la información?
2. ¿El documento de políticas de seguridad contiene aspectos para la regulación de la gestión del riesgo de seguridad informática? Explique su respuesta
3. ¿Qué controles han sido implementados en la red para mantener la seguridad de los sistemas y aplicaciones, incluyendo la información en tránsito?

4. ¿Existen planes de contingencia ante situaciones de desastres que puedan afectar los activos de la información?
5. ¿Qué tan concientizados están los usuarios en cuanto a los riesgos a los que están expuestos sus sistemas de información?
6. ¿Cuáles son los riesgos a nivel de seguridad de la información si la red fallara?
7. ¿Se han realizado evaluaciones de riesgos de seguridad de la información en la Red de la Universidad? Explique sus resultados de ser afirmativo.
8. ¿Se han realizado auditorias informática a la Red de la Universidad? ¿Indique de qué tipo?
9. ¿Se ejecutan pruebas a las aplicaciones o software desarrollados, para verificar que estén cumpliendo con los requisitos de seguridad definidos por la dirección? ¿De qué tipo?
10. ¿Se realizan pruebas de intrusión a la infraestructura tecnológica para detectar posibles vulnerabilidades y accesos a sistemas por usuarios no autorizados? ¿Cuáles?

[Anexo C]

Instrumento "B" (Entrevista para profesores expertos en seguridad de la información)

UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGIAS
COORDINACION DE POSTGRADO

Estimado Profesor(a):

_____

La presente tiene como finalidad Identificar los componentes para diseñar el proceso para la sistematización de la gestión de riesgos de seguridad Informática en la red de la Universidad Centroccidental "Lisandro Alvarado" como parte de un estudio para la realización del trabajo de grado titulado **SISTEMATIZACIÓN DE LA GESTIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN EN LA RED DE LA UNIVERSIDAD CENTROCCIDENTAL "LISANDRO ALVARADO"**

La información que usted aporte será de estricta confidencialidad para el investigador del presente estudio y solo será utilizada para los objetivos que en él se proponen, por ello no es necesario su identificación y firma.

Se agradece de antemano su colaboración.

Preguntas

1. ¿Conoce usted el estándar ISO 27001:2005 Sistemas de Gestión de Seguridad de la Información?
2. ¿Qué aspectos se deben contemplar al efectuar el proceso de análisis riesgos de seguridad de la información?
3. ¿Qué metodología considera apropiada para el Análisis de riesgos de seguridad de la información? Indique por qué

4. ¿Qué estrategias se pueden considerar para el tratamiento o reducción de los riesgos?
5. Según su opinión, ¿cuáles considera son las principales vulnerabilidades que presenta en la RedUCLA?
6. Según su opinión, ¿cuáles considera son las principales amenazas que presenta en la RedUCLA?
7. ¿Cómo experto en el área, indique como se puede mejorar su seguridad con un enfoque para la gestión de riesgos de seguridad de la información?

[Anexo D]

Instrumento "C" (Cuestionario para el Personal de Telecomunicaciones)

UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGIAS
COORDINACION DE POSTGRADO

La presente tiene como finalidad conocer su opinión sobre la Gestión de Riesgos de Seguridad Informática en la Red de la Universidad Centroccidental "Lisandro Alvarado" como parte de un estudio para la realización del trabajo de grado titulado **SISTEMATIZACIÓN DE LA GESTIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN EN LA RED DE LA UNIVERSIDAD CENTROCCIDENTAL "LISANDRO ALVARADO" (REDUCLA)**

INSTRUMENTOS DE RECOLECCION DE DATOS

1. Lea cuidadosamente cada uno de los planteamientos.
2. Marque en el espacio correspondiente, la alternativa que más se ajuste a su criterio y a lo que usted considere que ocurre en la Universidad.
5. Todas las preguntas deben ser respondidas
6. La información que usted aporte será de estricta confidencialidad para el investigador del presente estudio y solo será utilizada para los objetivos que en él se proponen, por ello no es necesario su identificación y firma.

Se agradece de antemano su colaboración.

1. ¿La Universidad cuenta con políticas de seguridad de la información formalmente documentada y aprobada por el consejo universitario?
   ☐ SI ☐ NO
2. ¿Dichas políticas contienen aspectos para la regulación de la gestión del riesgo de seguridad informática?
   ☐ SI ☐ NO

3. ¿Las políticas son del conocimiento de todo los usuarios de la red?

   ☐ SI ☐ NO

4. ¿Las políticas han sido diseñadas con base a la norma ISO 27001?

   ☐ SI ☐ NO

5. ¿Con que frecuencia se realizan inventarios de los equipos de comunicación asociados a la RedUCLA?

   ☐ Anual ☐ Semestral ☐ Eventual ☐ Nunca

6. ¿Existen reglas para el control de uso aceptable de los activos de la información?

   ☐ SI ☐ NO

7. ¿Existen planes de contingencia ante situaciones de desastres que puedan afectar los activos de la información?

   ☐ SI ☐ NO

8. ¿Existen controles para mitigar el riesgo?

   ☐ SI ☐ NO

9. Señale con una "X", la existencia de mecanismos de protección para minimizar el riesgo de amenazas al área de comunicaciones contra:

• **Incendios**	
• **Inundaciones**	
• **Terremotos**	
• **Disturbios Civiles**	
• **Caídas de energía**	
• **Daños humanos**	

10. Señale con una "X", Los mecanismos de protección contra amenazas que han sido implantados para el área de comunicaciones :

• **Extintores**	
• **Alarmas contra incendio**	
• **Generador de respaldo o UPS**	

• **Aire acondicionados**	
• **Circuito Cerrado de TV**	
• **Habitaciones Cerradas**	

11. ¿Las situaciones de contingencias son documentadas y notificadas oportunamente?

☐ SI ☐ NO

12. ¿Señale cual es la frecuencia de los siguientes incidentes en la red de la UCLA?

	Siempre	**Casi Siempre**	**Algunas Veces**	**Casi Nunca**	**Nunca**
1. Infección por Virus informático					
2. Acceso no autorizado					
3. Sustracción de información por terceros					
4. Perdida de información por accidente					
5. Negación de servicio					

13. ¿Señale con una X, el grado de afectación de las siguientes vulnerabilidades en la red de la UCLA?:

Vulnerabilidades	**Bajo**	**Medio**	**Alto**
1. Carencia de conciencia en seguridad			
2. Ausencia de mecanismos de monitoreo			
3. Falta de protección de los equipos			
4. Inadecuado control de cambio			
5. Inadecuada gestión de la red			
6. Falta de políticas para el uso de las telecomunicaciones			

14. ¿Existen mecanismos para la protección de la red contra códigos maliciosos?

☐ SI ☐ NO

15. ¿Los usuarios de la red tienen acceso solo a los servicios para los cuales han sido autorizados?

☐ SI ☐ NO

16. ¿Existen planes de mantenimiento preventivo de la infraestructura de hardware asociados a la RedUCLA?

☐ SI ☐ NO

17. ¿Existen planes de mantenimiento preventivo de la infraestructura de Software asociados a la RedUCLA?

☐ SI ☐ NO

18. ¿Se realizan proyecciones de los requerimientos de los sistemas a ser implementados dentro de la RedUCLA en cuanto a la capacidad, seguridad y desempeño requerido?

☐ SI ☐ NO

19. ¿Para lo siguiente activos, valore el nivel de afectación de la perdida de la Integridad?

Activo de Información	**1** **Muy bajo**	**2** **Bajo**	**3** **Medio**	**4** **Alto**	**5** **Muy Alto**
1. Base de datos					
2. Servidor de base de datos					
3. Servidor DNS					
4. Servidor Proxy					
5. Servidor de correo					
6. Servidor Web					
7. Switches					
8. Router					
9. Firewall					
10. Red de comunicación					
11. Telefonía					

20. ¿Para lo siguiente activos, valore el nivel de afectación de la perdida de la Confidencialidad?

Activo de Información	1	2	3	4	5
	Muy bajo	Bajo	Medio	Alto	Muy Alto
1. Base de datos					
2. Servidor de base de datos					
3. Servidor DNS					
4. Servidor Proxy					
5. Servidor de correo					
6. Servidor Web					
7. Switches					
8. Router					
9. Firewall					
10. Red de comunicación					
11. Telefonía					

21. ¿Para lo siguiente activos, valore el nivel de afectación de la perdida de la Disponibilidad?

Activo de Información	1	2	3	4	5
	Muy bajo	Bajo	Medio	Alto	Muy Alto
1. Base de datos					
2. Servidor de base de datos					
3. Servidor DNS					
4. Servidor Proxy					
5. Servidor de correo					
6. Servidor Web					
7. Switches					
8. Router					
9. Firewall					
10. Red de comunicación					
11. Telefonía					

[Anexo E]

Formato de la Validación del Instrumento

UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGIAS
COORDINACION DE POSTGRADO

Estimado Profesor(a):

_____

Presente.

Por medio de la presente, me dirijo a usted, como experto en el área con el propósito de validar los instrumentos a utilizar en el desarrollo de la investigación, la cual se titula: "**Sistematización de la Gestión de Riesgos de la Seguridad la Información en la Red de la Universidad Centroccidental "Lisandro Alvarado".** La información recolectada servirá de insumo para el trabajo de grado para la "Especialización en Tecnologías de Información y Comunicación", cursada en esta Universidad.

A tal fin, se anexa cuadro de operacionalización de variables, los instrumentos de recolección de datos (Cuestionario y Entrevistas) y el respectivo formato de revisión y validación, además de objetivo general y los objetivos específicos de la investigación.

Se debe resaltar, en cuanto a la investigación, que la misma es una investigación de campo, de caráter no experimental, descriptiva.

Sin más a que hacer referencia y agradeciendo su mayor colaboración al respecto,

_____

Atentamente,
Raúl Gil

OBJETIVOS DE LA INVESTIGACIÓN

Objetivo General

Sistematizar la Gestión de Riesgos de Seguridad de la Información en la Red de la Universidad Centroccidental “Lisandro Alvarado”

Objetivos Específicos

1. Diagnosticar el proceso actual de la Gestión de Riesgos de la Seguridad de la Información en la Red de la Universidad Centroccidentral “Lisandro Alvarado”

2. Identificar los componentes para diseñar el proceso para la Sistematización de la Gestión de Riesgos de la Seguridad de la Información en la Red de la Universidad Centroccidental “Lisandro Alvarado”

3. Presentar el diseño del proceso para la Sistematización de la Gestión de Riesgos de la Seguridad de la Información en la Red de la Universidad Centroccidental “Lisandro Alvarado”

Operacionalización de las Variables

Variable	Dimensión	Indicador	Instrumentos			Fuente
			A	B	C	
			Ítems			
Sistematización de la Gestión de Riesgos de la Seguridad de la Información en la Red de la Universidad Centroccidental "Lisandro Alvarado	**Gestión de Riesgos:** Actividades coordinadas para dirigir y controlar una organización con relación al riesgo.	**1. Políticas de Seguridad**	1,2, 3,4	1,2, 8	1	Personal de la Dirección de Telecomunicaciones y Profesores expertos en el área de seguridad de la Información del Decanato de Ciencias y Tecnologías de la UCLA
		2. Gestión de Activos	5,6, 7, 8	4	2,3,4	
		3. Amenazas	9, 10 11, 12	5	5	
		4. Vulnerabilidades	13, 16 17	3,6, 7,9, 10	6,7	
	Seguridad de la información: Protección de la confidencialidad, integridad y disponibilidad de los activos de información según sea necesario para alcanzar los objetivos de negocio de la organización.	**5. Integridad**	14,19			Personal de la Dirección de Telecomunicaciones
		6. Confidencialidad	15, 20			
		7. Disponibilidad	18, 21	3, 9		

UNIVERSIDAD CENTROCCIDENTAL
"LISANDRO ALVARADO"
DECANATO DE CIENCIAS Y TECNOLOGIA
COORDINACION DE POSTGRADO

Formato para la Revisión y Validación del Instrumento de Recolección de Datos

Nombres y Apellidos:_____

Título que posee:_____

Especialidad de Postgrado:_____

Cargo que Desempeña: _____

Instrucciones:

1. Lea detenidamente cada uno de los ítems relacionados con cada indicador.
2. Indique con una equis (X) en el espacio correspondiente al aspecto cualitativo que considere cumple cada ítem.
3. En la casilla de observaciones puede sugerir cualquier mejora al instrumento.

Validación del Instrumento "A" (Entrevista para el Director y Jefes de Unidades de la Dirección de Telecomunicaciones)

Ítems	CRITERIO						Observaciones
	Redacción		Claridad		Pertinencia		
	Si	No	Si	No	Si	No	
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							

Fecha: _____ Firma:_____

Validación del Instrumento "B" (Entrevista para profesores expertos en seguridad de la información)

Ítems	CRITERIO						Observaciones
	Redacción		Claridad		Pertinencia		
	Si	No	Si	No	Si	No	
1							
2							
3							
4							
5							
6							
7							

Fecha: _____ Firma:_____

Validación del Instrumento "C" (Cuestionario para el Personal de Telecomunicaciones)

Ítems	CRITERIO						Observaciones
	Redacción		Claridad		Pertinencia		
	Si	No	Si	No	Si	No	
1							
2							
3							
4							
5							
6							
7							
8							
9							
10							
11							
12							
13							
14							
15							
16							
17							
18							
19							
20							
21							

Fecha: ____ Firma:_____

[Anexo F]

ANALISIS DE CONFIABILIDAD DEL INSTRUMENTO C

Preguntas dicotómicas por formula de Kuder Richardson (kr20)

Estadísticos descriptivos

	N	Varianza
COMPUTE Suma=P.1+P.2+P.3+P.4+P.6+P.7+P.8+P.11+P.14+P.15+P.16+P.17+P.18	7	6,810
N válido (según lista)	7	

sujetos	P.1	P.2	P.3	P.4	P.6	P.7	P.8	P.11	P.14	P.15	P.16	P.17	P.18	Total
1	1	1	1	0	1	0	0	0	0	1	1	1	0	7
2	1	0	0	0	0	0	0	1	0	1	1	1	0	5
3	1	1	1	1	1	1	1	1	0	1	1	1	1	12
4	1	0	0	1	0	1	0	0	1	1	1	1	0	7
5	1	1	1	1	1	1	1	0	1	1	1	1	0	11
6	1	1	0	0	0	0	0	1	0	1	1	1	0	6
7	1	1	0	0	1	0	1	0	0	1	1	1	0	7
	7	5	3	3	4	3	3	3	2	7	7	7	1	Vt = 6,81
P	1	0,71	0,43	0,429	0,57	0,429	0,43	0,43	0,29	1	1	1	0,143	
q(1-p)	0	0,29	0,57	0,571	0,43	0,571	0,57	0,57	0,71	0	0	0	0,857	
Pq	0	0,2	0,24	0,245	0,24	0,245	0,24	0,24	0,2	0	0	0	0,122	∑ = 2

Sustituyendo los valores en la formula tenemos:

$r_{tt} = (K - R_{20}) = \{[7/(7-1)] * [(6.81 - 2)/ 6.81]\} =$ (1,167 * 0,706) = 0,824

$r_{tt} =$ 0,824

[Anexo G]

ANALISIS DE CONFIABILIDAD INSTRUMENTO C

PREGUNTAS DE ESCALA POR COEFICIENTE DE ALPHA CRONBACH

Resumen del procesamiento de los casos

		N	%
Casos	Válidos	7	100,0
	Excluidos[a]	0	,0
	Total	7	100,0

a. Eliminación por lista basada en todas las variables del procedimiento.

Estadísticos de fiabilidad

Alfa de Cronbach	N de elementos
,929	38

Resúmenes Procesamiento de los Casos - Instrumento C

	Casos					
	Incluidos		Excluidos		Total	
	N	Porcentaje	N	Porcentaje	N	Porcentaje
P.12.1	7	100,0%	0	,0%	7	100,0%
P.12.2	7	100,0%	0	,0%	7	100,0%
P.12.3	7	100,0%	0	,0%	7	100,0%
P.12.4	7	100,0%	0	,0%	7	100,0%
P.12.5	7	100,0%	0	,0%	7	100,0%
P.19.1	7	100,0%	0	,0%	7	100,0%
P.19.2	7	100,0%	0	,0%	7	100,0%
P.19.3	7	100,0%	0	,0%	7	100,0%
P.19.4	7	100,0%	0	,0%	7	100,0%
P.19.5	7	100,0%	0	,0%	7	100,0%
P.19.6	7	100,0%	0	,0%	7	100,0%
P.19.7	7	100,0%	0	,0%	7	100,0%
P.19.8	7	100,0%	0	,0%	7	100,0%
P.19.9	7	100,0%	0	,0%	7	100,0%
P.19.10	7	100,0%	0	,0%	7	100,0%
P.19.11	7	100,0%	0	,0%	7	100,0%
P.20.1	7	100,0%	0	,0%	7	100,0%
P.20.2	7	100,0%	0	,0%	7	100,0%
P.20.3	7	100,0%	0	,0%	7	100,0%
P.20.4	7	100,0%	0	,0%	7	100,0%
P.20.5	7	100,0%	0	,0%	7	100,0%
P.20.6	7	100,0%	0	,0%	7	100,0%
P.20.7	7	100,0%	0	,0%	7	100,0%
P.20.8	7	100,0%	0	,0%	7	100,0%
P.20.9	7	100,0%	0	,0%	7	100,0%
P.20.10	7	100,0%	0	,0%	7	100,0%
P.20.11	7	100,0%	0	,0%	7	100,0%
P.21.1	7	100,0%	0	,0%	7	100,0%
P.21.2	7	100,0%	0	,0%	7	100,0%
P.21.3	7	100,0%	0	,0%	7	100,0%
P.21.4	7	100,0%	0	,0%	7	100,0%
P.21.5	7	100,0%	0	,0%	7	100,0%
P.21.6	7	100,0%	0	,0%	7	100,0%
P.21.7	7	100,0%	0	,0%	7	100,0%
P.21.8	7	100,0%	0	,0%	7	100,0%
P.21.9	7	100,0%	0	,0%	7	100,0%
P.21.10	7	100,0%	0	,0%	7	100,0%
P.21.11	7	100,0%	0	,0%	7	100,0%

Resúmenes de casos – Instrumento A

sujetos / Preg.	1	2	3	4	5	6	7	Total N
P.12.1	4	2	2	4	3	3	3	7
P.12.2	2	2	2	2	2	2	1	7
P.12.3	2	2	1	1	2	2	3	7
P.12.4	1	2	2	1	2	2	3	7
P.12.5	2	2	1	3	3	3	4	7
P.19.1	1	5	2	2	5	4	4	7
P.19.2	3	2	2	3	5	3	4	7
P.19.3	1	5	2	4	5	1	4	7
P.19.4	2	4	2	1	3	2	5	7
P.19.5	1	3	2	4	5	3	3	7
P.19.6	4	5	2	3	5	4	3	7
P.19.7	1	4	3	4	3	3	3	7
P.19.8	3	5	3	3	5	5	5	7
P.19.9	1	1	3	4	4	3	5	7
P.19.10	5	3	3	4	5	4	4	7
P.19.11	1	5	2	3	4	3	4	7
P.20.1	1	4	3	4	3	5	5	7
P.20.2	1	5	3	4	3	5	5	7
P.20.3	1	1	2	4	4	5	4	7
P.20.4	1	5	2	3	3	5	4	7
P.20.5	2	2	2	4	4	4	4	7
P.20.6	1	2	2	4	5	5	3	7
P.20.7	3	5	2	4	4	3	4	7

P.20.8	1	3	2	4	1	5	3	7
P.20.9	1	5	2	4	5	2	4	7
P.20.10	5	1	2	4	2	5	5	7
P.20.11	1	3	2	3	5	1	3	7
P.21.1	1	3	2	4	2	1	4	7
P.21.2	4	5	3	4	3	5	3	7
P.21.3	1	2	3	5	4	1	4	7
P.21.4	1	2	3	3	2	1	5	7
P.21.5	1	5	3	5	3	3	3	7
P.21.6	1	4	3	4	1	2	3	7
P.21.7	1	5	3	5	4	1	4	7
P.21.8	1	3	3	1	5	3	1	7
P.21.9	1	5	3	2	3	1	2	7
P.21.10	1	2	4	5	5	4	5	7
P.21.11	1	1	3	4	1	1	3	7

[Anexo H]

Anexo A. Tabla A.1 Objetivos de control y Controles de la Norma ISO 27001:2005 Sistema de Gestión de Seguridad de la Información

A.5 Política de seguridad		
A.5.1 Política de seguridad de información Objetivo de control: Proporcionar dirección gerencial y apoyo a la seguridad de la información en concordancia con los requerimientos comerciales y leyes y regulaciones relevantes		
A.5.1.1	Documentar política de seguridad de información	Control La gerencia debe aprobar un documento de política, este se debe publicar y comunicar a todos los empleados y entidades externas relevantes.
A.5.1.2	Revisión de la política de seguridad de la información	Control La política de seguridad de la información debe ser revisada regularmente a intervalos planeados o si ocurren cambios significativos para asegurar la continua idoneidad, eficiencia y efectividad.
A.6 Organización de la seguridad de la información		
A.6.1 Organización interna Objetivo: Manejar la seguridad de la información dentro de la organización.		
A.6.1.1	Compromiso de la gerencia con la seguridad de la información	Control La gerencia debe apoyar activamente la seguridad dentro de la organización a través de una dirección clara, compromiso demostrado, asignación explícita y reconocimiento de las responsabilidades de la seguridad de la información.
A.6.1.2	Coordinación de la seguridad de información	Control Las actividades de seguridad de la información deben ser coordinadas por representantes de las diferentes partes de la organización con las funciones y roles laborales relevantes.
A.6.1.3	Asignación de responsabilidades de la seguridad de la información	Control Se deben definir claramente las responsabilidades de la seguridad de la información.
A.6.1.4	Proceso de autorización para los medios de procesamiento de información	Control Se debe definir e implementar un proceso de autorización gerencial para los nuevos medios de procesamiento de información
A.6.1.5	Acuerdos de confidencialidad	Control Se deben identificar y revisar regularmente los requerimientos de confidencialidad o los acuerdos de no-divulgación reflejando las necesidades de la organización para la protección de la información.
A.6.1.6	Contacto con autoridades	Control Se debe mantener los contactos apropiados con las autoridades relevantes.
A.6.1.7	Contacto con grupos de interés especial	Control Se deben mantener contactos apropiados con los grupos de interés especial u otros foros de seguridad especializados y asociaciones profesionales.
A.6.1.8	Revisión independiente de la seguridad de la información	Control El enfoque de la organización para manejar la seguridad de la información y su implementación (es decir; objetivos de control, controles, políticas, procesos y procedimientos para la seguridad de la información) se debe revisar independientemente a intervalos planeados, o cuando ocurran cambios significativos para la implementación de la seguridad.
A.6.2 Entidades externas		

Objetivo: Mantener la seguridad de la información de la organización y los medios de procesamiento de información a los cuales entidades externas tienen acceso y procesan; o son comunicados a o manejados por entidades externas.		
A.6.2.1	Identificación de riesgos relacionados con entidades externas	Control Se deben identificar los riesgos que corren la información y los medios de procesamiento de información de la organización y se deben implementar los controles apropiados antes de otorgar acceso.
A.6.2.2	Tratamiento de la seguridad cuando se trabaja con clientes	Control Se deben tratar todos los requerimientos de seguridad identificados antes de otorgar a los clientes acceso a la información o activos de la organización.
A.6.2.3	Tratamiento de la seguridad en contratos con terceras personas	Control Los acuerdos que involucran acceso, procesamiento, comunicación o manejo por parte de terceras personas a la información o los medios de procesamiento de información de la organización; agregar productos o servicios a los medios de procesamiento de la información deben abarcar los requerimientos de seguridad necesarios relevantes.
A.7 Gestión de activos		
A.7.1 *Responsabilidad por los activos* Objetivo*:* Lograr y mantener la protección apropiada de los activos organizacionales.		
A.7.1.1	Inventarios de activos	Control Todos los activos deben estar claramente identificados; y se debe elaborar y mantener un inventario de todos los activos importantes.
A.7.1.2	Propiedad de los activos	Control Toda la información y los activos asociados con los medios de procesamiento de la información deben ser 'propiedad' de una parte designada de la organización.
A.7.1.3	Uso aceptable de los activos	Control Se deben identificar, documentar e implementar las reglas para el uso aceptable de la información y los activos asociados con los medios de procesamiento de la información.
A.7.2 Clasificación de la información Objetivo: Asegurar que a información reciba un nivel de protección apropiado.		
A.7.2.1	Lineamientos de clasificación	Control La información debe ser clasificada en términos de su valor, requerimientos legales, confidencialidad y grado crítico para la organización.
A.7.2.2	Etiquetado y manejo de la información	Control Se debe desarrollar e implementar un apropiado conjunto de procedimientos para etiquetar y manejar la información en concordancia con el esquema de clasificación adoptado por la organización.
A.8 Seguridad de los recursos humanos		
A.8.1 Antes del empleo Objetivo*:* Asegurar que los empleados, contratistas y terceros entiendan sus responsabilidades, y sean adecuados para los roles para los cuales se les considera; y reducir el riesgo de robo, fraude o mal uso de los medios.		
A.8.1.1	Roles y responsabilidades	Control Se deben definir y documentar los roles y responsabilidades de seguridad de los empleados, contratistas y terceros en concordancia con la política de la seguridad de información de la organización.
A.8.1.2	Selección	Control Se deben llevar a cabo chequeos de verificación de antecedentes de todos los candidatos a empleados, contratistas y terceros en concordancia con las leyes, regulaciones y ética relevante, y deben ser proporcionales a los requerimientos comerciales, la clasificación de la información a la cual se va a tener acceso y los riesgos percibidos.
A.8.1.3	Términos y condiciones de empleo	Control Como parte de su obligación contractual; los empleados, contratistas y terceros deben aceptar y firmar los términos y condiciones de su contrato de empleo, el cual debe establecer sus responsabilidades y las de la

		organización para la seguridad de la información.
A.8.2 *Durante el empleo* Objetivo: Asegurar que todos los empleados, contratistas y terceros estén al tanto de las amenazas y inquietudes sobre la seguridad de información, sus responsabilidades y obligaciones, y que estén equipados para apoyar la política de seguridad organizacional en el curso de su trabajo normal, y reducir los riesgos de error humano.		
A.8.2.1	Gestión de responsabilidades	Control La gerencia debe requerir que los empleados, contratistas y terceros apliquen la seguridad en concordancia con las políticas y procedimientos establecidos de la organización.
A.8.2.2	Capacitación y educación en seguridad de la información	Control Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceros, deben recibir el apropiado conocimiento, capacitación y actualizaciones regulares de las políticas y procedimientos organizacionales, conforme sean relevantes para su función laboral.
A.8.2.3	Proceso disciplinario	Control Debe existir un proceso disciplinario formal para los empleados que han cometido una violación en la seguridad.
A.8.3 Terminación o cambio del empleo Objetivo: Asegurar que los empleados, contratistas y terceros salgan de una organización o cambien de empleo de una manera ordenada.		
A.8.3.1	Responsabilidades de terminación	Control Se deben definir y asignar claramente las responsabilidades para realizar la terminación o cambio del empleo.
A.8.3.2	Devolución de activos	Control Todos los empleados, contratistas y terceros deben devolver todos los activos de la organización que estén en su posesión a la terminación de su empleo, contrato o acuerdo.
A.8.3.3	Eliminación de derechos de acceso	Control Los derechos de acceso de todos los empleados, contratistas y terceros a la información y medios de procesamiento de la información deben ser eliminados a la terminación de su empleo, contrato o acuerdo, o se deben ajustar al cambio.
A.9 Seguridad física y ambiental		
A.9.1 *Áreas seguras* Objetivo: Evitar el acceso físico no autorizado, daño e interferencia al local y la información de la organización.		
A.9.1.1	Perímetro de seguridad física	Control Se debe utilizar perímetros de seguridad (barreras tales como paredes y puertas de ingreso controlado o recepcionistas) para proteger áreas que contienen información y medios de procesamiento de información.
A.9.1.2	Controles de entrada físicos	Control Se deben proteger las áreas seguras mediante controles de entrada apropiados para asegurar que sólo se permita acceso al personal autorizado.
A.9.1.3	Seguridad de oficinas, habitaciones y medios	Control Se debe diseñar y aplicar seguridad física en las oficinas, habitaciones y medios.
A.9.1.4	Protección contra amenazas externas y ambientales	Control Se debe diseñar y aplicar protección física contra daño por fuego, inundación, terremoto, explosión, disturbios civiles y otras formas de desastre natural o creado por el hombre.
A.9.1.5	Trabajo en áreas seguras	Control Se debe diseñar y aplicar protección física y lineamientos para trabajar en áreas seguras.
A.9.1.6	Áreas de acceso público, entrega y carga	Control Se deben controlar los puntos de acceso como las áreas de entrega y descarga y otros puntos donde personas no-autorizadas pueden ingresar a los locales, y cuando fuese posible, se deben aislar de los medios de procesamiento de la información para evitar un acceso no autorizado.

A.9.2 *Seguridad del equipo* Objetivo*:* Evitar la pérdida, daño, robo o compromiso de los activos y la interrupción de las actividades de la organización		
A.9.2.1	Ubicación y protección del equipo	Control El equipo debe estar ubicado o protegido para reducir los riesgos de las amenazas y peligros ambientales, y las oportunidades para el acceso no autorizado.
A.9.2.2	Servicios públicos	Control El equipo debe ser protegido de fallas de energía y otras interrupciones causadas por fallas en los servicios públicos.
A.9.2.3	Seguridad en el cableado	Control El cableado de la energía y las telecomunicaciones que llevan data o sostienen los servicios de información deben ser protegidos de la intercepción o daño.
A.9.2.4	Mantenimiento de equipo	Control El equipo debe ser mantenido correctamente para permitir su continua disponibilidad e integridad.
A.9.2.5	Seguridad del equipo fuera-del-local	Control Se debe aplicar seguridad al equipo fuera-del-local tomando en cuenta los diferentes riesgos de trabajar fuera del local de la organización.
A.9.2.6	Eliminación seguro o re-uso del equipo	Control Todos los ítems de equipo que contengan medios de almacenaje deben ser chequeados para asegurar que se haya removido o sobre-escrito de manera segura cualquier data confidencial y software con licencia antes de su eliminación.
A.9.2.7	Traslado de Propiedad	Control Equipos, información o software no deben ser sacados fuera de la propiedad sin previa autorización.
A.10 Gestión de las comunicaciones y operaciones		
A.10.1 Procedimientos y responsabilidades operacionales Objetivo: Asegurar la operación correcta y segura de los medios de procesamiento de la información		
A.10.1.1	Procedimientos de operación documentados	Control Se deben documentar y mantener los procedimientos de operación, y se deben poner a disposición de todos los usuarios que los necesiten.
A.10.1.2	Gestión de cambio	Control Se deben controlar los cambios en los medios y sistemas de procesamiento de la información.
A.10.1.3	Segregación de deberes	Se deben segregar los deberes y áreas de responsabilidad para reducir las oportunidades de una modificación no-autorizada o no-intencionada o un mal uso de los activos de la organización.
A.10.1.4	Separación de los medios de desarrollo y operacionales	Control Se deben separar los medios de desarrollo, prueba y operacionales para reducir los riesgos de accesos no-autorizados o cambios en el sistema de operación.
A.10.2 Gestión de la entrega del servicio de terceros Objetivo: Implementar y mantener el nivel apropiado de seguridad de la información y entrega del servicio en línea con los contratos de entrega del servicio de terceros.		
A.10.2.1	Entrega del servicio	Control Se debe asegurar que los terceros implementen, operen y mantengan los controles de seguridad, definiciones de servicio y niveles de entrega incluidos en el contrato de entrega del servicio de terceros.
A.10.2.2	Monitoreo y revisión de los servicios de terceros	Control Los servicios, reportes y registros provistos por terceros deben ser monitoreados y revisados regularmente, y las auditorías se deben llevar a cabo regularmente.
A.10.2.2	Manejar los cambios en los servicios de terceros	Control Se deben manejar los cambios en la provisión de servicios, incluyendo el mantenimiento y mejoramiento de las políticas, procedimientos y

		controles de seguridad existentes, tomando en cuenta el grado crítico de los sistemas y procesos comerciales involucrados y la reevaluación de los riesgos.
A.10.3 Planeación y aceptación del sistema Objetivo: Minimizar el riesgo de fallas en los sistemas.		
A.10.3.1	Gestión de capacidad	Control Se deben monitorear, afinar y realizar proyecciones del uso de los recursos para asegurar el desempeño del sistema requerido.
A.10.3.2	Aceptación del sistema	Control Se deben establecer los criterios de aceptación para los sistemas de información nuevos, actualizaciones y versiones nuevas y se deben llevar a cabo pruebas adecuadas del(los) sistema(s) durante su desarrollo y antes de su aceptación.
A.10.4 *Protección contra software malicioso y código móvil* Objetivo: Proteger la integridad del software y la información.		
A.10.4.1	Controles contra software malicioso	Control Se deben implementar controles de detección, prevención y recuperación para protegerse de códigos malicioso y se deben implementar procedimientos de conciencia apropiados.
A.10.4.2	Controles contra códigos móviles	Control Cuando se autoriza el uso de un código móvil, a configuración debe asegurar que el código móvil autorizado opere de acuerdo a una política de seguridad claramente definida, y se debe evitar que se ejecute un código móvil no-autorizado
A.10.5 Respaldo (back-up) Objetivo: Mantener la integridad y disponibilidad de los servicios de procesamiento de información y comunicaciones.		
A.10.5.1	Back-up o respaldo de la información	Control Se deben realizar copias de back-up o respaldo de la información comercial y software esencial y se deben probar regularmente de acuerdo a la política.
A.10.6 *Gestión de seguridad de redes* Objetivo: Asegurar la protección de la información en redes y la protección de la infraestructura de soporte.		
A.10.6.1	Controles de red	Control Las redes deben ser adecuadamente manejadas y controladas para poderlas proteger de amenazas, y para mantener la seguridad de los sistemas y aplicaciones utilizando la red, incluyendo la información en tránsito.
A.10.6.2	Seguridad de los servicios de red	Control Se deben identificar los dispositivos de seguridad, niveles de servicio y los requerimientos e incluirlos en cualquier contrato de servicio de red, ya sea que estos servicios sean provistos en-casa o sean abastecidos externamente.
A.10.7 Gestión de medios Objetivo: Evitar la divulgación, modificación, eliminación o destrucción no-autorizada de los activos; y la interrupción de las actividades comerciales.		
A.10.7.1	Gestión de los medios removibles	Control Deben existir procedimientos para la gestión de medios removibles.
A.10.7.2	Eliminación de medios	Control Los medios deben ser eliminados utilizando procedimientos formales y de una manera segura cuando ya no se les requiere.
A.10.7.3	Procedimientos de manejo de la información	Control Se deben establecer los procedimientos para el manejo y almacenaje de la información para proteger dicha información de una divulgación no autorizada o un mal uso.
A.10.8 Intercambio de información Objetivo: Mantener la seguridad de la información y software intercambiados dentro de una organización y con cualquier entidad externa.		

A.10.8.1	Procedimientos y políticas de información y software	Control Se deben establecer política, procedimientos y controles de intercambio formales para proteger el intercambio de información a través del uso de todos los tipos de medios de comunicación.
A.10.8.2	Acuerdos de intercambio	Control Se deben establecer acuerdos para el intercambio de información y software entre la organización y entidades externas.
A.10.8.3	Medios físicos en tránsito	Control Los medios que contienen información deben ser protegidos contra un acceso no-autorizado, mal uso o corrupción durante el transporte más allá de los límites físicos de una organización.
A.10.8.4	Mensajes electrónicos	Control Se debe proteger adecuadamente los mensajes electrónicos.
A.10.8.5	Sistemas de información comercial	Control Se deben desarrollar e implementar políticas y procedimientos para proteger la información asociada con la interconexión de los sistemas de información comercial.
A.10.9 Servicios de comercio electrónico Objetivo: Asegurar la seguridad de los servicios de comercio electrónico y su uso seguro		
A.10.9.1	Comercio electrónico	Control Se debe proteger la información involucrada en el comercio electrónico que se trasmite a través de redes públicas de cualquier actividad fraudulenta, disputa contractual y divulgación y modificación no autorizada.
A.10.9.2	Transacciones en-línea	Control Se debe proteger la información involucrada en las transacciones en-línea para evitar la transmisión incompleta, rutas equivocadas, alteración no-autorizada del mensaje, divulgación no-autorizada, y duplicación o reenvío no-autorizado del mensaje.
A.10.9.3	Información disponible públicamente	Control Se debe proteger la integridad de la información disponible públicamente para evitar la modificación no autorizada.
A.10.10 Monitoreo Objetivo: Detectar actividades de procesamiento de información no autorizadas.		
A.10.10.1	Registro de auditoría	Control Se deben producir registros de las actividades de auditoría, excepciones y eventos de seguridad de la información y se deben mantener durante un período acordado para ayudar en investigaciones futuras y monitorear el control de acceso.
A.10.10.2	Uso del sistema de monitoreo	Control Se deben establecer procedimientos para monitorear el uso de los medios de procesamiento de información y el resultado de las actividades de monitoreo se debe revisar regularmente.
A.10.10.3	Protección de la información del registro	Control Se deben proteger los medios de registro y la información del registro contra alteraciones y acceso no-autorizado.
A.10.10.4	Registros del administrador y operador	Control Se deben registrar las actividades del administrador y operador del sistema.
A.10.10.5	Registro de fallas	Control Las fallas se deben registrar, analizar y se debe tomar la acción apropiada.
A.10.10.6	Sincronización de relojes	Control Los relojes de los sistemas de procesamiento de información relevantes de una organización o dominio de seguridad deben estar sincronizados con una fuente de tiempo exacta acordada.
A.11 Control de acceso		

A.11.1 Requerimiento comercial para el control del acceso Objetivo: Controlar acceso a la información		
A.11.1.1	Política de control de acceso	Control Se debe establecer, documentar y revisar la política de control de acceso en base a los requerimientos de seguridad y comerciales.
A.11.2 Gestión del acceso del usuario Objetivo: Asegurar el acceso del usuario autorizado y evitar el acceso no-autorizado a los sistemas de información.		
A.11.2.1	Inscripción del usuario	Control Debe existir un procedimiento formal para la inscripción y des-inscripción para otorgar acceso a todos los sistemas y servicios de información.
A.11.2.2	Gestión de privilegios	Control Se debe restringir y controlar la asignación y uso de los privilegios.
A.11.2.3	Gestión de la clave del usuario	Control La asignación de claves se debe controlar a través de un proceso de gestión formal.
A.11.2.4	Revisión de los derechos de acceso del usuario	Control La gerencia debe revisar los derechos de acceso de los usuarios a intervalos regulares utilizando un proceso formal.
A.11.3 Responsabilidades del usuario Objetivo: Evitar el acceso de usuarios no autorizados, y el compromiso o robo de la información y los medios de procesamiento de la información.		
A.11.3.1	Uso de clave	Control Se debe requerir que los usuarios sigan buenas prácticas de seguridad en la selección y uso de claves.
A.11.3.2	Equipo de usuario desatendido	Control Se debe requerir que los usuarios se aseguren de dar la protección apropiada al equipo desatendido
A.11.3.3	Política de pantalla y escritorio limpio	Control Se debe adoptar una política de escritorio limpio para los documentos y medios de almacenaje removibles y una política de pantalla limpia para los medios de procesamiento de la información.
A.11.4 Control de acceso a redes Objetivo: Evitar el acceso no-autorizado a los servicios en red.		
A.11.4.1	Política sobre el uso de servicios en red	Control Los usuarios sólo deben tener acceso a los servicios para los cuales han sido específicamente autorizados a usar.
A.11.4.2	Autenticación del usuario para conexiones externas	Control Se debe utilizar métodos de autenticación para controlar el acceso de usuarios remotos.
A.11.4.3	Identificación del equipo en red	Control Se debe considerar la identificación automática del equipo como un medio para autenticar las conexiones desde equipos y ubicaciones específicas.
A.11.4.4	Protección del puerto de diagnóstico remoto	Control Se debe controlar el acceso físico y lógico a los puertos de diagnóstico y configuración.
A.11.4.5	Segregación en redes	Control Los servicios de información, usuarios y sistemas de información se deben segregar en las redes.
A.11.4.6	Control de conexión de redes	Control Se debe restringir la capacidad de conexión de los usuarios en las redes compartidas, especialmente aquellas que se extienden a través de los límites organizaciones, en concordancia con la política de control de acceso y los requerimientos de las aflicciones comerciales (ver 11.1).
A.11.4.7	Control de 'routing' de redes	Control Se deben implementar controles 'routing' para las redes para asegurar

		que las conexiones de cómputo y los flujos de información no infrinjan la política de control de acceso de las aplicaciones comerciales.
A.11.5 Control de acceso al sistema de operación Objetivo: Evitar acceso no autorizado a los sistemas operativos.		
A.11.5.1	Procedimientos de registro en el terminal	Control Se debe controlar el acceso los servicios operativos mediante un procedimiento de registro seguro.
A.11.5.2	Identificación y autenticación del usuario	Control Todos los usuarios deben tener un identificador singular (ID de usuario) para su uso personal y exclusivo, se debe elegir una técnica de autenticación adecuada para verificar la identidad del usuario.
A.11.5.3	Sistema de gestión de claves	Control Los sistemas de manejo de claves deben ser interactivos y deben asegurar la calidad de las claves.
A.11.5.4	Uso de utilidades del sistema	Control Se debe restringir y controlar estrictamente el uso de los programas de utilidad que podrían superar al sistema y los controles de aplicación.
A.11.5.5	Sesión inactiva	Control Las sesiones inactivas deben cerrarse después de un período de inactividad definido.
A.11.5.6	Limitación de tiempo de conexión	Control Se debe utilizar restricciones sobre los tiempos de conexión para proporcionar seguridad adicional a las aplicaciones de alto riesgo.
A.11.6 Control de acceso a la aplicación e información Objetivo: Evitar el acceso no autorizado a la información mantenida en los sistemas de aplicación.		
A.11.6.1	Restricción al acceso a la información	Control Se debe restringir el acceso de los usuarios y personal de soporte al sistema de información y aplicación en concordancia con la política de control de acceso definida.
A.11.6.2	Aislamiento del sistema sensible	Control Los sistemas sensibles deben tener un ambiente de cómputo dedicado (aislado).
A.11.7 Computación móvil y teletrabajo Objetivo: Asegurar la seguridad de la información cuando se utilice medios computación móvil y teletrabajo.		
A.11.7.1	Computación móvil y comunicaciones	Control Se debe establecer una política formal y adoptar las medidas de seguridad apropiadas para proteger contra los riesgos de utilizar medios de computación y comunicación móviles.
A.11.7.2	Tele-trabajo	Control Se deben desarrollar e implementar políticas, planes operacionales y procedimientos para actividades de tele-trabajo.
A.12 Adquisición, desarrollo y mantenimiento de los sistemas de información		
A.12.1 Requerimientos de seguridad de los sistemas Objetivo: Asegurar que la seguridad sea una parte integral de los sistemas de información.		
A.12.1.1	Análisis y especificación de los requerimientos de seguridad	Control Los enunciados de los requerimientos comerciales para sistemas nuevos, o mejorar los sistemas existentes deben especificar los requerimientos de los controles de seguridad.
A.12.2 Procesamiento correcto en las aplicaciones Objetivo: Evitar errores, pérdida, modificación no-autorizada o mal uso de la información en las aplicaciones.		
A.12.2.1	Validación de data de Insumo	Control El Insumo de data en las aplicaciones debe ser validado para asegurar que esta data sea correcta y apropiada.
A.12.2.2	Control de procesamiento interno	Control Se deben incorporar chequeos de validación en las aplicaciones para detectar cualquier corrupción de la información a través de errores de procesamiento o actos deliberados.

A.12.2.3	Integridad del mensaje	Control Se deben identificar los requerimientos para asegurar la autenticidad y protección de la integridad de mensaje en las aplicaciones, y se deben identificar e implementar los controles apropiados.
A.12.2.4	Validación de data de output	Control Se debe validar el output de data de una aplicación para asegurar que el procesamiento de la información almacenada sea correcto y apropiado para las circunstancias.
A.12.3 Controles criptográficos Objetivo: Proteger la confidencialidad, autenticidad o integridad de la información a través de medios criptográficos.		
A.12.3.1	Política sobre el uso de controles criptográficos	Control Se debe desarrollar e implementar una política sobre el uso de controles criptográficos para la protección de la información.
A.12.3.2	Gestión clave	Control Se debe utilizar una gestión clave para dar soporte al uso de las técnicas de criptografía en la organización.
A.12.4 Seguridad de los archivos del sistema Objetivo: Garantizar la seguridad de los archivos del sistema		
A.12.4.1	Control de software operacional	Control Se debe contar con procedimientos para controlar la instalación de software en los sistemas operacionales.
A.12.4.2	Protección de la data de prueba del sistema	Control Se debe seleccionar cuidadosamente, proteger y controlar la data de prueba
A.12.4.3	Control de acceso al código fuente del programa	Control Se debe restringir el acceso al código fuente del programa.
A.12.5 Seguridad en los procesos de desarrollo y soporte Objetivo*:* Mantener la seguridad del software e información del sistema de aplicación		
A.12.5.1	Procedimientos de control de cambio	Control La implementación de cambios se debe controlar mediante el uso de procedimientos formales de control de cambios.
A.12.5.2	Revisión técnica de las aplicaciones después de cambios en el sistema operativo	Control Cuando se cambian los sistemas operativos, se deben revisar y probar las aplicaciones críticas del negocio para asegurar que no exista un impacto adverso en las operaciones o seguridad organizacional.
A.12.5.3	Restricciones sobre los cambios en los paquetes de software	Control No se deben fomentar las modificaciones a los paquetes de software, se deben limitar a los cambios necesarios y todos los cambios deben ser controlados estrictamente.
A.12.5.4	Filtración de información	Control Se deben evitar las oportunidades de filtraciones en la información.
A.12.5.5	Desarrollo de outsourced software	Control El desarrollo de software que ha sido outsourced debe ser supervisado y monitoreado por la organización.
A.12.6 Gestión de vulnerabilidad técnica Objetivo: Reducir los riesgos resultantes de la explotación de vulnerabilidades técnicas publicadas.		
A.12.6.1	Control de vulnerabilidades técnicas	Control Se debe obtener información oportuna sobre las vulnerabilidades técnicas de los sistemas de información en uso; se debe evaluar la exposición de la organización ante esas vulnerabilidades; y se deben tomar las medidas apropiadas para tratar el riesgo asociado.
A. 13 Gestión de incidentes en la seguridad de la información		
A.13.1 Reporte de eventos y debilidades en la seguridad de la información Objetivo*:* Asegurar que la información de los eventos y debilidades en la seguridad de la información asociados con los sistemas de información sea comunicada de una manera que permita tomar una acción correctiva oportuna.		

A.13.1.1	Reporte de eventos en la seguridad de la información	Control Los eventos de seguridad de la información deben reportarse a través de los canales gerenciales apropiados lo más rápidamente posible.
A.13.1.2	Reporte de debilidades en la seguridad	Control Se debe requerir que todos los empleados, contratistas y terceros usuarios de los sistemas y servicios de información tomen nota y reporten cualquier debilidad observada o sospechada en la seguridad de los sistemas o servicios.
A.13.2 Gestión de incidentes y mejoras en la seguridad de la información Objetivo: Asegurar que se aplique un enfoque consistente y efectivo a la gestión de la seguridad de la información.		
A.13.2.1	Responsabilidades y procedimientos	Control Se deben establecer las responsabilidades y procedimientos gerenciales para asegurar una respuesta rápida, efectiva y ordenada a los incidentes de seguridad de la información.
A.13.2.2	Aprendizaje de los incidentes en la seguridad de la información	Control Deben existir mecanismos para permitir cuantificar y monitorear los tipos, volúmenes y costos de los incidentes en la seguridad de la información.
A.13.2.3	Recolección de evidencia	Control Cuando la acción de seguimiento contra una persona u organización después de un incidente en la seguridad de la información involucra una acción legal (sea civil o criminal), se debe recolectar, mantener y presentar evidencia para cumplir las reglas de evidencia establecidas en la(s) jurisdicción(es) relevantes.
A.14 Gestión de la continuidad comercial		
A.14.1 Aspectos de la seguridad de la información de la gestión de la continuidad comercial Objetivo: Contrarrestar las interrupciones de las actividades comerciales y proteger los procesos comerciales críticos de los efectos de fallas o desastres importantes o desastres en los sistemas de información y asegurar su reanudación oportuna.		
A.14.1.1	Incluir seguridad de la información en el proceso de gestión de continuidad comercial	Control Se debe desarrollar y mantener un proceso gerencial para la continuidad del negocio a través de toda la organización para tratar los requerimientos de seguridad de la información necesarios para la continuidad comercial de la organización.
A.14.1.2	Continuidad comercial y evaluación del riesgo	Control Se deben identificar los eventos que causan interrupciones en los procesos comerciales, junto con la probabilidad e impacto de dichas interrupciones y sus consecuencias para la seguridad de la información.
A.14.1.3	Desarrollar e implementar planes de continuidad incluyendo seguridad de la información	Control Se deben desarrollar e implementar planes para mantener o restaurar las operaciones y asegurar la disponibilidad de la información en el nivel requerido y en las escalas de tiempo requeridas después de la interrupción o falla en los procesos comerciales críticos.
A.14.1.4	Marco referencial para la planeación de la continuidad comercial	Control Se debe mantener un solo marco referencial de planes de continuidad comercial para asegurar que todos los planes sean consistentes y para tratar consistentemente los requerimientos de la seguridad de la información e identificar las prioridades de pruebas y mantenimiento.
A.14.1.5	Prueba, mantenimiento y reevaluación de planes de continuidad comerciales	Control Los planes de continuidad comercial se deben probar y actualizar regularmente para asegurar que estén actualizados y sean efectivos.
A.15 Cumplimiento		
A.15.1 Cumplimiento con requerimientos legales Objetivo*:* Evitar violaciones de cualquier ley, obligación reguladora o contractual y de cualquier requerimiento de seguridad		
A.15.1.1	Identificación de legislación	Control Se deben definir explícitamente, documentar y actualizar todos los

	aplicable	requerimientos estatutarios, reguladores y contractuales y el enfoque de la organización relevante para cada sistema de información y la organización.
A.15.1.2	Derechos de propiedad intelectual (IPR)	Control Se deben implementar los procedimientos apropiados para asegurar el cumplimiento de los requerimientos legislativos, reguladores y contractuales sobre el uso de material con respecto a los derechos de propiedad intelectual y sobre el uso de los productos de software patentados.
A.15.1.3	Protección los registros organizacionales	Control Se deben proteger los registros importantes de una organización de pérdida, destrucción y falsificación, en concordancia con los requerimientos estatutarios, reguladores, contractuales y comerciales.
A.15.1.4	Protección de data y privacidad de información personal	Control Se deben asegurar la protección y privacidad tal como se requiere en la legislación relevante, las regulaciones y, si fuese aplicable, las cláusulas contractuales.
A.15.1.5	Prevención de mal uso de medios de procesamiento de información	Control Se debe desanimar a los usuarios de utilizar los medios de procesamiento de la información para propósitos no-autorizados.
A.15.1.6	Regulación de controles criptográficos	Control Se deben utilizar controles en cumplimiento con los acuerdos, leyes y regulaciones relevantes.
A.15.2 Cumplimiento con las políticas y estándares de seguridad, y el cumplimiento técnico Objetivo: Asegurar el cumplimiento de los sistemas con las políticas y estándares de seguridad organizacional.		
A.15.2.1	Cumplimiento con las políticas y estándares de seguridad	Control Los gerentes deben asegurar que todos los procedimientos de seguridad dentro de su área de responsabilidad sean realizados correctamente en cumplimiento con las políticas y estándares de seguridad.
A.15.2.2	Chequeo de cumplimiento técnico	Control Los sistemas de información deben chequearse regularmente para el cumplimiento con los estándares de implementación de la seguridad.
A.15.3 Consideraciones de auditoría de los sistema de información Objetivo: Maximizar la efectividad de y minimizar la interferencia de/desde el proceso de auditoría de los sistema de información.		
A.15.3.1	Controles de auditoría de sistemas de información	Control Se deben planear cuidadosamente los requerimientos y actividades de las auditorías que involucran chequeo de los sistemas operacionales y se debe acordar minimizar el riesgo de interrupciones en los procesos comerciales.
A.15.3.2	Protección de las herramientas de auditoría de los sistemas de información	Se debe proteger el acceso a las herramientas de auditoría de los sistemas de información para evitar cualquier mal uso o compromiso posible.

[Anexo I]

Anexo C. Tabla C.1 Ejemplos de amenazas comunes norma NTC- ISO 27005:2009 Gestión de Riesgos en la Seguridad de la Información

ANEXO C
(Informativo)
EJEMPLOS DE AMENZAS COMUNES

La siguiente tabla presenta ejemplos de amenazas comunes. La lista se puede utilizar durante el proceso de valoración de las amenazas. Estas pueden ser deliberadas, accidentales o ambientales (naturales) y pueden dar como resultado, por ejemplo, daño o pérdida de los servicios esenciales. Para cada uno de los tipos de amenazas, la siguiente lista indica los casos en que D (deliberadas), A (accidentales) y E (ambientales) son pertinentes. La letra D se utiliza para todas las acciones deliberadas que tienen como objetivos los activos de la información, A se utiliza para las acciones humanas que pueden dañar accidentalmente los activos de información y E se utiliza para todos los incidentes que no se basa en las acciones humanas. Los grupos de amenazas no están en orden de prioridad.

Tipo	Amenazas	Origen
Daño Físico	Fuego	A, D, E
	Daño por agua	A, D, E
	Contaminación	A, D, E
	Accidente importante	A, D, E
	Destrucción de equipo o los medios	A, D, E
	Polvo, corrosión, congelamiento	A, D, E
Eventos Naturales	Fenómenos climáticos	E
	Fenómenos sísmicos	E
	Fenómenos volcánicos	E
	Fenómenos meteorológicos	E
	Inundación	E
Pérdida de los servicios esenciales	Falla en el sistema de suministro de agua o aire acondicionado	A, D
	Pérdida del suministro de energía	A, D, E
	Falla en el equipo de telecomunicaciones	A, D
Perturbación debida a la radiación	Radiación electromagnética	A, D, E
	Radiación térmica	A, D, E
	Impulsos electromagnéticos	A, D, E
Compromiso de la información	Intercepción de señales de interferencias comprometedoras	D
	Espionaje remoto	D
	Escucha encubierta	D
	Hurto de medios o documentos	D
	Hurto de equipo	D
	Recuperación de medios reciclados o desechados	D
	Divulgación	A, D
	Datos provenientes de de fuentes no confiables	A, D
	Manipulación con hardware	D
	Manipulación con software	A, D
	Detección de posición	D
Fallas técnicas	Falla del equipo	A
	Mal funcionamiento del equipo	A
	Saturación del sistema de información	A, D
	Mal funcionamiento del software	A
	Incumplimiento en el mantenimiento del sistema de información	A, D
Acciones no autorizadas	Uso no autorizado del equipo	D
	Copia fraudulenta del software	D
	Uso del software falso o copiado	A, D
	Corrupción de los datos	D
	Procesamiento ilegal de los datos	D

Tipo	Amenazas	Origen
Compromiso de las funciones	Error en el uso	A
	Abuso de derechos	A, D
	Falsificación de derechos	D
	Negación de acciones	D
	Incumplimiento en la disponibilidad del personal	A, D, E

Se recomienda poner atención particular a las fuentes de amenazas humanas. Éstas se desglosan específicamente en la siguiente tabla:

Fuente de amenazas	Motivación	Acciones amenazantes
Pirata informático, intruso ilegal	Reto Ego Rebelión Estatus Dinero	Piratería Ingeniería social Intrusión, accesos forzados al sistema Acceso no autorizado al sistema
Criminal de la computación	Destrucción de información Divulgación ilegal de la información Ganancia monetaria Alteración no autorizada de los datos	Crimen por computador (por ejemplo, espionaje cibernético) Acto fraudulento (por ejemplo, repetición, personificación, intercepción) Soborno de la información Suplantación de identidad Intrusión en el sistema
Terrorismo	Chantaje Destrucción Explotación Venganza Ganancia política Cubrimiento de los medios de comunicación	Bomba/terrorismo Guerra de la información (warfare) Ataques contra el sistema (por ejemplo, negación distribuida del servicio) Penetración en el sistema Manipulación del sistema
Espionaje industrial (inteligencia, empresas, gobiernos, extranjeros, otros intereses gubernamentales)	Ventaja competitiva Espionaje económico	Ventaja de defensa Ventaja Política Explotación económica Hurto de información Intrusión en la privacidad personal Ingeniería social Penetración en el sistema Acceso no autorizado al sistema (acceso a información clasificada, de propiedad y/o relacionada con la tecnología)
Intrusos (empleados con entrenamiento deficiente, descontentos, malentendidos, negligentes, deshonestos o despedidos)	Curiosidad Ego Inteligencia Ganancia monetaria Venganza Errores y omisiones no intencionales) por ejemplo, error en el ingreso de los datos, error de programación)	Asalto a un empleado Chantaje Observar información reservada Uso inadecuado del computador Fraude y hurto Soborno de información Ingreso de datos falsos o corruptos Intercepción Código malicioso do (por ejemplo, virus, bomba lógica, troyano) Venta de información personal Errores en el sistema (bugs) Intrusión del sistema Sabotaje del sistema Acceso no autorizado al sistema

[Anexo J]

Anexo D. Tabla D.1 Ejemplos de Vulnerabilidades norma NTC- ISO 27005:2009 Gestión de Riesgos en la Seguridad de la Información

ANEXO D

(Informativo)

EJEMPLOS DE VULNERABILIDADES

La siguiente tabla presenta ejemplos de vulnerabilidades en diversas áreas de seguridad, e incluye ejemplos de amenazas que pueden explotar vulnerabilidades. La lista puede brindar ayuda durante la valoración de las amenazas y vulnerabilidades, con el fin de determinar escenarios pertinentes de incidentes. Se hace énfasis en que algunos casos otras amenazas también pueden tomar ventaja de estas vulnerabilidades.

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Hardware	Mantenimiento insuficiente/instalación fallida de los medios de almacenamiento.	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de esquemas de reemplazo periódico	Destrucción de equipos o de medios
	Susceptibilidad a la humedad, el polvo y la suciedad	Polvo, corrosión, congelamiento
	Sensibilidad a la radiación electromagnética	Radiación electromagnética
	Ausencia de un eficiente control de cambios en la configuración	Error en el uso
	Susceptibilidad a las variaciones de voltaje	Perdida de suministro de energía
	Almacenamiento sin protección	Hurto de medios o documentos
	Falta de cuidado en la disposición final	Hurto de medios o documentos
	Copia no controlada	Hurto de medios o documentos
Software	Ausencia o insuficiencia de pruebas de software	Abuso de los derechos
	Defectos bien conocidos en el software	Abuso de los derechos
	Ausencia de "terminación de la sesión" cuando se abandona la estación de trabajo	Abuso de los derechos
	Disposición o reutilización de los medios de almacenamiento sin borrador adecuado	Abuso de los derechos
	Ausencia de pistas de auditoria	Abuso de los derechos
	Asignación errada de los derechos de acceso	Abuso de los derechos
	Software ampliamente distribuido	Corrupción de datos
	En términos de tiempo utilización de datos errados en los programas de aplicación	Corrupción de datos
	Interfaz de usuario compleja	Error en el uso
	Ausencia compleja	Error en el uso
	Ausencia de documentación	Error en el uso
	Configuración incorrecta de parámetros	Error en el uso
	Fechas incorrectas	Error en el uso
	Ausencia de mecanismos de identificación y autenticación de usuario	Falsificación de derechos
	Tablas de contraseñas sin protección	Falsificación de derechos
	Gestión deficiente de las contraseñas	Falsificación de derechos
	Habilitación de servicios innecesarios	Mal funcionamiento del software
	Software nuevo o inmaduro	Mal funcionamiento del software
	Especificaciones incompletas o no claras para los desarrolladores	Mal funcionamiento del software
	Ausencia de control de cambio eficaz	Mal funcionamiento del software
	Descarga y uso no controlados de software	Manipulación de software
	Ausencia de copias de respaldo	Manipulación de software

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Software	Ausencia de protección física de la edificación puertas y ventanas	Hurto de medios o documentos
	Falla en la producción de informes de gestión	Uso no autorizado del equipo
Red	Ausencia de pruebas de envió o recepción de mensajes	Negación de acciones
	Líneas de comunicación sin protección	Escucha encubierta
	Tráfico sensible sin protección	Escucha encubierta
	Conexión deficiente de los cables	Falla del equipo de telecomunicaciones
	Punto único de fallas	Falla del equipo de telecomunicaciones
	Ausencia de identificación y autenticación de emisor y receptor	Falsificación de derechos
	Arquitectura insegura de la red	Espionaje remoto
	Transferencia de contraseñas en claro	Espionaje remoto
	Gestión inadecuada de la red (Tolerancia a fallas en el enrutamiento)	Saturación del sistema de información
Personal	Ausencia de personal	Incumplimiento en la disponibilidad del personal
	Procedimientos inadecuados de contratación	Destrucción de equipos o medios
	Entrenamiento insuficiente en seguridad	Error de uso
	Uso incorrecta de software y hardware	Error de uso
	Falta de conciencia acerca de seguridad	Error de uso
	Ausencia de mecanismo de monitoreo	Procesamiento ilegal de los datos
	Trabajo no supervisado del personal externo o de limpieza	Hurto de medios o documento
	Ausencia de políticas para el uso correcto de los medios de telecomunicaciones y mensajería	Uso no autorizado o medios
Lugar	Uso inadecuado o descuidado del control de acceso físico a las edificaciones y los recintos	Destrucción de equipo o medios
	Ubicación en un área susceptible de inundación	Inundación
	Red energética inestable	Perdida del suministro eléctrico
	Ausencia de protección física de la edificación, puertas y ventanas	Hurto de equipo
Organización	Ausencia de procedimiento formal para el registro y retiro de usuarios	Abuso de los derechos
	Ausencia de proceso formal para la revisión (supervisión) de los derechos de acceso	Abuso de los derechos
	Ausencia o insuficiencia de disposición (con respecto a la seguridad) en los contratos con los clientes y/o terceras partes	Abuso de los derechos
	Ausencia de procedimientos de monitoreo de los recursos de procesamiento de información	Abuso de los derechos
	Ausencia de auditorías (supervisiones) regulares	Abuso de los derechos
	Ausencia de procedimientos de identificación y valoración de riesgos	Abuso de los derechos
	Ausencia de reportes de fallas en los registros de administradores y operadores	Abuso de los derechos
	Repuesta inadecuada de mantenimiento del servicio	Incumplimiento en el mantenimiento del sistema de información

Tipos	Ejemplos de vulnerabilidades	Ejemplos de amenazas
Organización	Ausencia de acuerdos de nivel de servicio, o insuficiencia en los mismos	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimientos de control de cambios	Incumplimiento en el mantenimiento del sistema de información
	Ausencia de procedimientos formal para el control de la documentación del SGSI	Corrupción de los datos
	Ausencia de procedimientos formal para la supervisión del registro del SGSI	Corrupción de los datos
	Ausencia de procedimiento formal para la autorización de la información disponible al público	Datos provenientes de fuentes no confiables
	Ausencia de asignación adecuada de responsabilidades en la seguridad de la información	Negación de acciones
	Ausencia de planes de continuidad	Falla del equipo
	Ausencia de políticas sobre el uso del correo electrónico	Error en el uso
	Ausencia de procedimientos para la introducción del software en los sistemas operativos	Error en el uso
	Ausencia de los registros en la bitácoras (logs) de administrador y operario	Error en el uso
	Ausencia de procedimientos para el manejo de información clasificada	Error en el uso
	Ausencia de responsabilidades en la seguridad de la información en la descripción de los cargos	Error en el uso
	Ausencia o insuficiencia en las disposiciones (con respecto a la seguridad de la información) en los contratos con los empleados	Procesamiento ilegal de datos
	Ausencia de procesos disciplinarios definidos en el caso de incidentes de seguridad de la información	Hurto de equipo
	Ausencia de política formal sobre la utilización de computadores portátiles	Hurto de equipo
	Ausencia de control de los activos que se encuentran fuera de la instalaciones	Hurto de equipo
	Ausencia o insuficiencia de política sobre la limpieza de escritorio y de pantalla	Hurto de medios o documentos
	Ausencia de autorización de los recursos de procesamiento de información	Hurto de medios o documentos
	Ausencia de mecanismos de monitoreo establecidos para la brechas de seguridad	Hurto de medios o documentos
	Ausencia de revisiones regulares por parte de la gerencia	Uso no autorizado del equipo
	Ausencia de procedimientos para la presentación de informes sobre debilidades en la seguridad	Uso no autorizado del equipo
	Ausencia de procedimientos del cumplimiento de las disipaciones con los derechos intelectuales	Uso de software falso o copiado